FAKULTETA ZA ZDRAVSTVO ANGELE BOŠKIN

DOKTORSKI ŠTUDIJ ZDRAVSTVENE VEDE

SMER ŠTUDIJA: ZDRAVSTVENI MANAGEMENT

POVEZANOST DIMENZIJ INFORMACIJSKE VARNOSTNE KULTURE Z NAMERO IZVEDBE KRŠITEV INFORMACIJSKE VARNOSTI S STRANI ZAPOSLENIH V ZDRAVSTVENI NEGI – PRESEČNA RAZISKAVA

THE CORRELATION BETWEEN THE DIMENSIONS OF INFORMATION SECURITY CULTURE AND THE INTENT TO VIOLATE INFORMATION SECURITY BY NURSING STAFF – A CROSS-SECTIONAL STUDY

DOKTORSKA DISERTACIJA

SAMANTA MIKULETIČ

Fakulteta za zdravstvo Angele Boškin
Angela Boškin Faculty of Health Care

Doktorska disertacija
Študijski program tretje stopnje
ZDRAVSTVENE VEDE

Smer študija: Zdravstveni management

POVEZANOST DIMENZIJ INFORMACIJSKE VARNOSTNE KULTURE Z NAMERO IZVEDBE KRŠITEV INFORMACIJSKE VARNOSTI S STRANI ZAPOSLENIH V ZDRAVSTVENI NEGI – PRESEČNA RAZISKAVA

THE CORRELATION BETWEEN THE DIMENSIONS OF INFORMATION SECURITY CULTURE AND THE INTENT TO VIOLATE INFORMATION SECURITY BY NURSING STAFF – A CROSS-SECTIONAL STUDY

Doktorska disertacija

Mentor:
red. prof. dr. Boštjan Žvanut
Somentorica:
red. prof. dr. Brigita Skela-Savič, znan. svet.

Kandidatka:
Samanta Mikuletič

Ljubljana, maj, 2024

Mentor: red. prof. dr. Boštjan Žvanut, Univerza na Primorskem, Fakulteta za vede o zdravju

Somentorica: red. prof. dr. Brigita Skela-Savič, znan. svet., Fakulteta za zdravstvo Angele Boškin

Člani Komisije za oceno primernosti teme in za oceno doktorske disertacije:

- red. prof. dr. Danica Železnik, Fakulteta za zdravstvene in socialne vede Slovenj Gradec;
- izr. prof. dr. Uroš Rajkovič, Fakulteta za organizacijske vede, Univerza v Mariboru;
- izr. prof. dr. Mirna Macur, Ministrstvo za zdravje, Urad za kakovost in investicije v zdravstvo in Fakulteta za zdravstvo Angele Boškin.

IN MEMORIAM

Amalija Mikuletič

ZAHVALA

»A journey of a thousand miles
must begin with a single step.« (Lao Tzu)

Do novega spoznanja je bilo treba po poti polnih ovinkov, tlakovani z vzponi in padci. Vendar z ramo ob rami in pravim popotnikom je pot lažja, včasih hecna, pa tudi polna pasti, zanimiva, avanturistična, adrenalinska. Imeti oporo in ostati v pokončnem položaju je dandanes težko. Veliko je popotnikov, spoznanih na točkah dilem in brez katerih pomoči in sugestij bi bil cilj potovanja težko dosegljiv. Vendar, prišli smo do konca, prišli smo do cilja in zahvaljujoč popotnikom je srž ugledala luč sveta …

Neizmerno se zahvaljujem mentorju, red. prof. Boštjanu Žvanutu, s katerim sva raziskovala področje informacijske varnosti v zdravstveni negi že nekaj let prej. Hvala za oporo, ob kateri sem raziskovalno rastla. Hvala za vodenje, spodbujanje, razumevanje, potrpljenje, skrb in srčnost. Iskreno se zahvaljujem tudi somentorici, red. prof. dr. Brigiti Skeli Savič, znan. svet. Zahvaljujem se članom Komisije za oceno primernosti teme in za oceno doktorske disertacije, red. prof. dr. Danici Železnik, izr. prof. dr. Urošu Rajkoviču, izr. prof. dr. Mirni Macur in red. prof. dr. Poloni Selič, znanstveni svetnici. Zahvaljujem se vam za nasvete, ki so izboljšali in utrdili temelje moje doktorske disertacije.

Posebna zahvala gre ostalim popotnikom. Hvala, ker ste se odzvali prošnji za pomoč in sodelovanje. Zahvaljujem se raziskovalcem Akhyari Nasir, Ruzaini Abdullah Arshah in Mohd Rashid Ab Hamid, ki so dovolili prevod, uporabo in adaptacijo merskega instrumenta, ter anglistkam Anji Hofman in Tini Grlj, ki sta sodelovali v postopku prevoda vprašalnika. Za svetovanje pri preliminarnem delu kvalitativne raziskave se zahvaljujem Maji Frencl Žvanut in izbranim medicinskim sestram ter informatikom iz kliničnega okolja. Hvala gre za uvodne debate pri uporabi Teorije razumne akcije in Teoriji načrtovanega vedenja dr. Evi Podošovnik. Za pomoč pri rabi psiholoških izrazov se zahvaljujem doc. Katarini Babnik in izr. prof. Maši Črnelič Bizjak. Za pregled vprašalnika in predloge se zahvaljujem informatiku, doc. dr. Patriku Pucerju in prav tako

strokovnjaku za informacijsko varnost, izr. prof. dr. Simonu Vrhovcu. Slednjemu se zahvaljujem tudi za sodelovanje pri nastajanju članka. Za lektoriranje povzetka in razširjenega povzetka v angleškem jeziku se zahvaljujem dr. Martini Paradiž, univ. dipl. ang. ter doktorici prevodoslovja, in dr. Alenki Čuš, univ. dipl. slov. za jezikovni pregled disertacije v slovenskem jeziku.

Velika zahvala gre Zbornici zdravstvene in babiške nege Slovenije – Zvezi strokovnih društev medicinskih sester, babic in zdravstvenih tehnikov Slovenije, ki je omogočila izvedbo presečne raziskave.

Zahvala gre tudi moji družini. Dominiku, ki je brezpogojno verjel vame in me podpiral, pa tudi veliko prenesel ob pisanju tega dela; in mojemu Marcelu, ki je bil kdaj prikrajšan moje prisotnosti, ter malemu Ožbeju. Zahvaljujem se svojima staršema, da sta mi privzgojila vrednote, ki so mi omogočile prepešačiti pot in me naučila, da je potrebno ostati skromen. Hvala vam, da ste pogostokrat priskočili na pomoč in prevzeli nase številne moje obveznosti.

Zahvaljujem se vsem, ki ste na kakršen koli način doprinesli košček k mozaiku novega spoznanja.

IZJAVA O AVTORSKEM DELU DOKTORSKE DISERTACIJE IN ISTOVETNOSTI TISKENAGE IN ELEKTRONSKEGA IZVODA DOKTORSKE DISERTACIJE

Podpisana Samanta Mikuletič izjavljam, da je doktorska disertacija z naslovom *Povezanost dimenzij informacijske varnostne kulture z namero izvedbe kršitev informacijske varnosti s strani zaposlenih v zdravstveni negi – presečna raziskava* lastno avtorsko delo, izdelano samostojno ob pomoči mentorja red. prof. dr. Boštjana Žvanuta in somentorice red. prof. dr. Brigite Skele-Savič.

Izjavljam, da je tiskani izvod doktorske disertacije istoveten elektronskemu izvodu.

Datum in kraj:
4. 5. 2024, Gornji Zemon

Podpis doktorantke:

IZVLEČEK

Opredelitev raziskovalnega problema: Zaposleni v zdravstveni negi imajo ključno vlogo pri varovanju zdravstvenih podatkov, saj predstavljajo levji delež zaposlenih v zdravstvu in imajo neposreden dostop do zdravstvenih podatkov.

Namen in cilji raziskave: Namen raziskave je bil preučiti dimenzije informacijske varnostne kulture in s pomočjo Teorije načrtovanega vedenja razložiti pojav kršitev informacijske varnosti s strani zaposlenih v zdravstveni negi. Cilj je bil preveriti koncept dimenzij in stanje na tem področju na populaciji zaposlenih v zdravstveni negi; preveriti povezanost dimenzij s konstrukti omenjene teorije ter ugotoviti, katere vzvode lahko uporabijo ustanove za zmanjšanje tveganja za kršitev zaupnosti zdravstvenih podatkov.

Metode: Izvedena je bila anketa med zaposlenimi v zdravstveni negi v Sloveniji (n = 527) v obdobju od aprila 2021, do marca 2022. S pridobljenimi podatki smo validirali merski instrument.

Rezultati: Rezultati analize PLS-SEM kažejo na posredno razmerje med dimenzijami informacijske varnostne kulture in nepooblaščenim dostopom do podatkov. Rezultati potrjujejo primernost Teorije načrtovanega vedenja za preučevanje kršitev informacijske varnosti. Največjo velikost učinka zasledimo pri povezavi med normativnimi prepričanji in vedenjsko namero kršitve informacijske varnosti.

Razprava: Pričujoča raziskava je ena prvih, ki preučuje nepooblaščen dostop do zdravstvenih podatkov z vidika informacijske varnostne kulture zaposlenih v zdravstveni negi. Definira in operacionalizira dve novi dimenziji informacijske varnostne kulture – usmerjenost k varnosti podatkov ter usmerjenost k zagotavljanju zasebnosti. Omejitve raziskave so v uporabi vprašalnika za vrednotenje vedenjske namere, samoocenjevanje, raba presečnega načrta in tveganje za napako nepokritja.

Prispevek k znanosti: Potrditev uporabnosti Teorije načrtovanega vedenja za preučevanje kršitev informacijske varnosti in identifikacija specifičnih dimenzij informacijske varnostne kulture, značilnih za področje zdravstvene nege ter prilagoditev in validacija merskega instrumenta za merjenje informacijske varnostne kulture.

Ključne besede: zasebnost in varnost podatkov, zdravstveni podatki, elektronski zdravstveni zapisi, kršenje varnosti podatkov, informacijska varnost, zdravstvo, izvajalci zdravstvenih storitev

SUMMARY

Research problem definition: Nurses play a critical role in protecting health data, as they constitute a significant portion of the healthcare workforce and have direct access to health data.

Research aims and objectives: The aim of research was to investigate the dimensions of information security culture and explain the occurrence of information security breaches by nursing staff by applying the Theory of Planned Behaviour. Its objective was to review the concept of the dimensions and state of information security culture, examine the associations between these dimensions and the constructs of the Theory of Planned Behaviour, and identify potential levers for institutions to reduce the risk of health data confidentiality breaches.

Methods: A survey was conducted among nursing staff in Slovenia (n = 527) between April 2021 and March 2022. The measurement instrument was validated.

Results: The PLS-SEM analysis revealed an indirect relationship between the dimensions of information security culture and unauthorised data access. Results strongly support the application of the Theory of Planned Behaviour, with the association between normative beliefs and behavioural intention showing the largest effect size.

Discussion: The present study is one of the first to examine unauthorised access to healthcare data from the perspective of information security culture among nursing staff. It defines and operationalises two new dimensions of information security culture – privacy oriented and security oriented. Limitations of the study include the use of questionnaires to assess behavioural intentions, self-assessment, cross-sectional design, and the risk of non-coverage error.

Contribution of the doctoral dissertation to science: Confirmation of the applicability of the Theory of Planned Behaviour and identification of specific dimensions of information security culture unique to the field of healthcare and nursing, along with the adaptation and validation of the measurement instrument used to measure information security culture.

Key words: data privacy and security, health data, electronic health records, data security breaches, information security, health care, healthcare providers

KAZALO

KAZALO SLIK

KAZALO TABEL

SEZNAM KRAJŠAV

ARCS	angl. »*Assessment of information security risk, Reduction of information security Cost and Sustainability of information security culture*«
ATB	Stališča do vedenja (angl. »*Attitude Toward the Behavior*«)
AVE	Povprečje izločenih varianc (angl. »*Average Variance Extracted*«)
BCa	Bootstrapping s popravkom in pospeškom (angl. »*Bias-Corrected and accelerated bootstrapping«)*
BI	Vedenjska namera (angl. »*Behavioral Intention*«)
CB-SEM	Modeliranje strukturnih enačb, ki temelji na kovariančni matriki (angl. »*A Structural Equation Modeling based on the covariance matrix*«)
CCA	Potrditvena kompozitna analiza (angl. »*Confirmatory Composite Analysis*«)
CFA	Konfirmativna ali potrditvena faktorska analiza (angl. »*Confirmatory Factor Analysis*«)
CI	Interval zaupanja (angl. »*Confidence Interval*«)
CLTRe Toolkit	Orodje za merjenje informacijske kulture
CMB	Pristranost zaradi skupne metode zbiranja podatkov (angl. »*Common Method Bias*«)
CMV	Varianca skupne metode (angl. »*Common Method Variance*«)
CseCRM	Raziskovalna metodologija kibernetske varnostne kulture (angl. »*Cyber security Culture Research Methodo*logy«)
CVF	angl. »*The Competing Values Framework*«
EFA	Eksploratorna faktorska analiza (angl. »*Exploratory Factor Analysis*«)
GDPR EU	Splošna uredba o varstvu podatkov (angl. »*EU General Data Protection Regulation*«)
GoF	Prileganje modela (angl. »*Goodness-of-Fit*«)
HIPAA	angl. »*The Health Insurance Portability and Accountability Act*«
HTMT	angl. »*The Heterotrait-Monotrait ratio of the correlations*«

IKT	Informacijsko-komunikacijska tehnologija
IS	Informacijski sistem
ISC	Informacijska varnostna kultura (angl. »*Information Security Culture*«)
ISCA	angl. »*Information Security Culture Assessment*«
ISCCM	angl. »*Information Security Culture Change Management*«
ISK	Znanje o informacijski varnosti (angl. »*Information Security Knowledge*«)
ISKS	Izmenjava znanja o informacijski varnosti (angl. »*Information Security Knowledge Sharing*«)
ISO	angl. »*International Organization for Standardization*«
ISP	Informacijska varnostna politika (angl. »*Information Security Policy*«)
IT	Informacijska tehnologija
KME	Komisija za medicinsko etiko Republike Slovenije
KMO	angl. »*Kaiser-Meyer-Olkin*«
MAE	Povprečna absolutna napaka (angl. »*the Mean Absolute Error*«)
MON	Nadzorovanje/spremljanje varnosti (angl. »*Security Monitoring*«)
NB	Normativna prepričanja (angl. »*Normative Belief*«)
PBC	Zaznan vedenjski nadzor (angl. »*Perceived Behavioural Control*«)
PCM	Postopkovni protiukrepi (angl. »*Procedural Countermeasures*«)
PDCA	Načrtuj, naredi, preveri, ukrepaj (angl. »*Plan, Do, Check, Act*«)
PLS	Metoda delnih najmanjših kvadratov (angl. »*Partial Least Squares*«)
PLS-SEM	angl. »*Partial Least Squares SEM*«
PLSc	angl. »*Partial Least Square consistent-SEM*«
PO	Usmerjenost k zagotavljanju zasebnosti« (angl. *»Privacy Oriented«)*
RM	Obvladovanje tveganj (angl. »*Risk Management*«)
RMSE	Povprečna kvadratna napaka (angl. »*the Root Mean Squared Error*«)
SE	Samoučinkovitost (angl. »*Self-Efficacy*«)
SEM	Modeliranje strukturnih enačb (angl. »*Structural Equation Modeling*«)

SETA	Varnostno izobraževanje, usposabljanje in ozaveščanje (angl. »*Security Education, Training and Awareness*«)
SN	Subjektivne norme (angl. »*Subjective Norm*«)
SO	Usmerjenost k varnosti podatkov« (angl. »*Security Oriented*«)
STOPE	angl. »*Strategy, Technology, Organization, People and Environment*«
TACT	angl. »*Target, Action, Contex, Time*«
TMC	Zavezanost vrhnjega managementa (angl. »*Top Management Commitment*«)
TRA	Teorija razumne akcije (angl. »*Theory of Reasoned Acti*on«)
TPB	Teorija načrtovanega vedenja (angl. »*Theory of Planned Behavior*«)
VIF	Faktor inflacije variance (angl. »*Variance Inflation Scores*«)

SEZNAM ČLANKOV

Mikuletič, S., Vrhovec, S., Skela-Savič, B. & Žvanut, B., 2024. Security and privacy oriented information security culture (ISC): Explaining unauthorized access to healthcare data by nursing employees. *Computers & Security*, 134, 103489. 10.1016/j.cose.2023.103489.

1 UVOD

Informacijska varnostna kultura izhaja iz načina vedenja zaposlenih v delovnem okolju do informacij in njihove varnosti. Način, s katerim zaposleni stopajo v interakcijo z informacijskimi viri in njihovo vedenje sčasoma postaneta ustaljen način dela v organizaciji. Zaposleni postane del organizacijske kulture in pomembno je, da njegov del postane tudi informacijska varnost. Vedenje zaposlenih do informacij mora biti sprejemljivo in mora biti del vsakdanjega življenja organizacije (Ovijač, et al., 2017). Informacijska varnostna kultura je pomemben element organizacijske kulture in se nanaša na vse oblike prizadevanj zmanjšanja tveganj kršitev informacijske varnosti in incidentov (Safa, 2017). Gre za zbirko varnostnih vrednot, prepričanj in predpostavk o informacijski varnosti v organizaciji in lahko vodi do nezavednega, običajnega ter varnostnega vedenja (Van Niekerk & Von Solms, 2010; Schein & Schein, 2019).

Z doktorsko disertacijo smo preučili vedenjsko namero zaposlenih v zdravstveni negi za izvedbo kršitve informacijske varnosti, t.j. nepooblaščenega dostopa do zdravstvenih podatkov v povezavi z informacijsko varnostno kulturo. Razumeti je namreč potrebno, kaj je tisto, kar v veliki meri posameznike vodi do izvedbe kršitev. Usmerjenost pogleda raziskovalca je v *dimenzije informacijske varnostne kulture* in njihovo povezanost s *stališči do vedenja*, *subjektivnimi normami*, *normativnimi prepričanji* ter *zaznanim vedenjskim nadzorom* posameznika. Preko navedenih konstruktov imajo dimenzije informacijske varnostne kulture učinek na posameznikovo vedenjsko namero in navsezadnje na vedenje – kršitev samo.

Zaposleni v organizaciji morajo biti izobraženi, usposobljeni in motivirani za upoštevanje varnostnih politik in postopkov (Chen, et al., 2012; Siponen & Vance, 2010). Zaradi zaščite informacijskih virov, poslovanja organizacije in njenega uspeha se vedno več organizacij nagiba k vpeljavi celovitih izobraževalnih programov (Chen, et al., 2015). Niso pa varnostna izobraževanja, usposabljanja in ozaveščanja ter varnostne politike edini pomembni dejavniki zagotavljanja varnosti informacij. Ti in drugi so opisani v nadaljevanju doktorske disertacije.

V uvodnem delu podpoglavja *Opis raziskovalnega problema* smo prikazali alarmantno stanje kršenja varnosti zdravstvenih podatkov v svetu, vendar se zaradi pomanjkanja podatkov nismo seznanili s stanjem v Republiki Sloveniji. Na področju zdravstvene nege je po nam znanih podatkih razmeroma malo raziskav, ki preučujejo obravnavano temo, predvsem pa takih, ki bi v zadostni meri pojasnjevale povezavo z namero kršitve informacijske varnosti.

V podpoglavju *Sistematični pregled literature* smo predstavili ugotovitve, analizirali teoretična spoznanja, definicije ter trende podatkov. Preučili smo organizacijsko varnostno kulturo, njeno subkulturo – informacijsko varnostno kulturo, razkorake v konsenzu uporabe faktorjev, dejavnikov ter dimenzij informacijske varnostne kulture, modele, orodja ter Teorijo utemeljene akcije in Teorijo načrtovanega vedenja.

V podpoglavju *Operacionalizacija raziskovalnega problema* smo opredelili ključna spoznanja, ki definirajo raziskovalni problem. Vsebuje argumentacijo izbire *Teorije načrtovanega vedenja* kot temelja in vključitev dveh novih konstruktov oz. dimenzij v že obstoječ vprašalnik avtorjev Nasir, et al. (2019a).

Sledi poglavje *Namen in cilji raziskave*, v katerem smo se opredelili do raziskovalnega vprašanja in hipotez.

V poglavju *Metode* smo predstavili raziskovalni načrt, udeležence raziskave – zaposlene v zdravstveni negi v Republiki Sloveniji. Podrobno smo opisali prevod in razvoj vprašalnika. Opisali smo potek raziskave in zbiranja potrebnih soglasij za opravljanje raziskave ter obdelavo podatkov.

V poglavju *Rezultati* smo opisno, tabelarično in grafično prikazali analizirane podatke, namenjene preverjanju hipotez in raziskovalnega vprašanja. Pri tem smo sledili smernicam za uporabo, analiziranje, prikazovanje in poročanje rezultatov (merilnih in strukturnih modelov), ki zadevajo analizo z orodjem PLS-SEM (Hair, et al., 2019a; Sarstedt, et al., 2021).

Pridobljene rezultate smo utemeljili in primerjali s predhodnimi spoznanji raziskav, v poglavju *Razprava.* Opredelili smo omejitve naše raziskave, možen prenos spoznanj raziskave na aplikativno raven in vprašanja, ki se dotikajo nadaljnjega preučevanja. Predstavili smo prispevek k znanosti in k razvoju stroke k znanstveni disciplini.

1.1 OPREDELITEV RAZISKOVALNEGA PROBLEMA

Preučevanja kršitev informacijske varnosti za javni in zasebni sektor v tujini kažejo na pomembnost človeškega dejavnika. Neposredna človeška napaka je vzrok za razkritje v 23 % primerov (Ponemon Institute, 2020). Po podatkih instituta Ponemon (2020) so stroški, ki nastanejo pri identificiranju teh kršitev, motenj v poslovanju organizacij, izgubi strank, povečanju obveščanja vseh vpletenih in pomoč žrtvam, veliki. Povprečni stroški so npr. za leto 2020 znašali 3,86 milijona dolarjev. Med industrijami z najvišjimi stroški prevladuje zdravstveni sektor. Oddelek za zdravstvo in službo za državljanske pravice ZDA na svojem spletnem portalu redno evidentira omenjene kršitve (angl. »*data breaches*«) (U.S. DSS, n.d.) in te se povečujejo iz leta v leto (McCoy & Perlis, 2018; Dolezel & McLeod, 2019). V letu 2017 je visoko na vrhu, čeprav rahlo v upadanju kotirala kršitev nepooblaščenega dostopa do podatkov in njihovega razkritja (McCoy & Perlis, 2018). Kljub temeljitemu pregledu razpoložljivih virov nismo identificirali uradnih podatkov o kršitvah varnosti in zasebnosti zdravstvenih podatkov v Sloveniji.
Poročilo akademske in raziskovalne mreže ARNES o kibernetski varnosti kaže, da se na mesec v Sloveniji odda 562 prijav incidentov. Za področje varnosti informacijskih virov so tako v letu 2020 obravnavali 26 incidentov, od tega 13 nepooblaščenih dostopov do podatkov, osem nepooblaščenih spreminjanj podatkov in pet odtekanj informacij (SI-CERT, 2021).

Gre za alarmanten problem in področje, za katero si organizacije nikakor ne smejo dovoliti, da bi zaostale na tem področju. V zvezi z zagotavljanjem varnosti informacijskih virov so tehnološke metode varovanja učinkovite le do določene mere. Raziskovalci svojo pozornost usmerjajo predvsem na zaposlene v organizacijah – etiketirajo jih z »najšibkejšim členom« informacijske varnosti.

Kršitev varnosti osebnih podatkov je lahko storjena nehote (malomarnost) ali pa načrtovano, zlonamerno (naklep) (Kwon & Johnson, 2018). Najpogostejši vzrok je malomarnost zaposlenih pri rokovanju s podatki in notranja razkritja. Najpogostejši viri incidentov so aktualni (34 %) in bivši zaposleni (29 %) (Price-Waterhouse-Coopers, 2016). Ti so za informacijske vire organizacij najbolj nevarni, predvsem zaradi poznavanja organizacijskega informacijskega sistema (v nadaljevanju IS) in dostopa do podatkov med delovnim procesom. Ključno vlogo pri vsem ima človeški dejavnik.

Kršitev varnosti osebnih podatkov je varnostni incident, ki ogroža zaupnost, celovitost in dostopnost do osebnih podatkov. V praksi se lahko kaže kot nepooblaščeni dostop do podatkov, posredovanje osebnih podatkov nepooblaščenemu naslovniku, izguba ali kraja informacijsko-komunikacijske tehnologije (v nadaljevanju IKT), nepooblaščeno uničenje baz z osebnimi podatki, sprememba osebnih podatkov brez potrebnega dovoljenja ali izguba dostopa do osebnih podatkov (npr. izguba gesla, opreme, nepooblaščena namestitev šifrirnega programa, ki onemogoča dostop do podatkov) (Johnson 2009; Informacijski pooblaščenec, n.d.).

Zaščita zdravstvenih podatkov je še posebej zahtevna (Terry, 2017) zaradi potencialnih groženj in vse večjega števila kršitev varnosti informacij (US DHSS, n.d.). Informacijska varnost in zasebnost imata zaradi naglega tehnološkega napredka – digitalizacije zdravstvenih zapisov in naraščajoče potrebe po njihovi uporabi in izmenjavi vse večji pomen; tega pa zaznamuje spolzko pobočje organizacijskih, tehničnih in navsezadnje etično-pravnih pomislekov (Natsiavas, et al., 2019).

Zdravstveni sektor je izpostavljen potencialni izgubi ugleda in morebitnim stroškom, ki so posledica razkritja zdravstvenih podatkov (Ponemon Institute, 2015). Številni avtorji (Gebrasilase & Lessa, 2011; Kwon & Johnson, 2012; Agaku, et al., 2013; Gartrell, 2014; Božić, 2016; Ferguson, 2016; Hai, et al., 2017; Hassan, et al., 2017; He & Johnson, 2017; Lambe, et al., 2018) opominjajo na veliko pojavnost kršenja varnosti osebnih podatkov v zdravstvu in so si enotni, da so zdravstveni podatki izredno občutljivi (Liu, et al., 2012; Tejero & de la Torre, 2012; Box & Pottas, 2013; Hsu, et al., 2013; Huang, et al., 2014; Kamoun & Nicho, 2014; Chernyshev, et al., 2018; Gong, et al., 2020).

Zdravstveni podatki so najbolj občutljivi in zaupni osebni podatki, katerih nepooblaščeno razkritje vodi do pravnih in finančnih posledic (Johnson, 2009). Poleg teh posledic sta pomembni tudi etična in moralna odgovornost (Price & Cohen, 2019).

Varstvo osebnih podatkov posamezniku zagotavlja že sama *Ustava Republike Slovenije* (1991). Ta v svojem 38. členu narekuje, da zbiranje, obdelovanje, namen uporabe, nadzor in varstvo tajnosti osebnih podatkov urejata *Zakon o pacientovih pravicah* (2008) in *Zakon o varstvu osebnih podatkov* (2007). Slednji v svojem 24. členu določa, da *»varovanje osebnih podatkov obsega organizacijske, tehnične in logično-tehnične postopke in ukrepe, s katerimi se varujejo osebni podatki, preprečuje slučajno ali namerno nepooblaščeno uničevanje podatkov, njihova sprememba ali izguba ter nepooblaščena obdelava ...«* (ZVOP-1, 24. člen, p. 12711). *Splošna uredba EU o varstvu podatkov* (2016) (v nadaljevanju GDPR EU – angl. »*EU General Data Protection Regulation*«) narekuje usklajen okvir varstva in državljanom omogoča nadzor nad svojimi osebnimi podatki, hkrati pa strogo predpisuje pogoje obdelave le-teh. Pod točkama 12 in 15 definira podatke o zdravstvenem stanju kot: »*osebne podatke, ki se nanašajo na telesno ali duševno zdravje posameznika, vključno z zagotavljanjem zdravstvenih storitev, in razkrivajo informacije o njegovem zdravstvenem stanju«*, ter opredeljuje, da je kršitev varstva osebnih podatkov: »*kršitev varnosti, ki povzroči nenamerno ali nezakonito uničenje, izgubo, spremembo, nepooblaščeno razkritje ali dostop do osebnih podatkov, ki so poslani, shranjeni ali kako drugače obdelani* (str. 34, 4. člen)« (GDPR, 4. člen, p. 34).

Posebnost zdravstvenega sektorja kot ključno vodilno načelo odnosa med pacientom in zdravstvenim delavcem je zasebnost obravnav. Kršitve varnosti zdravstvenih podatkov imajo pomemben vpliv na paciente in tudi ugled zdravstvenih organizacij. Razkritje ali zloraba zdravstvenih podatkov lahko povzroči resno škodo ugledu pacientov, kot so diskriminacija, stigmatizacija, izguba zavarovanja ali izguba zaposlitve (Appari & Johnson, 2010). Zaskrbljenost zaradi potencialne možnosti razkritja s strani pacientov lahko vodi do varnostnih pomislekov (Natsiavas, et al., 2019) in posledično do zamolčanja pomembnih podatkov zdravstvenim delavcem (Agaku, et al., 2013). Zaradi strahu pred razkritjem obstaja verjetnost, da pacient ne poda dejanske anamneze (npr.

duševne bolezni, HIV), saj bi njeno razkritje lahko povzročilo socialno stigmo in diskriminacijo (Appari & Johnson, 2010).

Grožnje informacijskim virom iz zunanjih in notranjih okolij so organizacije spodbudile ne le k namestitvi napredne strojne in programske opreme za zaščito pred morebitnimi zlonamernimi napadi od zunaj, temveč tudi k vzpostavitvi različnih politik in postopkov varovanja informacij, katerih namen je zmanjšanje in odvračanje namernih in nenamernih vedenj zaposlenih, ki bi lahko oslabili učinkovitost varovalnih sistemov strojne ali programske opreme. Samo izvajanje tehničnih rešitev za zavarovanje informacij ni samo po sebi dovolj (Butavicius, et al., 2020), saj je učinkovitost nadzora nad varnostjo informacij odvisna od usposobljenosti in zanesljivosti ljudi, ki te aktivnosti tudi izvajajo (Neame, 2014; Posey & Folger, 2020).

Gebrasilase in Lessa (2011) sta v svoji raziskavi ugotovila, da je v eni izmed bolnišnic v Etiopiji prisotno pomanjkanje zavesti med zaposlenimi, pomanjkanje zavezanosti in podpore vodstva za izvajanje informacijske varnosti ter odsotnost usposabljanja za zaposlene. Gartrell (2014) navaja, da je 70 % diplomiranih medicinskih sester zaposlenih v 12. bolnišnicah, lociranih v zveznih državah ZDA Maryland in Washington izrazilo skrb za zasebnost in varnost zdravstvenih podatkov na spletu pri uporabi elektronskih zdravstvenih zapisov. Agaku, et al. (2013) potrjujejo zaskrbljenost v raziskavo vključenih prebivalcev ZDA zaradi kršitev varnosti zdravstvenih podatkov, predvsem pri pošiljanju dokumentov preko faksa in elektronske pošte. He in Johnson (2017) sta pri preučevanju naletela na ovire pri učenju iz preteklih incidentov kršenja varnosti zdravstvenih podatkov. Podrobnosti ravnanja ob incidentu z nizko stopnjo resnosti niso bile, oz. so bile slabo dokumentirane in so se osredotočale zgolj na tehnične vidike. Hai, et al (2017) potrjujejo, da 74 % zaposlenih v ambulantah Vietnama, kjer se zdravijo pacienti s HIV-om, ni bilo deležnih izobraževanj s področja varstva osebnih podatkov in zasebnosti. Kljub temu pa je bila praksa zagotavljanja zaščite na sprejemljivi ravni. Večina osebja je skrbela za ohranjanje varnosti podatkov, imeli so dobro ali povprečno znanje in pozitivne zaznave glede vprašanj varnosti in zaupnosti. Ferguson (2016) je v svojo raziskavo vključil visoko usposobljene kirurške centre ZDA, ki so se z dobro prakso borili proti naraščajočemu trendu kršitev na področju varovanja podatkov. Rezultati so pokazali, da

je razvoj politike, procesov, postopkov, zavesti, izobraževanj ter usposabljanj ključnega pomena. Božić (2016) opisuje, da zaposleni v eni od zdravstvenih ustanov v Sloveniji slabo poznajo varnostno politiko. 21,7 % jih je že bila priča varnostnemu incidentu, medtem ko jih 35,6 % gesla deli med seboj. Lambe, et al. (2018) so ugotavljali, kako se varnost podatkov spreminja znotraj delovnega časa. Beležili so lokacijo vozičkov z zdravstveno dokumentacijo ter prisotnost zdravstvenega in drugega osebja v eni od bolnišnic v Dublinu (Irska). V 84 zabeleženih primerih so identificirali kar 33 % takih, ko so zdravstveni zapisi ostali brez nadzora. Kot taki so bili možen vir razkritja predvsem na hodnikih in postajah medicinskih sester (Lambe, et al., 2018).

Zgornji opisi situacij kažejo na alarmanten problem. Raziskovalci poudarjajo, da je potrebno izboljšati zaščito zaupnosti podatkov, zlasti pri dostopu, izmenjavi in njihovem prenosu (Hai, et al., 2017).

Podatki, ne glede na obliko, zahtevajo ustrezno zaščito, njihovi uporabniki pa so lahko potencialni predstavniki groženj (Appari & Johnson, 2010). Med tipičnim procesom zdravstvene nege ima lahko do 400 posameznikov dostop do zdravstvenih podatkov pacienta. Ker zaposleni v zdravstveni negi predstavljajo velik del le-teh, je informacijska varnost pomemben del njihovega vsakdanjega dela (Cannoy & Salam, 2010). Že sam kodeks etike v zdravstveni negi in oskrbi (v nadaljevanju Kodeks etike), v svojem III. načelu navaja: »*Izvajalci zdravstvene nege in oskrbe spoštujejo dostojanstvo in zasebnost pacienta v vseh stanjih zdravja, bolezni, ob umiranju ter po smrti*«. III. načelo Kodeksa etike se nanaša tudi na informacijsko zasebnost. Eden od standardov izvajanja v tem načelu je upoštevanje in spoštovanje pravice pacienta do zasebnosti ter intimnosti (Ovijač, et al., 2017). Informacijsko varnost zadeva tudi VI. načelo: »*Izvajalce zdravstvene nege in oskrbe zavezuje poklicna molčečnost*«. Standardi aktivnosti, ki zadevajo VI. načelo se nanašajo na (Ovijač, et al., 2017):

- *»Izvajalci zdravstvene nege in oskrbe so dolžni varovati poklicno skrivnost«.*
- *»Za poklicno skrivnost se šteje vse, kar izvajalci zdravstvene nege in oskrbe pri opravljanju svojega poklica izvedo o pacientu, o njegovih osebnih, družinskih, socialnih in drugih razmerah ter vse informacije v zvezi z zdravstveno nego, ugotavljanjem bolezni, zdravljenjem in rehabilitacijo«.*

- *»Če se je pacient tako odločil, so poklicno skrivnost dolžni varovati tudi pred družinskimi člani pacienta ali zanj pomembnimi drugimi, kar velja tudi po njegovi smrti«.*
- *»Poklicne molčečnosti izvajalce zdravstvene nege in oskrbe lahko razreši pacient sam, ali če tako določajo z zakonom sprejete posebne določbe«.*

Ustrezno usposobljeni in zanesljivi zaposleni, ki se držijo postopkov za zaščito informacijske varnosti in moralnih načel, so zato ključnega pomena za preprečevanje kršitev informacijske varnosti. Za učinkovito spoprijemanje z omenjenimi tveganji je za organizacije izjemnega pomena informacijska varnostna kultura (Safa, 2017). Zdravstvene in druge organizacije se lahko z zgoraj opisanimi problemi spopadejo z njeno ustrezno kultivacijo, ta pa bo razvijala ustrezno varnostno vedenje med zaposlenimi in podpirala doseganje ciljev organizacije (Sari, et al., 2021).

V nadaljevanju poglavja obravnavamo znanstvena spoznanja. Izvedli smo pregled literature, fokusiran na zdravstvene ustanove in specifične komponente za to panogo, kot sta npr. etika ter etika skrbi, v katerem smo analizirali relevantne raziskovalne članke, monografije, prispevke na konferencah in doktorske disertacije, objavljene od leta 2000. Rezultati pregleda so predstavljeni v Prilogi 1. Da bi dobili boljši vpogled v vzroke očitne zmede glede dejavnikov in dimenzij informacijske varnostne kulture, smo kot vodila uporabili dela dveh raziskovalnih skupin, in sicer Nasir, et al. (2019b) ter Uchendu, et al. (2021).

1.2 SISTEMATIČNI PREGLED LITERATURE

1.2.1 Opredelitev informacijske varnostne kulture

V letih od 2010 do 2020 je bilo največ raziskav informacijske varnostne kulture izvedenih v Južni Afriki. Sledijo ji Azija, Evropa, Severna in Južna Amerika ter Bližnji Vzhod. Večina raziskav predstavlja teoretične okvirje, modele ali pristope, v katerem je mogoče zgraditi in vzdrževati varnostno kulturo. Osredotočenost teh raziskav je usmerjena na razvoj novih okvirjev in orodij ter k analiziranju pristopov za izgradnjo informacijske

varnostne kulture. Na voljo je tudi nekaj raziskav, ki se osredotočajo na metode, s katerimi je mogoče oceniti ali izmeriti fenomen; ostale se osredotočajo na dejavnike, ki delujejo na fenomen ali pa na definiranje le-tega (Uchendu, et al., 2021).

Vprašalniki in ankete so najpogosteje uporabljeno orodje za merjenje informacijske varnostne kulture, vendar je moč zaslediti tudi raziskave, ki temeljijo na intervjujih ter pregledih literature (Uchendu, et al., 2021).

Vzorec v raziskavah so največkrat zaposleni v organizacijah. Nobena panoga oz. sektor raziskovanja ni prevladujoč. Študije primerov organizacij vključujejo široko paleto organizacij, od proizvodenj, visokošolskih ustanov do finančnih in zavarovalniških podjetij. Raziskave se osredotočajo tudi na panoge, kot so izključno zdravstvo, bančništvo, finance, maloprodaja in javne organizacije (vlada, šolstvo) (Uchendu, et al., 2021).

V zadnjem desetletju je prepoznavnost varnostne kulture močno porasla, tako v praksi kot na področju raziskovanja. Vzrok za to je bil v povečanju kršitev v organizacijah, za katere je bil v prvi vrsti odgovoren človeški dejavnik. Na področju raziskovanja se je pojavila uporaba številnih izrazov, vključno z varnostno kulturo, informacijsko varnostno kulturo ter kibernetsko varnostno kulturo. Čeprav se kibernetska varnost pogosto uporablja kot sinonim za informacijsko varnost na splošno, se narava obeh izrazov nedvomno razlikuje (Uchendu, et al., 2021). Po mnenju Astakhove (2014) informacijska varnostna kultura in kibernetska varnostna kultura nista sinonima, ker je jedro informacijske varnostne kulture zaščita varnosti podatkov/informacij.

Obstajata širša in ožja definicija informacijske varnostne kulture. Širša definicija se nanaša bolj na organizacijsko varnostno kulturo (Lundy & Cowling, 1996). Definiramo jo kot način, kako stvari potekajo v organizaciji. Gre za nenapisana življenjska pravila in predpostavko o načinu dela oz. kako je delo opravljeno. Ožja definicija razlikuje med informacijsko varnostno kulturo, ki je globoko zakoreninjena in manj opazna ter informacijsko varnostno klimo, ki naj bi bila njena vidna manifestacija, v obliki organizacijskih politik, praks in postopkov (Chan, et al., 2005; Kessler, et al., 2020).

Nadalje v literaturi zasledimo še številne definicije informacijske varnostne kulture. Lete pa jo predstavljajo kot vrednoto, zaščito, stališča, predpostavke, prepričanja o karakterizaciji informacijske varnostne kulture, dojemanje in vedenje zaposlenih (Uchendu, et al., 2021).

- Dhillon (1997, cited in Uchendu, et al., 2021) jo opisuje kot celotno človeško lastnost – »*vedenja, stališča in vrednote, ki prispevajo k zaščiti vseh vrst informacij, v neki organizaciji*«, kar podpira razmišljanje, da imajo človeške lastnosti pomembno vlogo v informacijski varnostni kulturi.
- Martins in Eloff (2002) jo opisujeta kot »*predpostavko o tem, kaj je in kaj ni sprejemljivo v zvezi z informacijsko varnostjo – katero vrsto vedenja informacijske varnosti je potrebno sprejeti in spodbujati, da se značilnosti informacijske varnosti vključijo kot način dela v organizaciji*«, kar nadalje kaže na vlogo, ki jo ima vedenje zaposlenih pri varovanju podatkov.
- Alnatheer in Nelson (2009) jo opredeljujeta kot »*niz karakteristik varovanja informacij in vrednoto, ki jo razvije skupina zaposlenih*«.
- Da Veiga in Eloff (2010) jo definirata kot »*odnose, prepričanja, ravnanja, dojemanja in stališča, ponotranjena na ravni organizacije*«.
- AlHogail in Mirza (2014a) pravita, da informacijska varnostna kultura »*odraža nabor zaznav, stališč, vrednot, predpostavk in znanja*«. Vse navedeno deluje na vedenje zaposlenih, da pri interakciji z organizacijskimi in informacijskimi viri ohranjajo pravo raven informacijske varnosti.

V literaturi zasledimo definicije s posebnim poudarkom na organizacijske temelje, na katerih je potrebno graditi informacijsko varnostno kulturo. Alnatheer, et al. (2012); Nævestad, et al. (2018); Nel in Drevin (2019); Ruhwanya in Ophoff (2019); Alshaikh (2020); Da Veiga, et al. (2020) ter Wiley, et al. (2020) vključujejo organizacijsko kulturo v definicije informacijske varnostne kulture. Alnatheer, et al. (2012), Nel in Drevin (2019) ter Wiley, et al. (2020) jo opredeljujejo kot subkulturo organizacijske kulture.

- Schlienger in Teufel (2003) jo definirata kot »*organizacijsko subkulturo, katere cilj je informacijska varnost. Informacijska varnostna kultura podpira vse*

dejavnosti v tej smeri, da informacijska varnost postane praksa prav vsakega zaposlenega«.

- Mokwetli in Zuva (2018) opisujeta koncept kot medsebojno povezan s korporativnimi sistemi in postopki. Slednji jo označujejo kot »*družbeno-kulturne ukrepe, ki podpirajo tehnično-varnostne ukrepe, tako da informacijska varnost postane naravni del vsakodnevnih aktivnosti zaposlenega*«.

Nævestad, et al. (2018) navajajo, da je varnostno kulturo mogoče razumeti preprosto kot varnostne vidike širše organizacijske kulture. Oh in Han (2020) označujeta organizacijsko kulturo v identificiranju, ali so zaposleni »*pripravljeni sodelovati v dejavnostih organizacijskega učenja*«, kar potrjuje tudi ugotovitev Nela in Drevina (2019), da informacijska varnostna kultura ni le subkultura organizacijske kulture. Le-ta naj bi sčasoma postala del organizacijskih funkcij.

V literaturi nadalje zasledimo definicije kibernetske varnostne kulture, ki so podobne definicijam informacijske varnostne kulture. Definicije kibernetske varnostne kulture so običajno širšega obsega in obenem manj specifične do zaščite informacij.

- Da Veiga (2016) jo opredeljuje kot nekaj, kar »*spodbuja ali zavira varstvo, varnost, zasebnost in državljanske svoboščine posameznikov, organizacij ali vlad*«, vse to pa zajema širše področje kot samo varnost podatkov ter vključuje ohranjanje varnosti ljudi in organizacij v celoti.
- Alshaikh (2020) jo označuje kot »*kontekstualizirano na vedenje ljudi v organizaciji*« – t.j. zaščito informacij, ki jih obvladuje organizacija, s pomočjo skladnosti z informacijsko varnostno politiko (angl. *»Information Security Policy«* – v nadaljevanju ISP) in razumevanjem, kako izvajati zahteve na previden in pozoren način, z redno komunikacijo, ozaveščanjem, usposabljanjem in izobraževalnimi pobudami.
- Ioannou, et al. (2019) jo opisujejo kot »*postopke, ki jih določi organizacija za vse svoje zaposlene in le-ti usmerjajo njihov potek delovanja v vseh situacijah, povezanih s celovitostjo podatkov*«, kar se navezuje na spodbujanje izboljšanja varnostnega vedenja zaposlenih, zlasti v zvezi s podatki/informacijami.

1.2.2 Razkorak v konsenzu faktorjev in dimenzij

V literaturi ni jasnega soglasja glede dejavnikov/faktorjev in dimenzij informacijske varnostne kulture. Številne raziskave se osredotočajo predvsem na dejavnike, ki so ključni za izgradnjo dobre varnostne kulture, medtem ko jo nekatere opredeljujejo z dimenzijami.

Dejavnik, ki je najbolj poudarjen za ohranjanje dobre varnostne kulture je *podpora in vodenje s strani vrhnjega managementa*. Sledi dejavnik *posedovanja jasnih politik in postopkov*, ki jih morajo zaposleni razumeti in upoštevati. Razumevanje zaposlenih je pogosto povezano s politikami in postopki, poznavanje le-teh pa je bistveni del gradnje in vzdrževanja varnostne kulture. Med dejavnike prištevamo tudi *programe ozaveščanja o varnosti* ter *usposabljanja*, ki sta bistvena za povečanje varnostne zavesti in s tem vzdrževanja ustrezne ravni informacijske varnostne kulture (Uchendu, et al., 2021). Eden bolj izstopajočih dejavnikov pa je zagotovo dejavnik *upravljanja sprememb*. AlHogail in Mirza (2014b) npr. navajata, da se številne raziskave osredotočajo na dejavnike, ki so pomembni za varnostno kulturo, a le redke omenjajo proces prehoda v smeri izgradnje informacijske varnostne kulture v organizaciji. Nel in Drevin (2019) ter Van‘t Wout (2019) vidijo upravljanje sprememb kot ključni dejavnik spodbujanja dejanskih sprememb, ki so potrebne za izgradnjo in vzdrževanje informacijske varnostne kulture. Dejavnik *skladnosti* je skupaj z razumevanjem politik in postopkov ključni vidik za zaposlene pri zagotavljanju ohranjanja vrednot organizacije. Skladnosti lahko sledimo iz različnih zornih kotov, kot npr. proces zagotavljanja, da zaposleni in organizacija kot celota upoštevajo standarde in predpise o varnosti (Uchendu, et al., 2021). Dejavnik *zavezanosti* se na splošno nanaša na dejavnosti, ki so potrebne za zagotovitev uporabe politike in spodbujanje močne kulture (Uchendu, et al., 2021). *Zaupanje* je prav tako obravnavano kot pomemben dejavnik za izgradnjo varnostne kulture. V raziskavah se o zaupanju razpravlja na različne načine (zaupanje v dejanja in namere zaposlenih, zaščita informacij s strani človeškega vidika itd.) (Uchendu, et al., 2021). Poleg zaupanja pa *zavzetost* zaposlenih nakazuje, da lahko odnos med organizacijo, njenim vodstvom in uporabniki določa stanje varnostne kulture (Uchendu, et al., 2021). Da bi dosegli spremembo vedenja in s tem vzpostavili informacijsko varnostno kulturo, Blythe, et al.

(2020) poudarjajo potrebo po *nagradah in sankcijah* kot del kampanje ozaveščanja o informacijski varnosti. Nagrade ali sankcije se uporabljajo za premostitev vrzeli med znanjem in prakso glede informacijske varnostne ozaveščenosti.

1.2.3 Okvirji in modeli

V sistematičnem pregledu literature, za obdobje od 2010 do 2020, avtorjev Uchendu, et al. (2021), je skupaj 37 raziskav od 58 preučevalo pristope, orodja ali okvirje v zvezi s kultivacijo ali vzdrževanjem informacijske varnostne kulture. Dollah in Ali (2012), Masrek, et al. (2017) in Tolah, et al. (2019) se osredotočajo na teoretične okvirje za vodenje razvoja takšnih varnostnih kultur. Konceptualne modele informacijske varnostne kulture so razvili Hassan in Ismail (2012); Martins in Da Veiga (2015); Masrek, et al. (2018); Mokwetli in Zuva (2018) ter Sherif, et al. (2015). Mokwetli in Zuva (2018) sta razvila konceptualni model IKT ter informacijske varnostne kulture, ki je sestavljen iz treh kategorij – organizacijske, okoljske in tehnološke. Rezultati njune raziskave so pokazali, da sprejetje modela pomaga zmanjšati človeške napake v malih in srednje velikih organizacijah. Zgolj manjšina raziskav je opravljenih za področje manjših, srednje velikih in mikro organizacij (Uchendu, et al., 2021). V literaturi ni zaznati raziskav, ki bi posebej izpostavljale, ali so bili pristopi (modeli, okvirji) razviti izključno za večje organizacije. Lacey (2010) in Tang, et al. (2016) so izvajali projekte v večjih organizacijah, medtem ko so Da Veiga, et al. (2020) preučevali male, srednje in večje organizacije. Lacey (2010) navaja, da imajo celo večje organizacije pogosto nizke proračune in vire, ki jih morajo usmeriti v razvoj učinkovitih kampanj za spremembe. Na splošno pa to sproža vprašanja glede uporabnosti navedenih pristopov za organizacije različnih velikosti. Santos-Olmo, et al. (2016) pojasnjujejo, da so številni okvirji namenjeni izboljšanju informacijske varnostne kulture zasnovani za večje organizacije, zato kot taki ne vključuje dejavnikov, ki so ključni predvsem za manjše organizacije. Manjše organizacije so pogostokrat v protislovju s prej navedenimi konceptualnimi modeli. Orodja, ki so razvita za večje organizacije niso cenovno dostopna manjšim, obenem pa so celo izredno zapletena (de Araújo Lima, et al., 2020). Čeprav gre predvsem za teoretične modele, organizacijam zagotavljajo osnovo za razumevanje, kako je mogoče kultivirati in krepiti dobro varnostno kulturo.

1.2.3.1 Scheinov model organizacijske kulture

Scheinova definicija organizacijske kulture se pogosto uporablja kot vodilo pri razumevanju pojma informacijske varnostne kulture. Zato je v nadaljevanju obravnavan Scheinov model organizacijske kulture. Omenjeni model je imel pomembno vlogo pri razvoju konceptualnih okvirjev, avtorjev Van Niekerk in Von Solms (2010) ter Reid in Van Niekerk (2014). Omenjeni avtorji uporabljajo Scheinov model organizacijske kulture z vključenim nivojem znanja, ki je osnova za razumevanje strukture varnostne kulture. Smircich (1983) je v svojemu delu zapisala, da kultura, ki temelji na skupnih vrednotah in prepričanjih zaposlenih oblikuje pomembne funkcije v organizaciji, kot npr. da zaposlenim daje občutek identitete, občutek pripadnosti k nečemu večjemu, povečuje stabilnost socialnih sistemov in vodi k oblikovanju vedenja zaposlenih.

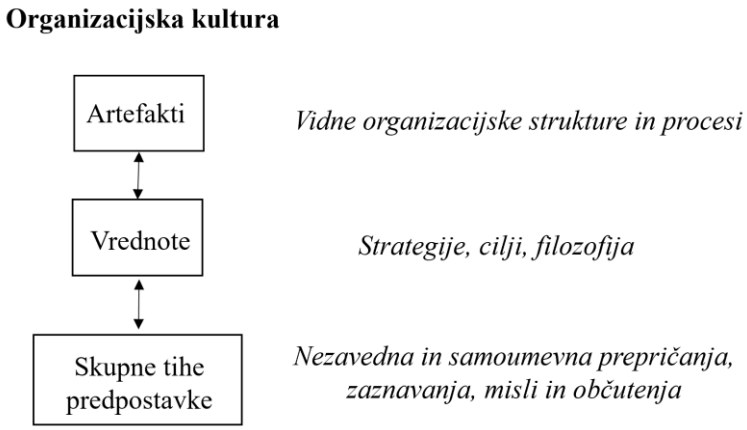
Kultura je v organizacijski literaturi opredeljena na različne načine in prav tako so različni tudi pristopi njenega preučevanja. Nekatere opredelitve sledijo instrumentalnemu pogledu in se osredotočajo na to, kako kultura oblikuje vrednote zaposlenih, njihove kognicije in vedenja v organizacijskem okolju (Smircich, 1983). Po mnenju omenjene avtorice organizacijska kultura izraža vrednote socialnih idealov in vzorce prepričanj, ki si jih zaposleni delijo med seboj v obliki mitov, ritualov, legend ali v uporabi specializiranih jezikov.

Drugi pogled na organizacijsko kulturo je osredotočen na povezavo med organizacijsko kulturo in vodenjem ter predpostavlja, da organizacijska kultura oblikuje in manipulira vrhnji management in da je le-ta lahko objektivno vodena (Smircich, 1983).

Tsui, et al. (2006) opisujejo organizacijsko kulturo kot nabor temeljnih vrednot, ki si jih soglasno delijo člani neke organizacije. Organizacijska kultura se razlikuje med organizacijami, saj ima vsaka med njimi svoj nabor značilnosti in vrednot, ki so zanjo pomembne (Robbins, 2001).

Schein in Schein (2019) pravita, da se organizacijska kultura manifestira na treh različnih ravneh – kot artefakti, vrednote in skupne tihe predpostavke (angl. »*taken-for-granted-*

assumptions«) (slika 1). *Raven artefaktov* predstavlja organizacijske strukture in procese. Gre za površinsko raven in organizacijsko kulturo lahko opazujemo npr. skozi vedenjske vzorce zaposlenih ter tako ne zagotavlja njihovega poglobljenega razumevanja. *Raven vrednot* se manifestira v viziji, poslanstvu, ciljih, strategiji, normah in filozofiji organizacije. Le-te so izražene v javnih dokumentih (Van Niekerk & Von Solms, 2010; Schein & Schein, 2019). Izobraževalni programi, usposabljanja in ozaveščanja so pogosti mehanizmi, ki jih organizacije izvajajo za ozaveščanje zaposlenih o viziji, poslanstvu in normah organizacije. Namen izobraževalnih programov je namreč organizacijsko kulturo premakniti s površinske ravni na raven vrednot z globljim dojemanjem zaposlenih (Van Niekerk & Von Solms, 2010). Najvišja raven organizacijske kulture predstavlja *skupne tihe predpostavke* – t.s. nezavedna in samoumevna prepričanja, zaznavanja, misli in občutenja, ki so globoko zakoreninjena v vsakodnevnem vedenju zaposlenih (Schein & Schein, 2019).



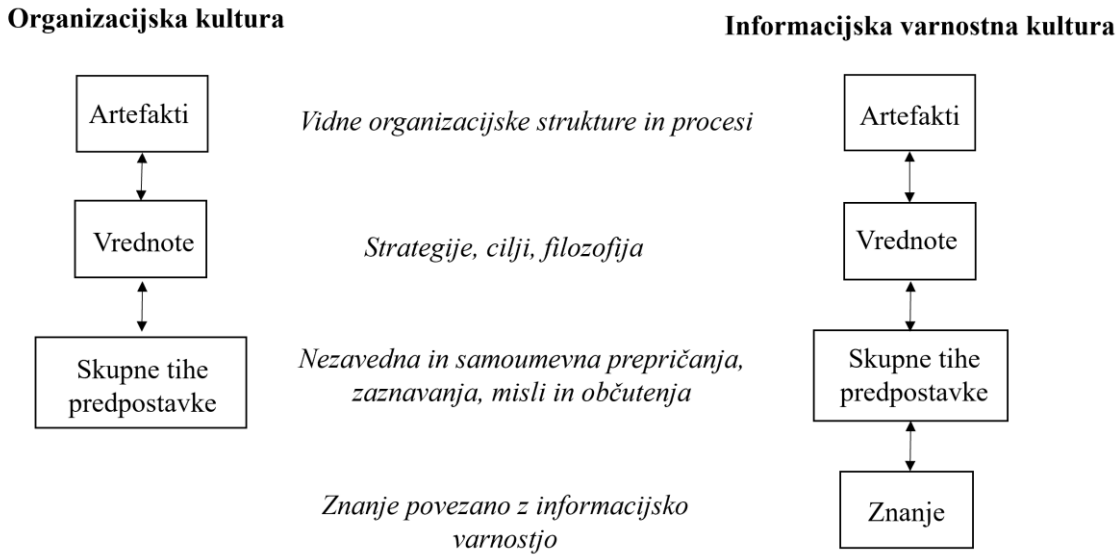
Slika 1: Tri ravni organizacijske kulture

(Schein & Schein, 2019, p. 21)

V literaturi, tako kot številne definicije organizacijske kulture, zasledimo tudi številne alternative dimenzij in okvirje, med njimi šest-dimenzionalni okvir avtorjev Hofstede, et al. (1990), pet dimenzij vrednot po Tsui, et al. (2006) in številne druge, ki sta jih v svojem delu opisala avtorja Cameron in Quinn (2011). Med vsemi navedenimi pa je najbolj poznana tipologija organizacijske kulture po Quinnu (1988), ki se je skozi leta spreminjala; njen temelj pa je ostajal nespremenjen.

1.2.3.2 Konceptualni okvir po Van Niekerku in Von Solmsu

Na podlagi Scheinovega modela organizacijske kulture Van Niekerk in Von Solms (2010) trdita, da ima informacijska varnostna kultura prav tako tri ravni – kakor organizacijska (slika 2). Vendar poudarjata, da v informacijski varnostni kulturi znanje podpira vse tri ravni organizacijske kulture in navajata, da brez ustreznega znanja ni mogoče zagotoviti informacijske varnosti. Soodvisnost med tremi organizacijskimi ravnmi kulture in četrto ravnjo – t.j. znanjem narekuje, kakšna bo informacijska varnost oz. informacijska varnostna kultura v organizaciji.



Slika 2: Van Niekerkov in Von Solmsov okvir informacijske varnostne kulture
(Van Niekerk & Von Solms, 2010)

Na *ravni artefaktov* je informacijsko varnostno kulturo moč opazovati skozi varnostne mehanizme, kot so npr.: zaklenjeni prostori, kjer se nahajajo računalniki, video nadzorni sistemi in avtentifikacijski mehanizmi, ter dokumenti, ki zadevajo varnostno politiko. Artefakti vključujejo predvsem fizične in tehnične nadzorne mehanizme (Chen, et al., 2015). Posamezniki se nanje običajno odzovejo s svojim zaznavanjem in prepričanjem o artefaktu samemu. Takšna zaznavanja in prepričanja se oblikujejo na podlagi njihovih

preteklih izkušenj s podobnim artefaktom ali s pomočjo organizacijske propagande, kot so izobraževalni programi (Srite & Karahanna, 2006).

Raven vrednot lahko opazujemo skozi varnostno politiko organizacije, varnostno izobraževanje, usposabljanje in ozaveščanje ter nadzore varnosti. Varnostna politika jasno opredeljuje vizijo, poslanstvo, norme in mišljenja v zvezi z informacijsko varnostjo. Le-te pa gradijo temelje za ustvarjanje skupnih vrednot in predpostavk na področju informacijske varnosti. Varnostno izobraževanje, usposabljanje in ozaveščanje so mehanizmi, s katerimi organizacija zagotavlja ozaveščenost zaposlenih o vrednotah in prepričanjih, ki jih vsebuje varnostna politika (Chen, et al., 2015).

Skupne tihe predpostavke so skupne misli in dojemanja o varnosti. Le-te pa so skladne z varnostnimi vrednotami in prepričanji v organizaciji in postanejo močna sila, ki vodi vedenja zaposlenih (Chen, et al., 2015).

Visoka raven informacijske varnostne kulture in skupne tihe predpostavke se ne oblikujejo v kratkem času. Gre za učni proces med organizacijo in zaposlenimi (Van Niekerk, & Von Solms, 2010).

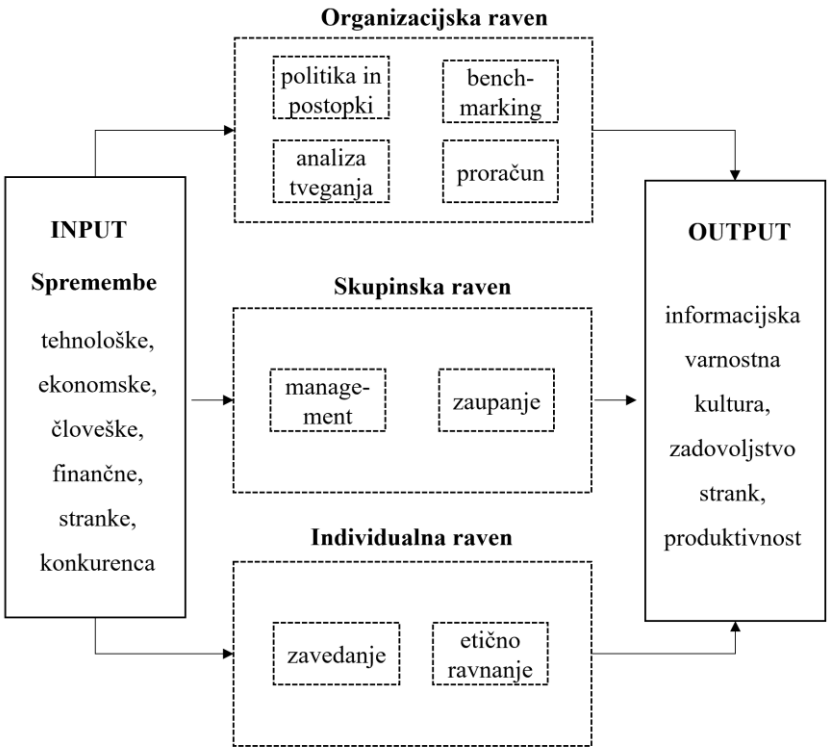
1.2.3.3 Model informacijske varnostne kulture po Martinsu in Eloffu

Martins in Eloff (2002) trdita, da je kultura povezana z načinom dela v organizaciji in ta z vedenjem zaposlenih. Zato ima vedenje zaposlenih v organizaciji učinek na informacijsko varnostno kulturo organizacije. V kolikor organizacija želi približati zaposlenim sprejemljivo vedenje, je slednje potrebno opazovati s treh različnih ravni – individualne, skupinske in organizacijske (Kreitner & Kinicki, 1995; Robbins, 2001).

Dobra primera nesprejemljivega vedenja sta metanje dokumentov v smeti in puščanje pomembnih podatkov v pisarni brez nadzora. Napram teh vedenj je potrebno stremeti k uporabi uničevalca dokumentov in zaklepanju pisarn. Informacijska varnostna kultura nastaja pri spodbujanju sprejemljivega informacijskega varnostnega vedenja. Primer je organizacija, ki zaposlene spodbuja, da po ustreznih kanalih poročajo o varnostnih

incidentih in ima vpeljano spodbujanje zaposlenih s strani vrhnjega managementa, da aktivnosti, ki jih opravljajo pri izvajanju svojega dela obravnavajo kot del organizacijske intelektualne lastnine, to pa je potrebno zaščititi (Martins & Eloff, 2002). Martins in Eloff (2002) predlagata, da organizacije pri vzpostavitvi informacijske varnostne kulture uporabijo model, ki ga prikazuje Slika 3 in svetujeta, da je potrebno določiti, na kateri ravni je informacijska varnostna kultura prisotna. Na ta način organizacija uvidi, kam usmeriti pozornost pri vzpostavitvi ali izboljševanju informacijske varnostne kulture. Posebno pozornost pa je potrebno nameniti zaposlenim. Vpeljava informacijske varnostne kulture ni lahka naloga in lahko traja več let (Gaunt, 2000).

Slika 3 prikazuje tri ravni modela informacijske varnostne kulture. Vsaka od njih predstavlja nabor različnih vprašanj, ki jih je potrebno obravnavati v zvezi s promocijo kulture, ki spodbuja zaščito informacijskih virov.



Slika 3: Model informacijske varnostne kulture po Martinsu in Eloffu

(Martins & Eloff, 2002)

Za primer vzemimo aktivnosti konkurence, ki zadeva vprašanja vseh treh ravni. Vse več organizacij strmi k uporabi ISO standarda (angl. *»International Organization for Standardization«* – v nadaljevanju ISO). Uporabljajo ga tako konkurenti kot potrošniki. Njegova uvedba deluje na organizacijsko raven, saj se pojavi potreba po pregledu ISP, kar vodi v finančni načrt. Management mora v tem primeru zagotoviti podporo za izvajanje novih procesov, z zagotavljanjem potrebnih sredstev in vzpostavitve ustreznih, predpisanih postopkov. Obenem se morajo zaposleni udeležiti izobraževanj in programov ozaveščanj, ki jim bodo omogočili izvajanje procesa. Prisotnost zaposlenih na takšnih programih deluje na njihovo vedenje glede varovanja informacijskih virov v organizaciji. Informacijska varnostna kultura je prisotna tam, kjer se spodbuja specifično vedenje, in to je skladnost s standardom. V opisanem primeru so uporabniki storitev zaupljivejši in samozavestnejši pri sodelovanju z organizacijo, saj vedo, da so informacijski viri organizacije ustrezno zavarovani.

Organizacijska raven:

- Politika in postopki

  ISP narekuje, kakšno mora biti vedenje zaposlenih in kaj se od njih pričakuje. Takšno vedenje sčasoma postane del informacijske varnostne kulture. Da se zaposleni vedejo s pričakovanji, se morajo v tej smeri tudi izobraževati, usposobiti in razviti zavedanje.
- Primerjalna analiza (angl. »*Benchmarking*«)

  Primerjanje smernic, ki zadevajo informacijsko varnost in procese, kot so ozaveščanje, usposabljanje in razporejanje sredstev, organizaciji omogoča, da se postavi ob ramo z drugimi podobnimi organizacijami in mednarodnimi standardi. Primerjanje zagotavlja vodila za interakcijo zaposlenih z informacijskimi viri in vodila za ustrezna vedenja in s tem zagotavljanje varnost informacij, kar pomaga kultivirati informacijsko varnostno kulturo.
- Analiza tveganja

  Z analizo tveganja je mogoče prepoznati nevarnosti, ki pretijo organizacijskim virom in varnostne ukrepe za razvoj ISP. Analiza tveganja organizaciji omogoča razvoj informacijske varnostne kulture, ki se med organizacijami razlikuje. Dober primer je zdravstvena organizacija. V tej organizaciji bodo vprašanja glede

zasebnosti in zaščite podatkov pacientov veliko bolj pomembna kot v primerjavi z evidenco strank v trgovinah. Da bi zaposleni analizo tveganja v organizaciji dojemali kot del informacijske varnostne kulture, jo morajo dojemati kot utečeno aktivnost in del vsakodnevnega življenja v organizaciji.

- Proračun

  Za implementacijo zadev, ki obravnavajo vprašanja informacijske varnostne kulture je potreben finančni načrt – npr.: zaposleni se morajo udeležiti usposabljanj, vpeljati je potrebno tehnični nadzor, ustanoviti je potrebno delovne skupine za oceno varnosti omrežij itd. Poraba sredstev za izvajanje ISP mora biti sprejeta kot ustaljena vsakodnevna aktivnost.

Skupinska raven:

- Management

  Za informacijsko varnost je odgovorno vodstvo, saj razvije vizijo in strategijo organizacije, ki je potrebna za zaščito informacijskih virov. Vedenje zaposlenih do zaščite informacijskih virov je vodeno s filozofijo in strategijo organizacije. Vodstvo mora strmeti k sprejemljivemu vedenju zaposlenih in da ta postane način dela. Sčasoma se razvije kultura, ki odraža vizijo, strategijo ter izkušnje zaposlenih, ki so jih pridobili ob njenem izvajanju.

- Zaupanje

  Informacijska varnost je najpomembnejše vprašanje, ki vzbuja zaupanje v okolju IKT. Če vodstvo zaupa svojim zaposlenim in obratno, je lažje vpeljati nove postopke in voditi zaposlene skozi spremembe informacijsko varnostnega vedenja. Zaupanje mora biti pozitivno in eno od značilnosti organizacije, ki bo pripomogla h kultivaciji informacijske varnostne kulture.

Individualna raven:

- Zavedanje

  Zaposleni v organizaciji imajo lahko različen odnos, in ta ima za posledico določeno vedenje. Zaposleni se morajo zavedati opredeljenih procesov na ravni organizacije, da bi se lahko primerno oz. ustrezno vedli. Od njihovega vedenja je odvisen uspeh na organizacijski in skupinski ravni. V kolikor zaposlene ne vodijo

vprašanja, ki zadevajo ozaveščenost, ne bodo mogli ustrezno ukrepati, četudi so to pripravljeni storiti na individualni ravni. Ker je učinkovitost nadzora informacijske varnosti odvisna od zaposlenih, ki ta nadzor izvajajo, je za zagotovitev varnosti informacijskih virov potrebno zaposlene ozavestiti in usposobiti, da se vedejo v skladu s pričakovanji.

- Etično ravnanje
  Organizacija dobre prakse ne pridobi le s predpisi, spodbujanjem in spremljanjem. Navedene zahteve morajo biti del kulture v organizaciji že prej. Zaposleni morajo etična vedenja, ki se dotikajo informacijske varnosti vključiti v svoj vsakdan.

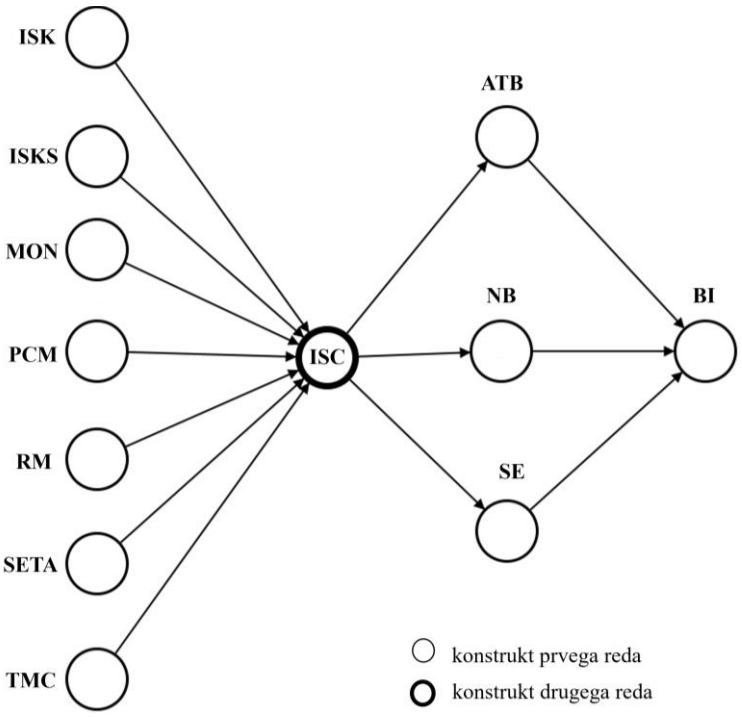
Vložek: Spremembe na področju informacijske varnosti morajo biti sprejete v pozitivni luči in uvedene tako, da jih zaposleni lahko vključujejo v svoje delovno okolje. Sprejete spremembe sčasoma postanejo del informacijske varnostne kulture.

1.2.3.4 Model dimenzij informacijske varnostne kulture po Nasirju in sodelavcih

Nasir, et al. (2019a) so v svojem delu predlagali model informacijske varnostne kulture, ki temelji na sedmih dimenzijah (slika 4) in so bile oblikovane na podlagi splošno sprejetih konceptov organizacijske (Schein & Schein, 2019) in informacijske varnostne kulture. Omenjeni avtorji so preučevali povezanost dimenzij informacijske varnostne kulture s konstrukti Teorije načrtovanega vedenja (Fishbein & Ajzen, 2011) za področje visokošolskih ustanov v Maleziji. Model temelji na univerzalnem konceptu organizacijske kulture in, kot navajajo, ga je možno aplicirati na različne organizacije (šolstvo, zdravstvo, vojska) in druge države. Informacijska varnostna kultura je zasnovana kot konstrukt drugega reda (angl. »*second order construct*«*)* in je definirana s sedmimi dimenzijami, konstrukti prvega reda (angl. »*first order construct*«):

- postopkovni protiukrepi (angl. »*Procedural Countermeasures*« – v nadaljevanju PCM),
- obvladovanje tveganj (angl. »*Risk Management*« – v nadaljevanju RM),
- varnostno izobraževanje, usposabljanje in ozaveščanje (angl. »*Security Education, Training and Awareness*« – v nadaljevanju SETA),

- zavezanost vrhnjega managementa (angl. »*Top Management Commitment*« – v nadaljevanju TMC),
- nadzorovanje/spremljanje varnosti (angl. »*Security Monitoring*« – v nadaljevanju MON),
- znanje o informacijski varnosti (angl. »*Information Security Knowledge*« – v nadaljevanju ISK),
- izmenjava znanja o informacijski varnosti (angl. »*Information Security Knowledge Sharing*« – v nadaljevanju ISKS).



Legenda:
SE – samoučinkovitost (angl. »*Self-Efficacy*«)
ISC – informacijska varnostna kultura (angl. »*Information Security Culture*«)

Slika 4: Model dimenzij informacijske varnostne kulture po Nasirju in sodelavcih (Nasir, et al., 2019a)

Znanje o informacijski varnosti

Znanje zaposlenih o informacijski varnosti, pridobljeno skozi življenje in skozi izobraževalne programe ozaveščanja in usposabljanja, deluje pozitivno na razvoj informacijske varnostne kulture v organizaciji. Vsak zaposleni poseduje znanje in

razumevanje ISP in kontrol, ki vplivajo na to, kako obdelujejo organizacijske informacije (Da Veiga, et al., 2020). Strokovnost na področju informacijske varnosti nakazuje na večjo zmogljivost pri odkrivanju kršitev. Od izkušenih posameznikov se pričakuje, da bodo sprejemali boljše odločitve. Pričakuje se, da izkušen posameznik zaznava napačne vzorce, ki jih recimo novinec ne bi. Znanje in pretekle izkušnje naredijo posameznike občutljivejše za namige, ki jih lahko novinec spregleda. Kot pišeta Ben-Asher in Gonzalez (2015), je takšno znanje specifično in se gradi z izkušnjami in intenzivno prakso. Strokovno znanje je lahko omejeno in odvisno od konteksta delovanja posameznika. Posameznika lahko naredi togega ter povzroči težave pri prilagajanju v dinamičnih okoljih. Poleg tega pa odvisnost od poznavanja le enega področja delovanja in zanemarjanje splošnih veščin in hevristike škoduje sposobnosti posameznikov. *Domensko znanje* ali *temeljno znanje* je pridobljeno s kontinuiranim pridobivanjem znanja. Vključuje teoretično znanje, ki ga posameznik pridobi s formalnim izobraževanjem, usposabljanjem ali certificiranjem. Domensko znanje vključuje tudi praktično znanje, pridobljeno s prakso in izkušnjami, metodami delovanja in potekom dela (Chi, 2006). Vendar domensko znanje vedno ni dovolj za odkrivanje in preprečevanje kršitev informacijske varnosti v operativnih okoljih. Poleg domenskega znanja je potrebno tudi situirano znanje (Goodall, et al., 2009). *Situirano znanje* je implicitno, težko ga je artikulirati in je odvisno od organizacije. Ta tip znanja je dinamičen in posameznik ga pridobi z nenehnimi interakcijami s specifičnim delovnim okoljem (Ben-Asher & Gonzalez, 2015).

Izmenjava znanja o informacijski varnosti

V kontekstih informacijske varnosti se lahko ustvarjanje znanja manifestira z zaposlitvijo strokovnjakov za informacijsko varnost, ki prenašajo znanje o informacijski varnosti na zaposlene. Organizacije lahko zaposlujejo posebne enote, ki so odgovorne za te dejavnosti (Flores, et al., 2014). Posamezniki, ki so sposobni učinkovito rokovati z novimi izkušnjami in informacijami ter jih uporabiti v različnih scenarijih, so pogosto opisani kot »posamezniki z znanjem«. Posameznikovo znanje, podatki in informacije skupaj opredeljujejo organizacijsko znanje. V kolikor so »posamezniki z znanjem« pravilno razdeljeni med druge člane organizacije, so le-ti dragocena dobrina, ki jo je moč

uporabiti za pomoč pri odločanju, izboljšanju učinkovitosti, zmanjševanju stroškov usposabljanja in zmanjšanju tveganj zaradi negotovosti (Pai, 2006). Izmenjava znanja je lahko eksplicitna ali tacitna (tiho znanje). Pri *eksplicitni* izmenjavi znanja gre za izmenjavo znanja, ki ga je mogoče artikulirati z besedami, kodirati in prenesti prek smernic, dokumentov in videov z navodili. *Tiho* znanje (uporaba neformalno pridobljenega znanja v vsakdanjih situacijah) je težje prenesti, saj se nahaja v glavah posameznikov in ni kodificirano v strukturirani obliki. Učinkoviti mehanizmi za izmenjavo znanja pomagajo posameznikom, da delijo svoje implicitno in tacitno znanje (Pai, 2006). Znanje se prenaša, ko ljudje komunicirajo drug z drugim z izmenjavo izkušenj ali medsebojno pomočjo.

Varnostno izobraževanje, usposabljanje in ozaveščanje

SETA programi se vpeljujejo ob uvajanju varnostnih politik, s pomočjo katerih organizacije nadalje razvijajo vrsto smernic in postopkov v zvezi s procesom preprečevanja, odkrivanja in izboljšanja upravljanja informacijske varnosti (Straub & Welke, 1998; Wilson & Hash, 2003; Chen, et al, 2015). SETA programi so glavno sredstvo za ustvarjanje in zagotavljanje ustrezne ravni ozaveščenosti o varnostnih politikah. Njihov namen je zagotavljanje ustreznega interpretiranja in razumevanja vsebine varnostnih politik (Chen, et al., 2015). Da bi se lahko spremenila miselnost zaposlenih glede varnosti, morajo biti takšni programi kontinuirani in ne le občasni (Chen, et al., 2015). Celoviti programi informacijske varnosti poskušajo spremeniti vedenje zaposlenih v smeri informacijske varnosti in jim ohranjati svežino v mišljenju med opravljanjem vsakodnevnega dela. Celovite izobraževalne programe sestavljajo (Chen, et al., 2015): poznavanje varnostne politike; SETA programi in nadzor oz. spremljanje varnosti. Za reševanje vprašanj skladnosti z varnostnimi politikami se SETA programi uporabljajo za povečanje ozaveščenosti zaposlenih o varnostnih politikah, izboljšanje varnostnih veščin in znanja v zvezi z vsakdanjimi delovnimi mesti zaposlenih, obveščanje o odgovornosti in vlogi zaposlenih pri informacijski varnosti v organizaciji ter zagotavljanje zavedanja sankcij in ukrepov proti kršitvam varnostnih politik (Wilson & Hash, 2003). SETA programi zagotavljajo, da zaposleni razumejo odgovornost za svoje vedenje do informacijske varnosti. Programi so lahko v različnih oblikah in se

izvajajo na različnih ravneh (Wilson & Hash, 2003). Lahko so usmerjeni na različne organizacijske ravni, od vodstva do na novo zaposlenih. Prav tako lahko zagotavljajo različne stopnje varnostnega usposabljanja, od splošnega zavedanja o informacijski varnosti ter pismenosti do poklicnega razvoja. Izobraževalni materiali so plakati, ohranjevalniki zaslona, video delavnice itd. Ne glede na oblike in ravni, ki jih taki programi zajemajo, si vsi od naštetih prizadevajo ustvariti močan občutek informacijske varnosti med zaposlenimi, na takšen način, da informacijska varnost postane naraven, neločljiv vidik njihovega vsakodnevnega dela (Whitman, 2003). Visoka raven ozaveščenosti o takšnih programih je močan pokazatelj njihove uspešnosti (D'Arcy, et al., 2009). S kampanjami sankcij in ukrepov proti kršitvam ISP SETA programi vplivajo na dojemanje zaposlenih o kršitvah (D'Arcy, et al., 2009).

Postopkovni protiukrepi

Varnostna politika je notranja »ureditev« in »pravilo«, ki služi za spodbujanje želenih vedenj zaposlenih do informacijske varnosti (Whitman 2003; D'Arcy, et al., 2009). Predstavlja tudi stališča do informacijske varnosti ter posledice kršitev pravil (Thomson, et al., 2006; Chen, et al., 2012). Zavedanje prisotnosti varnostnih politik oblikuje pri zaposlenih globje misli in dojemanje, kar spodbuja zaposlene, da ponotranjijo organizacijsko kulturo za področje varnosti (Chen, et al., 2015). Vzpostavitev formalne varnostne politike je zato prvi korak k oblikovanju informacijske varnostne kulture v organizaciji in velja za najboljšo prakso na področju upravljanja informacijske varnosti v skladu s predpisi in standardi, kot je npr. ISO standard.

Nadzorovanje/spremljanje varnosti

Varnostno spremljanje kot »odvračilni« mehanizem lahko zmanjša zlorabo IS in pojav vedenj, ki bi lahko bila sankcionirana (Straub & Welke, 1998; D'Arcy, et al., 2009) in obenem zagotavlja pregled ter povratne informacije SETA programov, ki so namenjeni nenehnemu izboljševanju in napredovanju (Wilson & Hash, 2003). Spremljanje varnosti z zbiranjem dokazov o skladnosti ali kršitvi varnostnih politik razkriva tiste skupne in napačno razumljene ali prezrte vrednote in predpostavke v zvezi z varnostjo ter uveljavlja

potrebne postopke za odpravo le-teh. Izrekanje kazni ob kršitvah ali nagrajevanju za skladnost vodi k spoštovanju moralnih standardov in vrednot oz. norm varnosti (Chen, et al., 2015). Zavedanje zaposlenih o prisotnosti spremljanja varnosti spreminja dojemanje zaposlenih o varnostnih politikah v smislu sankcij in zaposlenim prikaže, da so varnostne vrednote v organizaciji pomembna sila (D'Arcy, et al., 2009).

Obvladovanje tveganj

Na informacijsko varnostno kulturo je mogoče delovati tako, da organizacija identificira, preprečuje, zazna in se odziva na incidente informacijske varnosti. Sistem preprečevanja tveganj informacijske varnosti, praksa preverjanja zaposlenih ob zaposlitvi in spremljanje njihovega delovanja zmanjšuje kadrovska tveganja in povečuje verjetnost uspešnega razvoja informacijske varnostne kulture (Da Veiga, et al., 2020). Z ustreznim obvladovanjem tveganj je mogoče doseči ravnotežje med potencialnimi tveganji in sprejemljivimi tveganji (Stango, et al., 2009). Procesi obvladovanja tveganj morajo biti merljivi, ponovljivi in revizijski, moč pa jih je tudi modelirati (Jones, 2007). Obvladovanje tveganj obsega štiri procese: okvir za obvladovanje tveganj, ocenjevanje tveganja, odziv na tveganje in spremljanje tveganja (Shameli-Sendi, et al., 2016). *Okvir za obvladovanje tveganj* je prvi proces v pristopu obvladovanja tveganja informacijske varnosti in zadeva, kako organizacija gleda na tveganja, s katerimi se sooča. Glavni rezultat tega procesa je strategija obvladovanja tveganja, ki začrta meje obvladovanja tveganja znotraj organizacije (Shameli-Sendi, et al., 2016). *Ocena tveganja* je sestavljena iz analize in ovrednotenja tveganja. Zagotavlja sistematičen način, da organizacija pridobi celovit pogled na obstoječa tveganja za informacijsko varnost in posledice ter protiukrepe za spopadanje z njimi (Saleh, et al., 2011). Ker proces ocenjevanja vključuje tveganja, povezana z vsemi vrstami platform, operacijskimi sistemi, aplikacijskimi programi, omrežji, ljudmi in procesi ter medsebojnimi odvisnostmi med njimi, je to zahteven proces in v večini primerov organizacije potrebujejo zunanjo pomoč za njeno pravilno izvajanje (Jones, 2007). Pri tem je potrebno upoštevati, da so napake pri oceni tveganja lahko nevarne in drage. Podcenjevanje tveganj lahko naredi organizacijo ranljivo za resne grožnje, medtem ko se lahko s precenjevanjem teh tveganj umaknejo nekatere uporabne IKT (Huang, et al., 2010). *Odziv na tveganje* – na tveganja informacijske varnosti, ki so

nad mejo sprejemljivega tveganja, se je treba odzvati z obravnavo tveganja, in sicer z izogibanjem tveganju, prenosom ali z ublažitvijo (zmanjšanjem). Kot odziv na vsako nesprejemljivo tveganje, ki se mu ni mogoče izogniti ali ga prenesti, je potrebno uvesti ustrezno varovalo (zmanjšanje tveganja) (Jones, 2007). Zaščita informacijske varnosti (nadzor ali protiukrep) je postopkovna ali tehnična dejavnost, ki se uporablja za zmanjšanje tveganja organizacijskih virov, s čimer se minimizira morebitna izguba zaščite. Zaščitni ukrepi lahko vključujejo preventivne, detektivne ali korektivne ukrepe (Landoll, 2011). Cilj obvladovanja tveganja informacijske varnosti je nenehno merjenje in ohranjanje sprejemljive stopnje tveganja (Landoll, 2011). *Spremljanje tveganja* – stalni nadzor igra pomembno vlogo na področju informacijske varnosti. Za vsak standard, metodologijo ali model informacijske varnosti obstaja neke vrste spremljanje ali ocenjevanje, ki ga je potrebno redno izvajati, njegove rezultate pa dokumentirati. V tej fazi je mogoče zagotoviti učinkovitost procesa obvladovanja tveganja, kot tudi usklajenost načrtovanih odzivov na tveganja s poslanstvom organizacije, vladnimi predpisi, politikami, standardi in smernicami (Shameli-Sendi, et al., 2016).

Zaveza vrhnjega managementa

Von Solms in Von Solms (2004) sta med prvimi, ki sta identificirala vrhnji management kot enega izmed kritičnih elementov informacijske varnosti. Mehanizmi, s katerimi lahko vrhnji management oblikuje odnos, prepričanja in norme zaposlenih so naslednji:

- *Mehanizem legitimnosti*

  S podpiranjem novih pobud, programov ali politik, z artikulacijo jasne vizije in strategije ter določanjem ciljev in njihovih ukrepov, jim vrhnji management daje legitimnost. Legitimnost, povezana z informacijsko varnostjo, je še posebej pomembna, ker se takšne pobude, programi in politike pogosto obravnavajo kot »dodatno delo« ali celo breme znotraj delovnega procesa (Hu, et al., 2012).
- *Mehanizem zavzetosti*

  Sodelovanje vrhnjega managementa izraža zavzetost k zastavljenim ciljem. Če se zavzetost dojema kot »zaslužna«, se bodo zaposleni odzvali z zaupanjem v vodstvo in sprejemanjem odločitev v skladu z zagovarjanjem novih programov in politik (James, 2000). Vrhnji management mora vztrajati z uresničevanjem ciljev

in pozvati vodje z nižjih ravni in zaposlene k odgovornosti za neustrezna in tvegana delovanja. Sodelovanje vrhnjega managementa pomaga pri reševanju konfliktov med različnimi deležniki in dodeljevanju sredstev ter ustvarja organizacijske strukture in vloge, ki olajšajo izvajanje novih programov in politik, ki bi sicer lahko »iztirile« zaradi drugačnih pogledov med enotami in bojev za oblast (Smith, et al., 2010). Ta mehanizem je učinkovit v primeru motiviranja zaposlenih, da se zavežejo k zaželenim oz. skladnim vedenjem, tako, da se udeležijo usposabljanj in na ta način pridobijo ustrezne veščine (Hu, et al., 2012).

- *Mehanizem poštenosti in pravičnosti*

  Zaposleni doživljajo pravila kot legitimna, logična in utemeljena takrat, ko so prepričani, da organizacija, v kateri delajo izvršuje avtoriteto po poštenih postopkih. Ta učinek pravičnosti in poštenosti je vsesplošen in nakazuje, da postopkovna pravičnost in poštenost spodbujata legitimnost, predanost in upoštevanje pravil (Tyler, et al., 2007). Organizacijsko okolje, za katerega so značilni pošteni procesi, izzove močno organizacijsko identifikacijo zaposlenih ter želeno vedenje na delovnem mestu. Sodelovanje vrhnjega managementa v pobudah, programih in politikah omogoča zaposlenim, da izrazijo svoja mnenja, sodelujejo pri evalvacijah, nadzorujejo delovanje pristranosti in sodelujejo pri načrtovanju sistema vodenja, kjer bi se lahko pojavili pomisleki v zaznavanju poštenosti in pravičnosti postopkov (Tyler, et al., 2007).

1.2.3.5 Ostali modeli informacijske varnostne kulture

Konceptualni okvir Masreka, et al. (2017) gradijo dimenzije, ki jih je mogoče porazdeliti na dejavnike, ki imajo učinek na kulturo. Kulturo model porazdeljuje na šest razsežnosti: podporo managementa, politiko in postopke, skladnost, ozaveščenost, proračun in tehnologijo.

Bakryov (2004) okvir STOPE (angl. »*Strategy, Technology, Organization, People, and Environment*« – v nadaljevanju STOPE) je uporabljen v številnih raziskavah kot temelj usmeritve razvoja varnostne kulture.

AlHogail (2015a) je združil okvir Informacijske varnostne kulture (AlHogail, 2015b) z okvirjem STOPE, da bi lahko ustvaril nov pristop k razumevanju fenomena. Namen kombiniranega modela je pokrivanje štirih področij dejavnikov človeškega vedenja – pripravljenost, odgovornost, upravljanje ter družba in predpisi. Model vključuje tudi načela upravljanja sprememb za spodbujanje in podporo potrebnih sprememb v organizacijah (Alhogail & Mirza, 2014a).

Poznani so procesi in modeli upravljanja sprememb avtorjev Reid, et al. (2014); Da Veiga (2018); ter Van‘t Wout (2019). Upravljanje sprememb se nanaša na prepričevanje zaposlenih, da spremenijo svoje vedenje v smeri zahtev organizacije (Van‘t Wout, 2019).

Da Veiga in Eloff (2010) sta razvila *Security culture cultivation framework*. Avtorja trdita, da komponente informacijske varnosti (varnostna politika, upravljanje varnostnih programov, izobraževanje in usposabljanje, spremljanje/nadzorovanje varnosti) lahko delujejo na varnostno vedenje, in to na vseh treh ravneh (organizacijski, skupinski in individualni). Varnostno vedenje pa kultivira informacijsko varnostno kulturo.

Model ISCCM (angl. »*Information Security Culture Change Management*« – ISCCM) avtorja Da Veiga (2018) raziskuje holistični pristop k upravljanju sprememb informacijske varnostne kulture. Njegov namen je teženje organizacij k pozitivni varnostni kulturi z obvladovanjem tveganj, ki jih predstavljajo človeški dejavniki pri varovanju informacij. Sestavljajo ga štiri faze za upravljanje in izvajanje sprememb vedenja.

Okvir sprememb informacijske varnostne kultur*e* (angl. »*Information Security Culture Change Framework*«) avtorjev Alhogail in Mirza (2014a) se osredotoča na kultivacijo fenomena s pomočjo spreminjanja vedenja z vključevanjem načel upravljanja sprememb in preučevanjem človeških elementov.

ARCS okvir (angl. »*Assessment of information security risk, Reduction of information security cost and sustainability of information Security Culture*«) avtorjev Govender, et al. (2020) predlaga, da razumevanje, upravljanje, podpora in spreminjanje informacijske

varnostne kulture temeljijo na razumevanju trenutnega stanja informacijske varnosti, vlaganju v posebne pobude, katere hkrati zmanjšujejo stroške in tveganje za informacijsko varnost, ter ustvarjanju trajnostnega pristopa k upravljanju in izboljševanju informacijske varnostne kulture. Okvir vsebuje nabor vprašanj o kakovosti in učinkovitosti stanja ocen informacijske varnosti, zmanjševanju stroškov in kulturi znotraj organizacije.

1.2.4 Merjenje informacijske varnostne kulture

Večina raziskav za merjenje informacijske varnostne kulture uporablja vprašalnike; nekateri od njih so predstavljeni v nadaljevanju.

Da Veiga in Eloff (2010) sta razvila Instrument za oceno informacijske varnostne kulture (angl. »*Information Security Culture Assessment*« – v nadaljevanju ISCA), ki je namenjen tako oceni kot tudi spremljanju informacijske varnostne kulture znotraj organizacije. Gre za instrument, ki je zgrajen na Okviru informacijske varnostne kulture (angl. »*Information Security Culture Framework*«), ki ga sestavlja sedem kategorij: vodenje in upravljanje, varnostno upravljanje in delovanje, varnostna politika, upravljanje varnostnih programov, upravljanje varnosti uporabnikov, zaščita tehnologije in njena uporaba. Instrument sestavlja 85 elementov, merjenih na 5-stopenjski Likertovi lestvici, ki se nanašajo na ozaveščenost in dojemanje glede zaščite informacij.

Martins in Da Veiga (2015) sta prav tako uporabila ISCA, pri čemer sta se oprla na elemente vprašalnika, ki so se osredotočali na človeške vidike informacijske varnostne kulture. Ocenjevanje se osredotoča na razumevanje znanja, vedenja in stališč zaposlenih, ki naj bi oblikovala varnostno kulturo.

Eden od instrumentov, ki ga predlaga Da Veiga (2016), je Raziskovalna metodologija kibernetske varnostne kulture (angl. »*Cyber security Culture Research Methodology*« – CseCRM). Gre za orodje za merjenje kibernetske varnostne kulture in razumevanje stopnje tveganja zaradi človeških vidikov. Instrument sestavlja 11 dimenzij, ki med drugim vključujejo spremembe, dojemanje zasebnosti, upravljanje uporabnikov ter

kibernetsko varnost v praksi. Elementi vprašalnika so merjeni na 5-stopenjski Likertovi lestvici.

Za ocenjevanje varnostne kulture so bila uporabljena tudi druga orodja, npr. kratki testi, ki so bili razviti za male in srednje velike organizacije, z namenom kultivirati in vzdrževati pozitivno varnostno kulturo, ne da bi s tem povzročili visoke stroške vzdrževanja. Raziskovalci Santos-Olmo, et al. (2016) so uporabili postopek testiranja, ki je vključeval vprašanja, povezana z varnostjo. Uporabnik je moral pravilno odgovoriti na več kot 50 % vprašanj, da je bila raven znanja ocenjena kot ustrezna. Vendar 50-% prag sam po sebi velja kot potencialno sporen pristop k presoji.

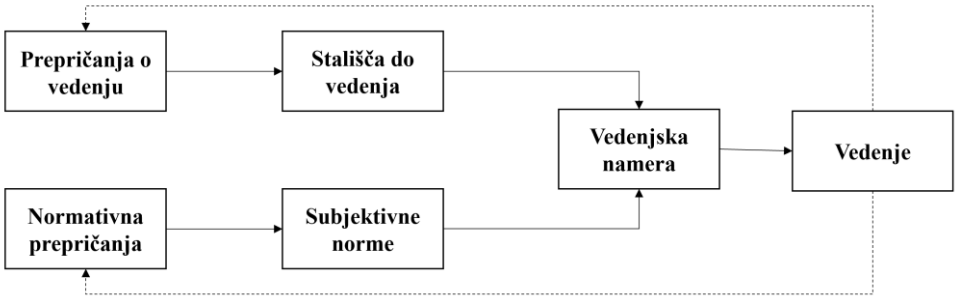
Za oceno informacijske varnostne kulture se uporabljajo tudi usposabljanja v kombinaciji z anketami. Olivos (2012) je za ocenjevanje znanja uporabila vprašalnik, s katerim je preučila učni stil posameznikov, da bi kasneje na delavnicah lahko zagotovila značilnosti vseh učnih tipov. Delavnice so vključevale izpolnjevanje predhodnega testa, predavanja in opravljanje naknadnega testa (preverjanje znanja). Tako so na primer na začetku delavnic zabeležili nekaj posameznikov, ki so svoja gesla posojali drugim sodelavcem.

1.2.5 Teorija razumne akcije in Teorija načrtovanega vedenja

»Želeno vedenje je tisto, ki je v posamezniku ponotranjeno –
voznik sledi prometnim znakom in pravilom, da lahko
varno in učinkovito doseže svoj cilj.« (Hu, et al., 2012)

Osnova raziskavam so teorije različnih znanstvenih področij (Omidosu & Ophoff, 2016). V veliki meri sta uporabljeni t. i. socio-psihološki teoriji – Teorija razumne akcije (angl. »*Theory of Reasoned Action*«, v nadaljevanju TRA) (Fishbein & Ajzen, 1975) in Teorija načrtovanega vedenja (angl. »*Theory of Planned Behavior*« – v nadaljevanju TPB) (Ajzen, 1991). Temeljna predpostavka TRA in TPB, katerih izhodišče je posameznik je ta, da je vedenjska namera tista, ki neposredno napoveduje kakšno bo vedenje posameznika.

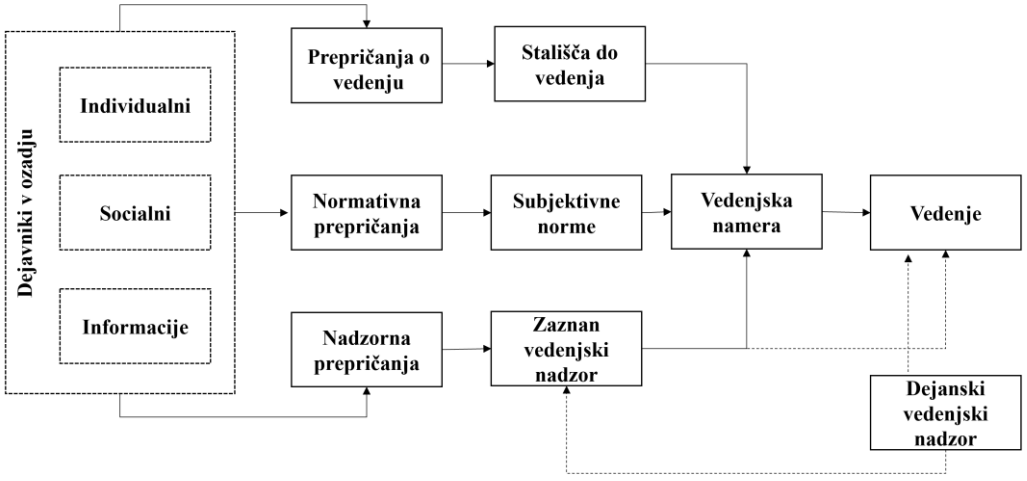
Fishbein in Ajzen (1975) sta najprej razvila TRA (slika 5), ki pojasnjuje vedenja, katera se dogodijo pod posameznikovim zavestnim nadzorom. Ajzen (1991, 2002) je kasneje v omenjeno teorijo vključil dodaten konstrukt in jo s tem preoblikoval v TPB (slika 6).



Slika 5: Shematski prikaz konceptualnega okvirja za napovedovanje specifičnih namer in vedenj – TRA

(Fishbein & Ajzen, 1975, p. 16)

TPB je najpogosteje uporabljena pri pojasnjevanju odnosa med kognicijo in vedenjem posameznika. Po omenjeni teoriji je posameznikovo vedenje določeno z njegovo vedenjsko namero. Napoveduje vedenje posameznika, ki nima popolnega nadzora nad svojim vedenjem.



Slika 6: Shematski prikaz TPB in povezava med konstrukti.

(Ajzen, 1991, p. 182; Fishbein & Ajzen, 2011, p. 22)

TPB se osredotoča na konstrukte prepričanja (angl. »*belief*«), ki imajo na vedenje vpliv (Ajzen, 2005). Gre za konstrukte prepričanj o vedenju in stališču do vedenja v socialnem kontekstu. Selič (1999, p. 42) na primeru vedenja povezanega z zdravjem navaja, da je vedenje mogoče najbolj pravilno napovedati, če poznamo namere posameznikov. V organizacijskem okolju je vedenje posameznika pogosto omejeno, oblikovano, manipulirano s strani organizacijske kulture, struktur, procesov in pravil vrhnjega managementa (Hu, et al., 2012).

Stališča do vedenja (angl. »*Attitude Toward the Behaviour*«, v nadaljevanju ATB) so prepričanja o vedenju, ki delujejo na posameznikov način razmišljanja in njegovo vedenje. Če je izid vedenja zaznan kot ugoden, bo posameznik imel pozitivno naravnana stališča do vedenja in verjetnost za izvedbo vedenja bo večja (Fishbein & Ajzen, 2011).

Subjektivne norme (angl. »*Subjective Norm*« – v nadaljevanju SN) izhajajo iz *normativnih prepričanj* (prepričanja o mnenju pomembnih drugih) (angl. »*Normative Belief*«, v nadaljevanju NB). Gre za intenzivnost pritiska, ki ga posameznik občuti nad izvedbo ali opustitvijo določenega vedenja. Večje kot je zaznavanje pritiska s strani posameznika po željah drugih, večja je motivacija za izvedbo vedenja in večja je verjetnost, da se bo oblikovala namera za izvedbo vedenja. Družbene moči, ki delujejo na posameznikovo vedenje, so moč prisile, moč nagrajevanja, legitimna, strokovna in referenčna moč (Fishbein & Ajzen, 2011, p. 130).

Zaznan vedenjski nadzor (angl. »*Perceived Behavioural Control*«, v nadaljevanju PBC) izhaja iz prepričanj o posameznikovem nadzoru vedenja. Gre za posameznikove zaznave v zvezi s prisotnostjo dejavnikov, ki otežujejo izvedbo določenega vedenja. Posameznik presodi, ali ima potrebna sredstva za premagovanje ovir, da bi lahko izvedel določeno vedenje (Ajzen, 1991). Višja stopnja PBC je prisotna takrat, ko ima posameznik primeren dostop do virov, ki olajšajo izvedbo vedenja, zato ima v tem primeru PBC pozitiven učinek na namero za določeno vedenje. Vedenje je pod individualnim nadzorom, če se posameznik lahko po želji odloči, ali bo neko vedenje izpeljal ali ne. V nekaterih situacijah se lahko zgodi, da posameznik nima popolnega nadzora nad vedenjem, četudi si to želi (Ajzen, 1991).

Dejanski vedenjski nadzor (angl. »*Actual Behavioral Control*«) se nanaša na posameznikove spretnosti, vire, priložnosti, znanje ter pripomočke ali druge pogoje, ki so potrebni za udejanjanje določenega vedenja. Dejanski vedenjski nadzor ima na vedenje posreden ali neposreden učinek (Fishbein & Ajzen, 2011).

Vedenjska namera (angl. »*Behavioural Intention*«, v nadaljevanju BI) je obseg, do katerega je posameznik pripravljen izvesti vedenje na določen način. BI za določeno vedenje pojasnjujejo posameznikova ATB, SN ter PBC. BI zajema motivacijske dejavnike, ki imajo učinek na posameznikovo vedenje. Posameznik bo verjetneje izvedel določeno vedenje, če je prisotna BI (Fishbein & Ajzen, 2011).

Vedenje (angl. »*Behaviour*«) opredelimo s t. i. TACT (angl. »*Target, Action, Context, Time*«) (Ajzen, 1991; D'arcy & Herath, 2011). TPB v kontekstu vedenja v informacijski varnosti razlaga posameznikovo BI sprejetja varnostnih ukrepov in vedenja v skladu s temi.

Dejavniki v ozadju, kot so spol, starost, socialno-ekonomski status, izobrazba itd., imajo posreden učinek na ATB in BI ter so povezani z razlikami v vedenju (Fishbein & Ajzen, 2011). Spol ni vedno povezan z razlikami v vedenju. Mlajši moški so pogosteje vpleteni v prometne nesreče, kakor starejši moški in kakor ženske (Fishbein & Ajzen, 2011, p. 234). Posamezniki (ekstroverti in introverti) imajo lahko različne izkušnje v enakem družbenem okolju. Med interakcijo z drugimi so lahko izpostavljeni različnim vrstam informacij in te podatke lahko uporabijo na različne načine. Posledično bodo verjetno oblikovali zelo različna vedenjska, normativna in nadzorna prepričanja (Fishbein & Ajzen, 2011, p. 237). Večje znanje posamezniku omogoča sprejemanje bolj informiranih odločitev, ki so v skladu z njegovimi osebnimi željami. Informacije posamezniku omogočajo, da izbere način delovanja, ki bo najbolje služil njegovim osebnim interesom. Za obrazložitev vzemimo spodnja dva primera. Več kot posameznik ve o kandidatih na volitvah, lažje se bo odločil za kandidata, ki bo zastopal njegove interese; ali pa več kot posameznik ve o raku ali drugih boleznih, večja je možnost, da bo izbral potek zdravljenja, ki je zanj najprimernejši (Fishbein & Ajzen, 2011, p. 241).

1.3 OPERACIONALIZACIJA RAZISKOVALNEGA PROBLEMA

Informacijsko varnostno kulturo raziskovalci proučujejo več kot 20 let. Kljub temu še vedno ne obstaja splošni konsenz glede dimenzij in faktorjev (Lopes & Oliveira, 2014; Alnatheer, 2015; Tolah, et al., 2017). Pregled literature kaže predvsem na nesoglasja in zamenjavo obeh konceptov – dimenzij in faktorjev, kar povzroča dodatno zmedo. Zaslediti gre, da prihaja do neskladij med teoretičnimi zasnovami in samim pojmom ter dejansko uporabo koncepta v organizacijah (Orehek, 2017). Chen, et al. (2015) na primer navajajo SETA programe ter MON kot dejavnike informacijske varnostne kulture, medtem ko jih Nasir, et al. (2019a) obravnavajo kot dimenzije informacijske varnostne kulture. Vse opisane težave prispevajo k nejasnim teoretičnim zasnovam.

Raziskovalci se poslužujejo različnih pristopov pri konceptualizaciji in operacionalizaciji informacijske varnostne kulture. Nekaj raziskav jo operacionalizira kot samostojen konstrukt (Knapp, et al., 2006; Brady, 2010; Narain Singh, et al., 2014; Chen, et al., 2015; Hayden, 2016; Parsons, et al., 2015; Rocha Flores & Ekstedt, 2016; Wong, et al., 2019; Pridmore & Oomen, 2021; Sari, et al., 2021), druge pa kot večdimenzionalni (sestavljeni) konstrukt. Spet tretje jo preučujejo s strani faktorjev oz. dejavnikov, ki jo oblikujejo (Martins & Eloff, 2002; Da Veiga, et al., 2007; Da Veiga & Eloff, 2010; Gebrasilase & Lessa, 2011; D'Arcy & Greene, 2014), ter njenih dimenzij (Alnatheer, et al., 2012; Safa, et al., 2015; Amankwa, et al., 2018; Da Veiga, 2018; Nasir, et al., 2019a; Sarbaz, et al., 2019) ali jo celo manifestirajo z informacijsko varnostno klimo (Chan, et al., 2005; Kessler, et al., 2020; Dong, et al., 2021).

Čeprav smo s pregledom literature (priloga 1) ugotovili, da obstaja nekaj raziskav s področja zdravstva (Brady, 2010; Gebrasilase & Lessa, 2011; Sarbaz, et al., 2019; Kessler, et al., 2020; Dong, et al., 2021; Pridmore & Oomen, 2021; Sari, et al., 2021), ali pa zdravstvo kot panogo vključuje v širše raziskave (Knapp, et al., 2006; Alnatheer, et al., 2012; D'Arcy & Greene, 2014; Safa, et al., 2015; Rocha Flores & Ekstedt, 2016; Amankwa, et al., 2018), pa nobena izmed njih ne vključuje povezanosti etične komponente z informacijsko varnostno kulturo, ki je za poklic zdravstva in zdravstvene nege kot discipline izrednega pomena.

Več raziskav je ne glede na domeno poudarilo pomen etike v informacijski varnosti (Martins & Eloff, 2002; Da Veiga, et al., 2007; Brady, 2010; Da Veiga & Eloff, 2010; Gebrasilase & Lessa, 2011; D'Arcy & Greene, 2014; Narain Singh, et al., 2014; Hayden, 2016; Safa, et al., 2015; Da Veiga, 2018; Wong, et al., 2019; Kessler, et al., 2020; Sari, et al., 2021), vendar je samo ena od njih (Martins & Eloff, 2002) preučila odnos med etiko in informacijsko varnostno kulturo. Nekateri raziskovalci poudarjajo pomembno vlogo moralnih prepričanj pri nameri zaposlenih s skladnostjo z ISP (Siponen & Vance 2010; D'arcy & Herath, 2011) in delovanjem informacijske varnostne kulture na namero skladnosti (Greene & D'Arcy, 2010).

Pri oblikovanju spremenljivk doktorske naloge smo izhajali iz Ajzenove (1991) TPB, saj predstavlja dobro teoretično podlago za pojasnjevanje vedenja posameznika v različnih organizacijskih in socio-kulturnih okoljih. TPB velja za eno najbolj vplivnih razlag človeškega vedenja (Hu, et al., 2012; Jalali, et al., 2020). Po TPB so ATB, SN ter PBC pomembni napovedovalci BI (Rocha Flores & Ekstedt, 2016; Rajab & Eydgahi, 2019; Vrhovec, et al., 2023).

TPB je uporabljena v številnih raziskavah, povezanih z informacijsko varnostjo (Aigbefo, et al., 2022; Alanazi, et al., 2022; Hong & Furnell, 2022; Ma, 2022; Philip, et al., 2023; Vrhovec, et al., 2023) in velja za drugo najbolj uporabljeno teorijo za preučevanje vedenja na področju kibernetske varnosti (Alsharida, et al., 2023). TPB in njene različice so uporabljene za pojasnitev skladnosti z ISP (Herath & Rao, 2009b; Nasir, et al., 2019a, 2022), skrbno vedenje glede varnosti (Safa, et al., 2015), upiranje socialnemu inženiringu (Rocha Flores & Ekstedt, 2016), za sledenje gradivom ozaveščanja o socialnem inženiringu (Vrhovec, et al., 2023) ter izogibanje grožnjam spletnega izsiljevanja na družbenih omrežjih (Al Ghanboosi, et al., 2023). V pregledu literature avtorjev Mayer, et al. (2017) so bile vedenjske teorije preučevane za oceno zanesljivosti različnih dejavnikov v kontekstu informacijske varnosti. Z raziskavo so prikazali zanesljivost učinkov 11 dejavnikov, vključno z ATB, SN, PBC in BI, kar kaže na dodatno podporo TPB v kontekstu informacijske varnosti.

V do sedaj objavljeni literaturi so na voljo raziskave, ki povezujejo informacijsko varnostno kulturo ter konstrukte TPB. Takšna med njimi je raziskava avtorjev Rocha Flores & Ekstedt (2016), ki sta raziskovala povezave v kontekstu upiranja socialnemu inženiringu. Nasir, et al. (2019a) so potrdili neposredne povezave med informacijsko varnostno kulturo in konstrukti TPB v kontekstu skladnosti z ISP. Hong & Furnell (2022) so našli pomembne povezave med formalizacijo (tj. faktorjem informacijske varnostne kulture) in konstrukti TPB. Al Ghanboosi, et al. (2023) navajajo, da je informacijska varnostna kultura povezana s SN in ATB v kontekstu razlage motivacije za izogibanje spletnim grožnjam na družbenih omrežjih.

Pri pregledu literature smo zasledili raziskavo avtorjev Ma, et al. (2015), katere rezultati so pokazali, da so ATB, SN in PBC pomemben napovedovalec BI medicinskih sester, da pri svojem delu zavarujejo elektronske zdravstvene zapise. Omenjena raziskava ni proučevala povezanosti dimenzij informacijske varnostne kulture s konstrukti TPB.

Za področje organizacijskega okolja se raziskovalci srečujejo s težavami pri merjenju dejanske izvedbe vedenja in se tudi zato glede na močno povezanost med BI in dejansko izvedbo vedenja (Ajzen, 2005) odločajo za preučevanje BI kot odvisne spremenljivke (Herath & Rao, 2009a, 2009b; Bulgurcu, et al., 2010; Siponen & Vance, 2010; Hu, et al., 2012).

Uporabili smo konceptualizacijo informacijske varnostne kulture po avtorjih Nasir, et al. (2019a), saj je omenjena skupina raziskovalcev sistematizirala njene dimenzije. V njihovi raziskavi je informacijska varnostna kultura definirana kot multidimenzionalni konstrukt. Omenjen koncept je zasnovan kot konstrukt drugega reda (angl. »*second order construct*«*)* in je definiran s sedmimi dimenzijami, konstrukti prvega reda (angl. »*first order construct*«). Sedem latentnih konstruktov v modelu definira konstrukt informacijske varnostne kulture, kar nakazuje na povezanost konstrukta informacijske varnostne kulture s formativnimi konstrukti nižjega reda (Nasir, et al., 2019a). Konceptualizacija in operacionalizacija informacijske varnostne kulture na ta način omogoča raziskovalcem, da teoretizirajo in ovrednotijo učinek konstrukta višjega reda (npr. en niz odnosov), namesto učinka njegovih dimenzij (npr. sedem ali več nizov

odnosov) na odvisno spremenljivko (Polites, et al., 2012). Pristop avtorjev Nasir, et al. (2019a) je skladen s ciljem njihove raziskave, ki validira koncept informacijske varnostne kulture in raziskuje učinek konstrukta višjega reda na vedenje zaposlenih glede skladnosti z ISP in ne raziskuje njegove posamezne dimenzije.

Skupni imenovalec identificiranih raziskav je, da dimenzije informacijske varnostne kulture temeljijo na organizacijskih/vodstvenih vidikih. Z vidika zdravstvene nege in etike v zdravstveni negi konstrukti informacijske varnostne kulture temeljijo na deontoloških, utilitarističnih, na pravilih temelječih in intuicionističnih teorijah (angl. »intuitionist theories«) (Noureddine, 2001).

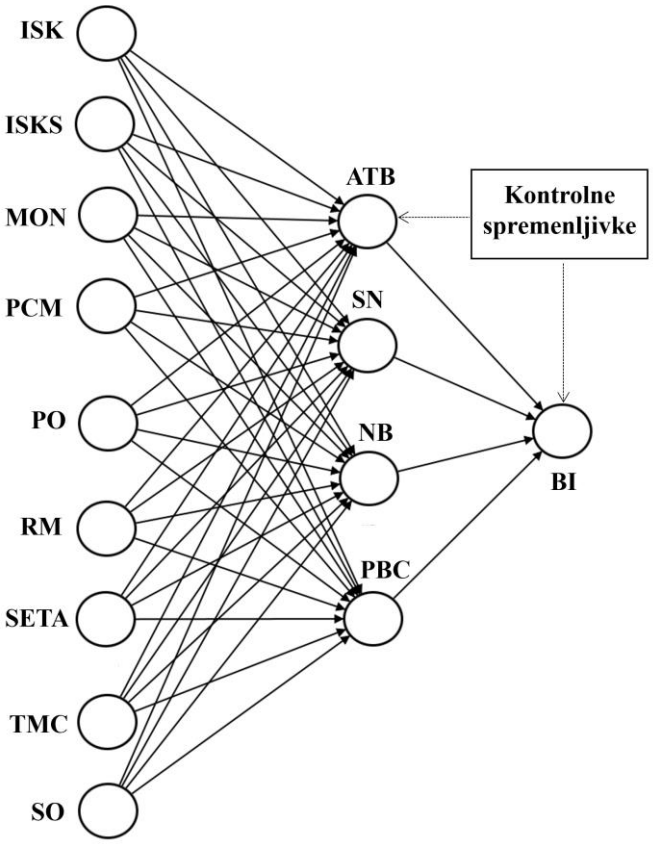
Ko govorimo o področju zdravstvene nege, se mora koncept informacijske varnostne kulture razširiti onkraj organizacijskih, vodstvenih in tehničnih vidikov, tako da vključuje tudi edinstvene elemente, značilne za zdravstveno nego, npr. etiko in moralo. Etika skrbi je npr. že bila opredeljena kot potencialni vodilni filozofski okvir v informacijski varnosti (Blanken-Webb, 2020). Nobena od prejšnjih raziskav ne upošteva omenjenega vidika v konceptualizaciji informacijske varnostne kulture, saj temu področju v zdravstveni negi ni bilo namenjeno posebne pozornosti, zato smo v raziskovalni model (slika 7) dodali dve novi dimenziji informacijske varnostne kulture (Mikuletič, et al., 2024), t.j. usmerjenost k varnosti podatkov (angl. »*Security Oriented*« – v nadaljevanju SO) in usmerjenost k zagotavljanju zasebnosti« (angl. »*Privacy* O*riented«* – v nadaljevanju PO), ki smo ju identificirali s pomočjo pregledane literature (priloga 1) in preliminarno kvalitativno raziskavo (priloga 2).

Dimenzija SO se nanaša na zaznavanje posameznika o prisotnosti dobre prakse zagotavljanja varovanja podatkov v zdravstveni organizaciji, medtem ko se dimenzija PO nanaša na zaznavanje posameznika o poklicni molčečnosti, zagotavljanju in varovanju zasebnosti pacientov ter zagovarjanju pravic do zasebnosti (Mikuletič, et al., 2024).

Čeprav sta dimenziji SO in PO na novo opredeljeni dimenziji informacijske varnostne kulture, je mogoče v literaturi zaslediti številne dokaze za njuno utemeljenost.

Medtem ko večina raziskav sloni na varnostnem vidiku, se samo ena raziskava osredotoča na vidik zasebnosti, in sicer z vpeljavo informacijske varnostne kulture (Da Veiga & Martins, 2015). Čeprav sta varnost in zasebnost povezana pojma, se vedno ne povezujeta med seboj (Da Veiga & Martins, 2015). Na primer organizacija z močno varnostno kulturo morda ni nujno tudi organizacija z močno zasebnostno kulturo. Na osnovi teh dopolnjujočih se vidikov informacijske varnostne kulture ima smisel opredeliti njene dimenzije tudi v varnost (SO) in zasebnost (PO) (Mikuletič, et al., 2024). Na voljo do sedaj razen naše raziskave (Mikuletič, et al., 2024) ni bilo raziskav, ki bi hkrati opredelile ali empirično potrdile omenjeni dimenziji.

Pojem »kršitev informacijske varnosti« smo operacionalizirali z nepooblaščenim dostopom do zdravstvenih podatkov (McCoy & Perlis, 2018; U.S. Department of Health & Human Services – Office for Civil Rights, n.d.). V Tabeli 1 smo prikazali definicije konstruktov raziskovalnega modela.



Slika 7: Uporabljeni raziskovalni model

Tabela 1: Operacionalizacija

Konstrukt	Definicija	Primarni vir
PCM	Ozaveščenost zaposlenega glede ISP v organizaciji.	Nasir, et al. (2019a)
RM	Dojemanje zaposlenega glede analize in ocene tveganja za informacijsko varnost ter njegovo mnenje o tem, ali gre za neizogiben postopek.	Nasir, et al. (2019a)
SETA	Dojemanje zaposlenega glede usposabljanja na področju informacijske varnosti znotraj organizacije, ki je povezano z izobraževanjem o varnosti, varnostnim usposabljanjem in programom za dvig ozaveščenosti.	Nasir, et al. (2019a)
TMC	Mnenje zaposlenega o vključenosti višjega vodstva v vprašanja, povezana z informacijsko varnostjo organizacije.	Nasir, et al. (2019a)
MON	Mnenje zaposlenega o organizacijskih dejavnostih, povezanih z računalniškim sledenjem in o izvajanju revizij informacijske varnosti.	Nasir, et al. (2019a)
ISK	Mnenje zaposlenega o poznavanju informacijske varnosti, ki velja znotraj organizacije.	Nasir, et al. (2019a)
ISKS	Mnenje zaposlenega o deljenju znanja o informacijski varnosti znotraj organizacije in ali je to po njegovem mnenju pomembno.	Nasir, et al. (2019a)
PO	Zaznavanje posameznika o poklicni molčečnosti, zagotavljanju in varovanju zasebnosti pacientov ter zagovarjanju pravic do zasebnosti.	Nastal na podlagi izvedenih intervjujev
SO	Zaznavanje posameznika o prisotnosti dobre prakse zagotavljanja varovanja podatkov v organizaciji.	Nastal na podlagi pregledane literature
ATB	Presoja posameznika o tem ali je dobro ali slabo izvesti določeno vedenje.	Ajzen, 1991
SN	Posameznikovo zaznavanje o tem ali določeno vedenje sprejema in spodbuja njemu pomemben družbeni krog ljudi.	Ajzen, 1991
NB	Zaznan socialni pritisk posameznika glede skladnosti z zahtevami organizacije, povezano z organizacijsko politiko in prakso, ki ga povzročajo sodelavci, podrejeni ali nadrejeni.	Ajzen, 1991
PBC	Zaznana težavnost izvedbe določenega vedenja in posameznikov, občutek o tem ali ima veščine in sredstva za izvedbo določenega vedenja.	Ajzen, 1991
BI	Obseg, do katerega je posameznik pripravljen izvesti vedenje na določen način.	Ajzen, 1991

Legenda: PCM – postopkovni protiukrepi, RM – obvladovanje tveganj, SETA – varnostno izobraževanje, usposabljanje in ozaveščanje, TMC – zavezanost vrhnjega managementa, MON – nadzorovanje/spremljanje varnosti, ISK – znanje o informacijski varnosti, ISKS – izmenjava znanja o informacijski varnosti, SO – usmerjenost k varnosti podatkov, PO – usmerjenost k zagotavljanju zasebnosti, ATB – stališča do vedenja, SN – subjektivne norme, NB – normativna prepričanja, PBC – zaznan vedenjski nadzor, BI – vedenjska namera.

2 NAMEN IN CILJI RAZISKAVE

Namen doktorske disertacije je preučiti pojav nepooblaščenega dostopa do zdravstvenih podatkov na slovenski populaciji zaposlenih v zdravstveni negi ter povezanost dimenzij informacijske varnostne kulture s stališči do vedenja, subjektivnimi normami, z normativnimi prepričanji, zaznanim vedenjskim nadzorom ter namero za izvedbo omenjene kršitve.

Cilji doktorske disertacije so:

- Preveriti koncept dimenzij in stanje informacijske varnostne kulture pri zaposlenih v zdravstveni negi v Republiki Sloveniji.
- Preveriti povezanost dimenzij informacijske varnostne kulture s konstrukti TPB.
- Ugotoviti, katere vzvode, ki se nanašajo na informacijsko varnostno kulturo, lahko uporabijo zdravstvene in socialnovarstvene ustanove za zmanjšanje tveganja za kršitev zaupnosti zdravstvenih podatkov s strani zaposlenih v zdravstveni negi.

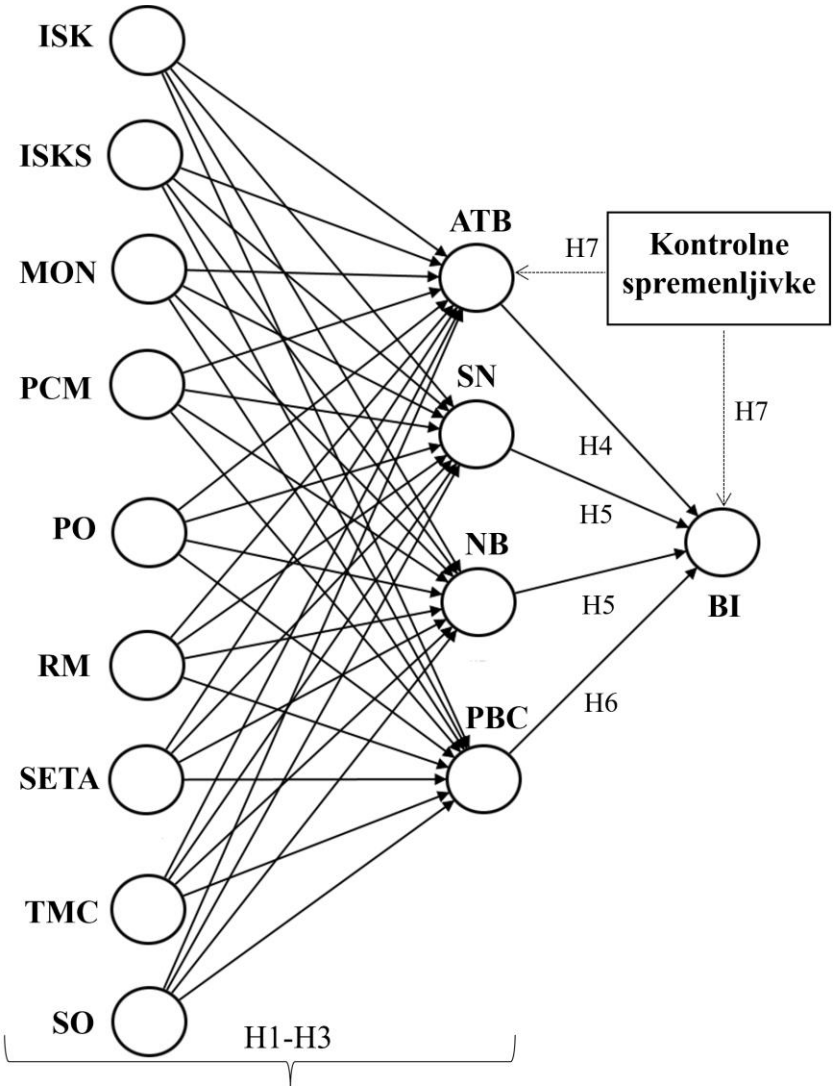
2.1 RAZISKOVALNO VPRAŠANJE IN HIPOTEZE

Raziskovalno vprašanje na katerega smo poskušali z doktorsko disertacijo odgovoriti, se glasi: *»V kolikšni meri so dimenzije informacijske varnostne kulture dober pokazatelj vedenjske namere kršitev informacijske varnosti pri zaposlenih v zdravstveni negi«.*

Skladno z literaturo, ki preučuje dimenzije informacijske varnostne kulture in odnose med konstrukti TPB, smo v nadaljevanju oblikovali sedem hipotez. Raba besedne zveze »dimenzije informacijske varnostne kulture« v H1–H3 obsega vseh devet dimenzij, predstavljenih v Tabeli 1. Hipotetični okvir odvisnih in neodvisnih spremenljivk smo prikazali na Sliki 8, Tabeli 2 in Tabeli 3. Hipoteze zastavljene v nadaljevanju predpostavljajo, da je povezanost dimenzij informacijske varnostne kulture preko manifestnih vrednot na vedenje zaposlenih posredovano preko konstruktov prepričanj zaposlenih v zdravstveni negi.

- H1: Dimenzije informacijske varnostne kulture so negativno povezane z ATB zaposlenih v zdravstveni negi glede izvedbe nepooblaščenega dostopa do zdravstvenih podatkov.
- H2: Dimenzije informacijske varnostne kulture so negativno povezane s SN oz. NB zaposlenih v zdravstveni negi glede izvedbe nepooblaščenega dostopa do zdravstvenih podatkov.
- H3: Dimenzije informacijske varnostne kulture so negativno povezane s PBC zaposlenih v zdravstveni negi glede izvedbe nepooblaščenega dostopa do zdravstvenih podatkov.
- H4: ATB zaposlenih v zdravstveni negi do izvedbe nepooblaščenega dostopa do zdravstvenih podatkov so pozitivno povezana z BI glede izvedbe omenjene kršitve.
- H5: SN in NB zaposlenih v zdravstveni negi do izvedbe nepooblaščenega dostopa do zdravstvenih podatkov so pozitivno povezana z BI glede izvedbe omenjene kršitve.
- H6: PBC zaposlenih v zdravstveni negi nad izvedbo nepooblaščenega dostopa do zdravstvenih podatkov je pozitivno povezana z BI glede izvedbe omenjene kršitve.
- H7: Spremenljivke *starost*, *izobrazba* in *delovna doba* zaposlenih v zdravstveni negi so negativno povezane z njihovimi ATB in BI glede izvedbe nepooblaščenega dostopa do podatkov.
- H7a: Spremenljivka *starost* zaposlenih v zdravstveni negi je negativno povezana z njihovimi ATB glede izvedbe nepooblaščenega dostopa do zdravstvenih podatkov.
- H7b: Spremenljivka *starost* zaposlenih v zdravstveni negi je negativno povezana z njihovo BI glede izvedbe nepooblaščenega dostopa do zdravstvenih podatkov.
- H7c: Spremenljivka *izobrazba* zaposlenih v zdravstven negi je negativno povezana z njihovimi ATB glede izvedbe nepooblaščenega dostopa do zdravstvenih podatkov.
- H7d: Spremenljivka *izobrazba* zaposlenih v zdravstveni negi je negativno povezana z njihovo BI glede izvedbe nepooblaščenega dostopa do zdravstvenih podatkov.

- H7e: Spremenljivka *delovna doba* zaposlenih v zdravstveni negi je negativno povezana z njihovimi ATB glede izvedbe nepooblaščenega dostopa do zdravstvenih podatkov.
- H7f: Spremenljivka *delovna doba* zaposlenih v zdravstveni negi je negativno povezana z njihovo BI glede izvedbe nepooblaščenega dostopa do zdravstvenih podatkov.



Slika 8: Hipotetični okvir

Tabela 2: Hipotetični okvir neodvisnih spremenljivk

Konstrukt		Neodvisne spremenljivke
PCM	PCM1	Hovav & D'Arcy (2012); Chen, et al. (2015)
	PCM2	Hovav & D'Arcy (2012); Nasir, et al. (2019a)
	PCM3	Chen, et al. (2015)
	PCM4	Hovav & D'Arcy (2012)
RM	RM1	Da Veiga (2008)
	RM2	Nasir, et al. (2019a)
	RM3	Nasir, et al. (2019a)
SETA	SETA1	Hovav & D'Arcy (2012); Chen, et al. (2015)
	SETA2	Nasir, et al. (2019a)
	SETA3	Nasir, et al. (2019a)
	SETA4	Hovav & D'Arcy (2012)
TMC	TMC1	Hu, et al. (2012)
	TMC2	Hu, et al. (2012); Nasir, et al. (2019a)
	TMC3	Hu, et al. (2012); Nasir, et al. (2019a)
	TMC4	Knapp, et al. (2006)
MON	MON1	Hovav & D'Arcy (2012); Chen, et al. (2015)
	MON2	D'Arcy & Greene (2014); Chen, et al. (2015)
	MON3	Hovav & D'Arcy (2012); D'Arcy & Greene (2014); Chen, et al. (2015)
ISK	ISK1	Da Veiga (2008)
	ISK2	Da Veiga (2008)
	ISK3	Van Niekerk & Von Solms (2006, 2010); Zakaria (2006)
ISKS	ISKS1	Safa, et al. (2016)
	ISKS2	Nasir, et al. (2019a)
	ISKS3	Nasir, et al. (2019a)
	ISKS4	Nasir, et al. (2019a)
PO	PO1	Mikuletič, et al. (2024)
	PO2	Mikuletič, et al. (2024)
	PO3	Mikuletič, et al. (2024)
	PO4	Mikuletič, et al. (2024)
	PO5	Mikuletič, et al. (2024)
SO	SO1	Chen, et al. (2015)
	SO2	Chen, et al. (2015)
	SO3	Chen, et al. (2015)
	SO4	Chen, et al. (2015)
	SO5	Rocha Flores & Ekstedt (2016)
Demografski podatki	Spol	Mikuletič, et al. (2024)
	Starost	Mikuletič, et al. (2024)
	Izobrazba	Mikuletič, et al. (2024)
	Delovna doba	Mikuletič, et al. (2024)

Legenda: Tabela 1

Tabela 3: Hipotetični okvir odvisnih spremenljivk

Konstrukt		Odvisne spremenljivke
ATB	ATB1	Herath & Rao (2009a); Moody, et al. (2018)
	ATB2	Herath & Rao (2009a)
	ATB3	Herath & Rao (2009a); Moody, et al. (2018)
SN	SN1	Park & Smith (2007)
	SN2	Park & Smith (2007)
	SN3	Park & Smith (2007)
NB	NB1	Ajzen (1991); Bulgurcu, et al. (2010); Kranz & Haeussinger (2014)
	NB2	Nasir, et al. (2019a)
	NB3	Mikuletič, et al. (2024)
PBC	PBC1	Lee (2009); Moody, et al. (2018)
	PBC2	Lee (2009); Moody, et al. (2018)
	PBC3	Lee (2009); Moody, et al. (2018)
BI	BI1	Moody, et al. (2018); Murko & Vrhovec (2019)
	BI2	Moody, et al. (2018); Murko & Vrhovec (2019)
	BI3	Moody, et al. (2018); Murko & Vrhovec (2019)

Legenda:Tabela 1

3 METODE

3.1 RAZISKOVALNI NAČRT

Izbrani pristop k raziskovanju predstavljenega raziskovalnega problema je deduktiven, zaznan s pozitivistično paradigmo. Uporabljen je bil kvantitativni, ne-eksperimentalni pristop z izvedbo deskriptivne (opisne) raziskave. Izvedena je bila presečna raziskava z enkratnim vzorcem, kar velja za najpogosteje uporabljen raziskovalni dizajn v sociooloških znanostih. Gre za najprimernejši raziskovalni dizajn za ugotavljanje razširjenosti fenomenov, situacij, problemov, odnosov ali vprašanj pri izbrani populaciji. Nudi pridobitev celotne slike v enkratnem časovnem oknu. Ker se izvaja le enkrat (en stik s populacijo), je izvedba presečne raziskave cenovno in časovno ugodna (Kumar, 2011).

3.2 UDELEŽENCI RAZISKAVE

3.2.1 Populacija in vzorec

Udeleženci raziskave so zaposleni v zdravstveni negi v Republiki Sloveniji. Gre za izvajalce, ki so vpisani v Register izvajalcev zdravstvene nege (Zbornica – Zveza, 2019). Velikost populacije je po podatkih Nacionalnega inštituta za javno zdravje v letu 2020 znašala 22.307 zaposlenih v zdravstveni negi (NIJZ, n.d.), kar v našem primeru predstavlja 2,4-odstotno stopnjo odziva.

Značilnosti vzorca in populacije so predstavljene v Tabeli 4. Opazne so nekatere razlike med značilnostmi vzorca in populacije. Najpomembnejša razlika se nanaša na stopnjo dosežene izobrazbe. V vzorcu je opazno višji delež respondentov z diplomo (72,9 %), v primerjavi z deležem v populaciji (37,3 %). Vzorec se zdi rahlo pristranski, saj vključuje manj respondentov v kategorijah do 39 let in več respondentov v kategorijah med 40 in 59 let. Vzorec vključuje tudi bolj enakomeren delež zastopanosti nivojev organizacij (tj. štiri glavne kategorije so skoraj enako zastopane), medtem ko bi v populaciji morala biti

deleža nivojev I in III nekoliko višja, delež socialno-varstvenih zavodov pa nižji kot v vzorcu.

Tabela 4: Značilnosti vzorca in populacije

	Vzorec	**Populacija**
Spol		
Moški	70 (13,3 %)	3,458 (15,5 %)
Ženski	457 (86,7 %)	18,849 (84,5 %)
Starost		
< 30	74 (14,0 %)	4,330 (19,4 %)
30–39	130 (24,7 %)	6,374 (28,6 %)
40–49	167 (31,7 %)	5,170 (23,2 %)
50–59	137 (26,0 %)	5,439 (24,4 %)
> 60	19 (3,6 %)	994 (4,4 %)
Formalna izobrazba		
Brez diplome (srednja medicinska sestra, višja medicinska sestra)	143 (27,1 %)	13,976 (62,7 %)
Z diplomo (diplomirana medicinska sestra, magistrica zdr. nege)	384 (72,9 %)	8,331 (37,3 %)
Nivo zdravstvenega varstva/organizacija		
I	128 (24,3 %)	6,830 (30,6 %)
II	124 (23,5 %)	5,437 (24,4 %)
III	132 (25,0 %)	6,240 (28,0 %)
Socialno-varstveni zavodi	125 (23,7 %)	3,198 (14,3 %)
Ostalo	17 (3,2 %)	602 (2,7 %)
N/A	1 (0,2 %)	-

Legenda: N/A – podatek ni na voljo (angl. »*Not Available*«)

3.2.2 Profil udeležencev

V raziskavo je bilo vključenih 527 udeležencev, zaposlenih v zdravstveni negi z različno stopnjo izobrazbe, iz vseh treh ravni zdravstvenega varstva in socialno-varstvenih ustanov. Udeleženci raziskave predstavljajo heterogeno skupino naključnega vzorca ciljne populacije. Podatki za profil udeležencev so na voljo v Prilogi 3.

V raziskavi je sodelovalo (n = 527) udeležencev, 70 (13,3 %) moških in 457 (86,7 %) žensk. Njihova povprečna starost znaša 42,4 let (SD = 10,4); najmlajši udeleženec ima 22 let, najstarejši pa 63 let. Povprečna delovna doba v organizaciji, kjer so trenutno zaposleni udeleženci, znaša 16,7 let (SD = 11,9), minimalna še ne kot leto dni, medtem ko najvišja šteje 42 let.

Srednje medicinske sestre predstavljajo 23,5 % (n = 124), višje medicinske sestre/višji medicinski tehniki 3,6 % (n = 19), diplomirane medicinske sestre/diplomirani zdravstveniki 58,4 % (n = 308) in magistri/-ce zdravstvene nege 14,4 % (n = 76) vzorca.

Izobrazbo na drugih področjih od skupaj 166 (n = 531) jih ima 49,4 % (n = 82) visoko-strokovno izobrazbo; 27,1 % (n = 45) strokovni magisterij; 16,9 % (n = 28) univerzitetno izobrazbo in 6,6 % (n = 11) znanstveni magisterij.

Zaposlitveni status v 92,2 % (n = 486) predstavlja zaposlitev za polni delovni čas; 2,8 % (n = 15) zaposlitev za polovični delovni čas; 1,1 % (n = 6) bolniško odsotnost z dela; 1,3 % (n = 7) porodniški dopust in 2,5 % (n = 13) ostalo.

Tip organizacije, kjer so zaposleni udeleženci v 24,3 % (n = 128) predstavljajo zdravstveni domovi; 19 % (n = 100) splošne bolnišnice; 4,6 % (n = 24) specialistične bolnišnice; 20,7 % (n = 109) klinični centri (vključno s klinikami); 3% (n = 16) samostojne klinike; 1,3 % (n = 7) inštituti; 23,8 % (n = 125) socialno varstveni zavodi in 3,2 % (n = 17) drugo.

Okolje organizacije iz katerega prihajajo udeleženci v 76,9 % (n = 405) predstavlja urbano/mestno okolje in 23,1 % (n = 122) ruralno/podeželsko okolje.

3.3 INSTRUMENTI RAZISKAVE

Oluka, et al. (2014) so v svojem sistematičnem pregledu literature, kjer so ocenjevali kakovost vprašalnikov, ki temeljijo na TPB, ugotovili pomanjkanje podrobnih opisov postopka razvoja vprašalnika. Omenjeni avtorji navajajo, da je zaradi pomanjkanja opisov razvoja vprašalnikov nemogoče oceniti njihovo zanesljivost. Smernice za razvoj vprašalnika je opisal tudi teoretični avtor Ajzen (2002), vse pogosteje pa se uporabljajo smernice za raziskovalce v zdravstveni dejavnosti (Francis, et al., 2004). Orehek (2017) je v svoji metaanalizi ugotavljala obstoj in kakovost merskih instrumentov za merjenje informacijske varnostne kulture. Ugotovila je, da je na voljo več merskih instrumentov,

ki merijo sorodne koncepte, ni pa razpoložljivih veljavnih in zanesljivih kakovostnih vprašalnikov, ki bi merili omenjen koncept.

V nadaljevanju doktorske disertacije sledi podrobno opisan razvoj merskega instrumenta, njegov prevod in adaptacija, pred-test in pilotno testiranje, testiranje vprašalnika na veljavnost, zanesljivost ter pristranost zaradi uporabe ene metode.

3.3.1 Razvoj merskega instrumenta

Za merjenje dimenzij informacijske varnostne kulture smo uporabili preveden in prilagojen vprašalnik avtorjev Nasir, et al. (2019a). Elementi vprašalnika so rezultat dela številnih raziskovalcev (tabela 5) in so bili v preteklosti že validirani. Izjema so elementi konstruktov RM in ISK, ki so bili v preteklosti že validirani, vendar pa so jih raziskovalci Nasir, et al. (2019 b) prilagodili za namen svoje raziskave. Straub in Welke (1998) trdita, da je uporaba že predhodno validiranih merilnih instrumentov zaželjena, saj tako povečajo in zagotovijo vsebinsko veljavnost in zanesljivost merilnih elementov konstruktov (Nunnally & Bernstein, 1994). Konstrukte TPB smo merili s prilagojenimi elementi avtorjev Ajzen (1991); Park & Smith (2007); Lee (2009); Herath & Rao (2009a); Bulgurcu, et al. (2010); Kranz & Haeussinger (2014); Moody, et al. (2018); Nasir, et al. (2019a) ter Murko & Vrhovec (2019). Vprašalniku smo dodali dva nova konstrukta, in sicer PO in SO ter scenarij nepooblaščenega dostopa do zdravstvenih podatkov (Mikuletič, et al., 2024). Omenjena konstrukta in uporaba scenarija so nastali pri pregledu literature in z rezultati izvedene preliminarne kvalitativne raziskave (priloga 2). V vprašalnik smo z namenom zmanjšanja problema pristranosti zaradi skupne metode zbiranja podatkov (angl. »*Common Method Bias*«, v nadaljevanju CMB) in variance skupne metode (angl. »*Common Method Variance*«, v nadaljevanju CMV) vnesli spremenljivko, ki se nanaša na družbeno zaželenost (angl. »*social desirability*«) (Hays, et al., 1989). Slednjo smo uporabili za ugotavljanje CMV učinka v kasnejši fazi analize podatkov (Podsakoff, et al., 2003).

V zasnovi vprašalnika smo izvedli več modifikacij pri dizajnu vprašalnika. Ker se podatki zbirajo samo iz enega vira, smo uvedli metodološko ločitev z namenom prekinitve

povezave med neodvisnimi in odvisnimi spremenljivkami. Kombinirali smo 5- in 7-stopenjsko Likertovo lestvico (Podsakoff, et al., 2003, 2012; Tehseen, et al., 2017; Nasir, et al., 2019a). 5-stopenjsko lestvico smo dodelili za konstrukte PO, SO, RM, TMC, ISK, SN, BI, 7-stopenjsko lestvico pa konstruktom SETA, MON, ISK, ATB, NB in PBC. Interval meritev na 7-stopenjski Likertovi lestvici zajema strinjanje oz. nestrinjanje z navedenimi trditvami, in sicer: (1) močno se ne strinjam, (2) se ne strinjam, (3) delno se ne strinjam, (4) nevtralno, (5) delno se strinjam, (6) se strinjam, (7) močno se strinjam. Interval meritev na 5-stopenjski lestvici zajema strinjanje oz. nestrinjanje z navedenimi trditvami, in sicer: (1) močno se ne strinjam, (2) se ne strinjam, (3) nevtralno, (4) se strinjam, (5) močno se strinjam. Dizajn vprašalnika predstavlja različne strani, za vsak del in temo ločeno, kar zagotavlja proksimalno ločitev in povečanje razdalje med meritvami (Podsakoff, et al., 2003).

Z namenom zagotavljanja anonimnosti, osebnih podatkov, kot so ime, priimek, naslov prebivališča, e-naslov, ime zaposlitvene organizacije nismo zbirali. Na ta način smo zmanjšali možnost pričakovanih odgovorov (Degirmenci, et al., 2013; Uffen, et al., 2012).

Tabela 5: Elementi vprašalnika

	Elementi	Vir
PO	*V naši organizaciji smo zavezani k poklicni molčečnosti.*	Mikuletič, et al., 2024
	V naši organizaciji smo zavezani k zagotavljanju zasebnosti pacientov.	Mikuletič, et al., 2024
	V naši organizaciji varujemo zasebnost pacientov.	Mikuletič, et al., 2024
	V naši organizaciji zagovarjamo pravice pacientov do zasebnosti.	Mikuletič, et al., 2024
	V naši organizaciji se držimo pravila »ne delaj drugim, kar ne želiš, da bi drugi naredili tebi" glede zasebnosti pacientov.	Mikuletič, et al., 2024
SO	*V naši organizaciji je prisotna kultura spodbujanja dobrih praks za varovanje podatkov o pacientih.*	Chen, et al., 2015
	Varnost podatkov o pacientih je od nekdaj pomembna vrednota naše organizacije.	Chen, et al., 2015
	Zagotavljanje dobre varnosti podatkov o pacientih je sprejet način dela v naši organizaciji.	Chen, et al., 2015
	Zagotavljanje varnosti podatkov o pacientih je ključna norma, ki velja za vse zaposlene.	Chen, et al., 2015
	V naši organizaciji je varnost podatkov o pacientih kolektivna odgovornost.	Rocha Flores & Ekstedt, 2016

	Elementi	Vir
PCM	*Naša organizacija ima pravila, ki zaposlenim prepovedujejo dostopati v informacijski/-e sistem(e), za katerega/-e niso pooblaščeni.*	Hovav & D'Arcy, 2012; Chen, et al., 2015
	Naša organizacija ima vzpostavljena pravila obnašanja glede uporabe informacijskih virov.	Hovav & D'Arcy, 2012; Nasir, et al., 2019a
	Naša organizacija ima izdelane smernice dela z računalniki in ostalimi napravami.	Chen, et al., 2015
	Naša organizacija ima izdelane smernice o primerni uporabi elektronske pošte.	Hovav & D'Arcy, 2012
RM	*Naša organizacija primerno nadzoruje grožnje informacijskim virom.*	Da Veiga (2008)
	Menim, da ima naša organizacija ustrezno vzpostavljene postopke prepoznavanja morebitnih tveganj povezanih z izgubo zaupnosti, celovitosti in razpoložljivosti informacijskih virov.	Nasir, et al., 2019a
	Menim, da naša organizacija dobro prepoznava šibke točke svojih informacijskih virov.	Nasir, et al., 2019a
SETA	*Zaposleni v naši organizaciji so seznanjeni s posledicami nepooblaščenega spreminjanja podatkov.*	Hovav & D'Arcy, 2012; Chen, et al., 2015
	Zaposleni v naši organizaciji so seznanjeni s posledicami nepooblaščenega dostopanja do informacijskih sistemov.	Nasir, et al., 2019a
	Naša organizacija izobražuje zaposlene o odgovornosti zaposlenih glede varnosti podatkov.	Nasir, et al., 2019a
	Naša organizacija zagotavlja usposabljanja, kjer lahko zaposleni izboljšajo svojo varnostno ozaveščenost.	Hovav & D'Arcy, 2012
TMC	*Menim, da ima višje vodstvo naše organizacije jasno vizijo o informacijski varnosti.*	Hu, et al., 2012
	Menim, da ima višje vodstvo naše organizacije jasno oblikovano strategijo doseganja visoke stopnje informacijske varnosti.	Hu, et al., 2012*;* Nasir, et al., 2019a
	Menim, da je višje vodstvo naše organizacije postavilo jasne cilje za doseganje visoke stopnje informacijske varnosti.	Hu, et al., 2012*;* Nasir, et al., 2019a
	Višje vodstvo naše organizacije smatra informacijsko varnost kot prioriteto.	Knapp, et al., 2006
MON	*Menim, da naša organizacija izvaja redne revizijske presoje, katerih cilj je odkrivanje uporabe nepooblaščene programske opreme na službenih računalnikih oz. napravah.*	Hovav & D'Arcy, 2012; Chen, et al., 2015
	Menim, da naša organizacija spremlja aktivnosti zaposlenih pri delu z informacijskimi sistemi.	Chen, et al., 2015; D'Arcy & Greene, 2014
	Menim, da naša organizacija redno nadzira zgodovino aktivnosti, ki jih izvedejo zaposleni v informacijskem sistemu (npr. prijava/odjava v sistem, vnos, sprememba, brisanje podatkov).	Hovav & D'Arcy, 2012; D'Arcy & Greene 2014; Chen, et al., 2015
ISK	*Naša organizacija ima na voljo kompetentne(ga) strokovnjaka/-e (zunanje oz. notranje), ki zagotavljajo izvajanje nadzora nad informacijsko varnostjo.*	Da Veiga, 2008
	Menim, da ima naša organizacija na voljo ustrezno znanje (zunanje oz. notranje), da lahko skladno z veljavno zakonodajo izvede notranji nadzor stanja informacijske varnosti.	Da Veiga, 2008
	Menim, da ima naša organizacija na voljo ustrezno znanje (zunanje oz. notranje kadre), da lahko izvede/organizira programe/promocije na področju informacijske varnosti (npr. izobraževanja, seminarji, tečaji).	Van Niekerk & Von Solms, 2006, 2010; Zakaria, 2006

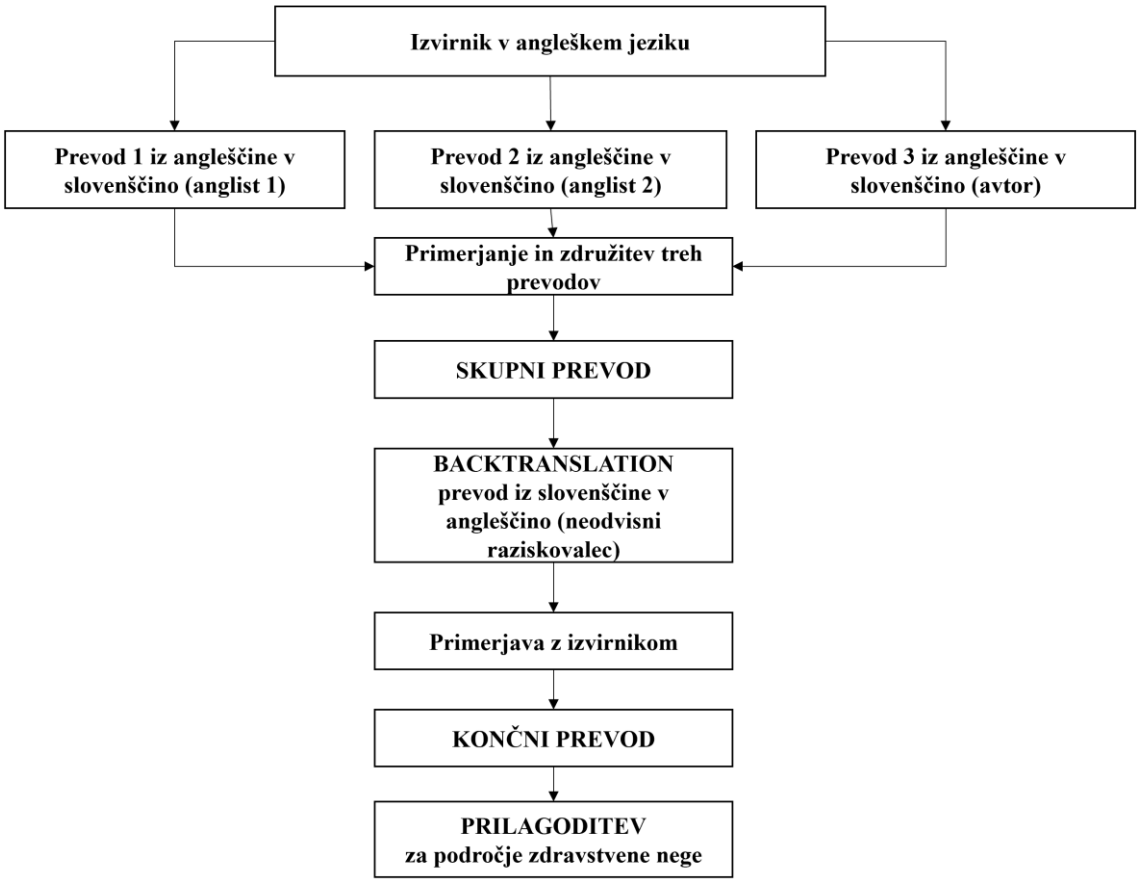
	Elementi	Vir
ISKS	*V naši organizaciji si zaposleni medsebojno izmenjujejo znanja in izkušnje glede informacijske varnosti.*	Safa, et al., 2016
	Vsi zaposleni so aktivno vključeni v izmenjavo znanja in izkušenj o informacijski varnosti.	Nasir, et al., 2019a
	Menim, da obstoječa izmenjava znanja in izkušenj med zaposlenimi o informacijski varnosti učinkovito pomaga razumeti obstoječa pravila naše organizacije na tem področju.	Nasir, et al., 2019a
	Menim, da je izmenjava znanja in izkušenj med zaposlenimi o informacijski varnosti običajna utečena praksa.	Nasir, et al., 2019a
ATB	*Ravnati kot ga. Novak bi bila zelo dobra ideja.*	Herath & Rao, 2009a; Moody, al., 2018
	Ravnati kot ga. Novak bi bilo zelo koristno.	erath & Rao, 2009a
	Ravnati kot ga. Novak bi bilo zelo pametno.	Herath & Rao, 2009a; Moody, et al., 2018
SN	*Večina meni pomembnih ljudi meni, da bi morala ravnati kot ga. Novak.*	Park & Smith, 2007
	Večina ljudi, katere cenim, meni, da bi morala ravnati kot ga. Novak.	Park & Smith, 2007
	Od mene se pričakuje, da ravnam kot ga. Novak.	Park & Smith, 2007
NB	*Moji nadrejeni menijo, da bi morala ravnati kot ga. Novak.*	Ajzen, 1991; Bulgurcu, et al., 2010; Kranz & Haeussinger, 2014
	Moji sodelavci menijo, da bi morala ravnati kot ga. Novak.	Nasir, et al., 2019a
	Moj vodja izmene meni, da bi morala ravnati kot ga. Novak.	Mikuletič, et al., 2024
PBC	*Zmožna sem, da se samostojno odločim, da ravnam kot ga. Novak.*	Lee, 2009; Moody, et al.,2018
	Pod nadzorom imam, da se odločim, da ravnam kot ga. Novak.	Lee, 2009; Moody, et al., 2018
	Menim, da imam sredstva, znanje in sposobnosti, da se odločim, da ravnam kot ga. Novak.	Lee, 2009; Moody, et al., 2018
BI	*Če bi se znašla v primerljivih okoliščinah, bi ravnala kot ga. Novak.*	Moody, et al., 2018; Murko & Vrhovec, 2019
	Ravnati enako kot ga. Novak je nekaj, kar bi naredila tudi sama, če bi se znašla v primerljivih okoliščinah.	Moody, et al., 2018; Murko & Vrhovec, 2019
	Predstavljam si, da bi ravnala enako kot ga. Novak, če bi se znašla v primerljivih okoliščinah.	Moody, et al., 2018; Murko & Vrhovec, 2019

Legenda: Tabela 1

3.3.2 Postopek prevoda vprašalnika

Vprašalnik smo iz angleškega v slovenski jezik prevedli (angl. *»forward translation«*) trije prevajalci. Sledila je primerjava in konsolidacija vseh treh prevodov. Končen prevod je iz slovenščine nazaj v angleščino (angl. *»backtranslation*«) izvedel drugi raziskovalec. Dobljeno angleško različico smo primerjali z izvirnim vprašalnikom in preverili odstopanja. Vprašalnik je bil s konsenzom dveh raziskovalcev adaptiran za področje zdravstvene nege ter tematike nepooblaščenega dostopa do podatkov, saj je bil prvotni

vprašalnik avtorjev Nasir, et al. (2019a) namenjen malezijskim visokošolskim ustanovam. Postopek prevoda merskega instrumenta je prikazan na Sliki 9.



Slika 9: Postopek prevoda vprašalnika

3.3.3 Pred-test vprašalnika in vsebinska veljavnost

Vsebinska veljavnost je opredeljena kot stopnja, do katere elementi predstavljajo konstrukt, ki ga merimo. Vsebinsko veljavnost običajno ocenjuje strokovnjak z raziskovalnega področja. Ocenjuje jo na podlagi pregledane literature (Straub, et al., 2004). V naši raziskavi je vsebinska veljavnost zagotovljena z uporabo predhodno uporabljenih merilnih elementov, s pregledom obstoječe literature ter s pregledom elementov vprašalnika s strani strokovnjakov s področja informacijske varnosti ter zaposlenih v zdravstveni negi. Vsebinsko veljavnost vprašalnika smo zagotovili tudi z uporabo besednih zvez intervjuvancev (priloga 2). Tako smo preprečili morebitno

napačno razumevanje na strani anketiranih zaposlenih v zdravstveni negi. Četudi je bila večina merilnih elementov vprašalnika prevedena iz že prej validiranih raziskav, smo zaradi postopka prevoda iz angleškega v slovenski jezik, izvedli pred-test vprašalnika. Vprašalnik sta neodvisno eden od drugega pregledala raziskovalca in strokovnjaka za področje informatike in informacijske varnosti, ki v postopku prevajanja nista sodelovala. Omenjena strokovnjaka sta vprašalnik pregledala s fokusom na teoretičnem in praktičnem dizajnu. Vsi njuni predlogi in izboljšave so bili upoštevani. Novo nastala različica vprašalnika je bila nato dana v pregled in izpolnjevanje štirim medicinskih sestram, zaposlenim v eni izmed bolnišnic na Primorskem. Prosili smo jih, da identificirajo kakršne koli dvoumne besedne zveze, ki bi utegnile ustvariti dvom pri udeležencih raziskave. Ocena vprašalnika je bila podana ustno, s pisnimi opombami na papirnato različico vprašalnika. Opravljena je bila diskusija o vsakem posameznem elementu vprašalnika. Vsi vložki tega procesa so bili izvedeni z namenom izboljšanja merilnih elementov pred samo izvedbo glavne oz. osrednje raziskave. Vprašalnik je na voljo v Prilogi 4.

3.3.4 Pilotno testiranje

Zaradi preobširnosti vprašalnika smo testirali le del vprašalnika za merjenje konstruktov TPB (razen NB) in novo razvita konstrukta SO in PO ter tri scenarije. Zbiranje podatkov je trajalo od 3. 3. do 11. 6. 2020. Pilotno testiranje je bilo opravljeno pri izrednih študentih zdravstvene nege na eni od zdravstvenih fakultet v Sloveniji. Anketa je bila izvedena v papirnati in spletni obliki. Izpolnjenih papirnih anket je bilo 83, elektronskih pa 110. Vzorec je štel 193 študentov. Prečiščeni podatki so dali n = 155 enot vzorca vključenih študentov.

Faktorska analiza podatkov pilotne raziskave je pokazala, da je potrebno izključiti dva elementa konstrukta SO. Prav tako smo iz vprašalnika za glavno raziskavo izključili dva dodatna scenarija.

3.3.5 Faktorske analize

Ena od metod za razvoj in ocenjevanje kakovosti merjenja je eksploratorna faktorska analiza (angl. »*Exploratory Factor Analysis*« – v nadaljevanju EFA), ki jo uporabljamo za redukcijo in preučevanje teoretičnih struktur psiholoških pojavov. Njen cilj je identifikacija niza latentnih konstruktov iz velikega števila posameznih spremenljivk (elementov), rezultat pa zanesljive in veljavne merske lestvice (Hair, et al., 2020). To metodo običajno uporabljamo, kadar nimamo predhodnih hipotez o obstoječih faktorjih ali vzorcih merjenih spremenljivk in imamo zato veliko število opazovanih spremenljivk, za katere domnevamo, da so povezane z manjšim številom »neopazovanih« faktorjev (Brown, 2015; Kline, 2015).

Konfirmativno ali potrditveno faktorsko analizo (angl. »*Confirmatory Factor Analysis*«, v nadaljevanju CFA) so v preteklosti raziskovalci uporabljali za razvijanje in izboljševanje reflektivno merjenih konstruktov. CFA raziskovalcem omogoča ovrednotenje konstruktov z večjim naborov elementov in je smiselna takrat, ko že obstaja teorija o odnosih med posameznimi spremenljivkami in o tem, kako so povezane s teoretičnimi koncepti (Hair, et al., 2020).

V primerjavi s CFA je potrditvena kompozitna analiza (angl. »*Confirmatory Composite Analysis*«, v nadaljevanju CCA) nedavno predlagani alternativni pristop, ki se uporablja za potrjevanje merilnega modela pri uporabi metode PLS-SEM (modeliranje strukturnih enačb z metodo delnih najmanjših kvadratov, angl. »*Partial least squares Structural Equation Modeling*«). CCA vključuje več korakov za potrjevanje tako reflektivnih kot tudi formativnih merilnih modelov. Z njeno uporabo se preizkušajo hipoteze, da obstaja teoretična povezava med opazovanimi spremenljivkami in njihovimi osnovnimi latentnimi konstrukti. Njen cilj je potrjevanje merskih lastnosti spremenljivk (indikatorjev) za merjenje določenega in operativno definiranega latentnega konstrukta (Hair, et al., 2020).

Pri CCA je pomembno razumeti da so reflektivni merilni modeli sestavljeni latentni konstrukti, katerih elementi (merjene spremenljivke) naj bi bili pod vplivom osnovne

latentne spremenljivke, na katere vpliva ali jih povzroča (Sarstedt, et al., 2016). Sprememba latentnega konstrukta se tako odraža v spremembi vseh njegovih indikatorjev. Indikatorji so manifestacija empiričnih nadomestkov (nadomestnih spremenljivk, angl. »*proxy variables*«) za latentno spremenljivko (Hair, et al., 2020).

Za izvedbo CCA za reflektivni merilni model je potrebno upoštevati (Hair, et al., 2020):

- indikatorske obremenitve in njihove statistične značilnosti,
- zanesljivost indikatorjev (elementov),
- sestavljeno zanesljivost (konstrukt),
- povprečje izločenih varianc (angl. »*Average Variance Extracted*«, v nadaljevanju AVE),
- diskriminantno veljavnost (angl. »*the heterotrait-monotrait ratio of the correlation*s«, v nadaljevanju HTMT),
- nomološko veljavnost in
- napovedno veljavnost.

Cilj EFA je redukcija podatkov, medtem ko je cilj CCA in CFA potrditev teorije. EFA se pogosto zaključi z identifikacijo faktorjev, medtem ko CCA in CFA začneta s predlaganjem teoretičnih konstruktov, ki jih je treba potrditi, in skoraj vedno preideta na strukturno modeliranje, potem ko so bili merilni modeli potrjeni (Hair, et al., 2020). Izbira med CCA in CFA je globoko prepletena z izbiro PLS-SEM ali CB-SEM (modeliranje strukturnih enačb, ki temelji na kovariančni matriki, angl. »*A Structural Equation Modeling Based on the Covariance matrix*«).

EFA (metoda glavnih komponent, rotacija varimaks) TPB konstruktov nakazuje prisotnost petih faktorjev. Od tega spremenljivke konstruktov ATB kažejo pozitivno nasičenost izključno na faktor 2, spremenljivke konstrukta SN na faktor 4, spremenljivke konstrukta PBC na faktor 1, spremenljivke konstrukta BI na faktor 3, spremenljivke konstrukta NB na faktor 5. Pri spremenljivki SN3 smo identificirali manjše težave, in sicer nizko nasičenost faktorske uteži > 0,7 (0,659) (tabela 6). Identificiranih 5 faktorjev pojasni kar 86,689 % variance. Vrednost Kaiser-Meyer-Olkin (v nadaljevanju KMO) merila za konstrukte TPB znaša 0,886, kar je precej nad najmanjšo sprejemljivo ravnjo,

t.j. 0,50 (Tabachnick & Fidell, 2018). Bartlettov test sferičnosti za konstrukte je statistično značilen ($p < 0,001$), kar nakazuje na obstoj ustreznih odnosov med spremenljivkami, vključenimi v analizo (priloga 5).

Tabela 6: EFA za TPB konstrukte

Element	Faktor					
	1	**2**	**3**	**4**	**5**	**Komunalitete**
ATB1		0,839				0,831
ATB2		0,847				0,887
ATB3		0,817				0,831
SN1				0,864		0,878
SN2				0,853		0,904
SN3				0,659		0,678
PBC1	0,912					0,883
PBC2	0,935					0,912
PBC3	0,919					0,881
BI1			0,822			0,925
BI2			0,826			0,929
BI3			0,822			0,924
NB1					0,728	0,819
NB2					0,778	0,807
NB3					0,865	0,914
Lastna vrednost	2,752	2,748	2,591	2,474	2,439	
% variance	18,349	18,320	17,273	16,490	16,257	
Kumulativni %	18,349	36,669	53,942	70,432	86,689	

Metoda ekstrakcije faktorjev: PCA; metoda rotacije: Varimax with Kaiser Normalization; konvergiralo v šestih iteracijah.

EFA (metoda glavnih osi, rotacija varimaks) dimenzij informacijske varnostne kulture nakazuje prisotnost desetih faktorjev, od tega spremenljivke konstrukta PCM kažejo pozitivno nasičenost izključno na faktor 5, spremenljivke konstrukta TMC na faktor 4; spremenljivke konstrukta ISK na faktor 6 in spremenljivke konstrukta ISKS na faktor 2, spremenljivke konstrukta MON na faktor 7 in spremenljivke konstrukta RM na faktor 8. Identificirane so težave pri spremenljivkah konstrukta SETA, ki kažejo nasičenost na dva faktorja, in sicer 9 (SETA 1 in 2) in 10 (SETA 3 in 4). Pri spremenljivkah PCM (1, 3, 4), RM (1, 2, 3), SETA (3, 4) TMC (4), MON (1), ISK (1), PO (5), in SO (1, 2, 5) smo identificirali težave, in sicer nizko nasičenost faktorske uteži > 0,7. Najmanjša nasičenost faktorske uteži med naštetimi je pri RM3 (0,592) (tabela 7).

Identificiranih deset komponent pojasni kar 82,365 % variance. Kljub nekaterim nizkim nasičenostim, spremenljivk nismo odstranili iz nadaljnje analize, saj je bila nasičenost faktorjev ustrezna (≥ 0,50) (Tabachnick & Fidell, 2018).

Vrednost KMO merila za dimenzije informacijske varnostne kulture znaša 0,952, kar je tudi nad najmanjšo sprejemljivo ravnjo, t.j. 0,50 (Tabachnick & Fidell, 2018). Bartlettov test sferičnosti za konstrukte je statistično značilen ($p < 0,001$), kar nakazuje na obstoj ustreznih odnosov med spremenljivkami, vključenimi v analizo (priloga 6).

Tabela 7: EFA za dimenzije informacijske varnostne kulture

	1	2	3	4	5	6	7	8	9	10	Kom.
PCM1					0,677						0,675
PCM2					0,764						0,847
PCM3					0,684						0,744
PCM4					0,636						0,740
RM1								0,625			0,767
RM2								0,675			0,866
RM3								0,592			0,805
SETA1									0,791		0,973
SETA2									0,708		0,883
SETA3										0,641	0,900
SETA4										0,632	0,829
TMC1				0,745							0,904
TMC2				0,782							0,954
TMC3				0,740							0,918
TMC4				0,640							0,799
MON1							0,645				0,847
MON2							0,706				0,878
MON3							0,756				0,906
ISK1						0,660					0,751
ISK2						0,785					0,887
ISK3						0,722					0,836
ISKS1		0,698									0,766
ISKS2		0,724									0,848
ISKS3		0,737									0,805
ISKS4		0,797									0,893
PO1	0,859										0,802
PO2	0,883										0,844
PO3	0,805										0,806
PO4	0,866										0,872
PO5	0,690										0,650
SO1			0,697								0,795
SO2			0,695								0,782
SO3			0,783								0,890
SO4			0,735								0,774
SO5			0,609								0,590
Lastna vrednost	4,501	3,766	3,743	3,525	3,116	2,597	2,497	2,009	1,774	1,300	
% variance	12,860	10,759	10,696	10,070	8,902	7,419	7,134	5,741	5,069	3,715	
Kumul-ativni%	12,860	23,619	34,315	44,385	53,287	60,705	67,839	73,581	78,650	82,365	

Metoda ekstrakcije faktorjev: PAF; metoda rotacije: Varimax with Kaiser Normalization.; konvergiralo v osmih iteracijah.
Kom. – komunalitete

CCA nakazuje prisotnost štirinajstih faktorjev (tabela 8).

Tabela 8: CCA z metodo PLS-SEM

Element	Faktor				
	1	**2**	**3**	**4**	**5**
ATB1	0,857				
ATB2	0,906				
ATB3	0,883				
SN1		0,826			
SN2		0,867			
SN3		0,849			
NB1			0,811		
NB2			0,853		
NB3			0,913		
PBC1				0,990	
PBC2				0,912	
PBC3				0,838	
BI1					0,944
BI2					0,942
BI3					0,942
	6	**7**	**8**	**9**	**10**
PCM1	0,934				
PCM2	1,085				
PCM3	0,666				
PCM4	0,564				
RM1		0,924			
RM2		1,006			
RM3		0,757			
SETA1			0,974		
SETA2			0,859		
SETA3			0,862		
SETA4			0,664		
TMC1				0,941	
TMC2				0,941	
TMC3				0,918	
TMC4				0,967	
MON1					0,968
MON2					0,965
MON3					0,862
	11	**12**	**13**	**14**	
ISK1	0,990				
ISK2	0,936				
ISK3	0,762				
ISKS1		1,042			
ISKS2		0,935			
ISKS3		0,750			
ISKS4		0,858			
PO1			0,824		
PO2			0,870		
PO3			0,984		
PO4			0,976		
PO5			0,708		
SO1				0,880	
SO2				0,903	
SO3				0,934	
SO4				0,930	
SO5				0,687	

Od tega spremenljivke konstrukta SN kažejo pozitivno nasičenost izključno na faktor 12; spremenljivke konstrukta PBC na faktor 7; spremenljivke konstrukta BI na faktor 2 in spremenljivke konstrukta NB na faktor 6. Spremenljivke konstrukta PO kažejo pozitivno nasičenost izključno na faktor 9; spremenljivke konstrukta SO na faktor 13. Pri spremenljivki SO5 smo identificirali manjše težave, in sicer nizko nasičenost faktorske uteži > 0,7 (0,687). Nasičenost izključno na faktor 8 kažejo spremenljivke konstrukta PCM, vendar smo tudi pri tej identificirali manjše težave, in sicer faktorske uteži < 0,7, pri spremenljivki PCM3 (0,666) in PCM4 (0,564). Spremenljivke konstrukta RM kažejo izključno pozitivno nasičenost na faktor 10; spremenljivke konstrukta SETA na faktor 11. Tudi pri SETA smo identificirali manjše težave, saj ima spremenljivka SETA 4 nizko nasičenost faktorske uteži, in sicer 0,664. Spremenljivke konstrukta TMC kažejo izključno pozitivno nasičenost na faktor 14; spremenljivke konstrukta MON na faktor 5; ISK na faktor 2, ISKS na faktor 4 in ATB na faktor 1. Kljub nekaterim nizkim nasičenostim spremenljivk slednjih nismo odstranili iz nadaljnje analize, saj kot navaja Wong (2019), je najmanjša še sprejemljiva vrednost 0,4.

Korelacije med latentno spremenljivko in elementi so v primeru reflektivnega modela prikazani za zunanji model (angl. »outer loadings«).

3.3.6 Zanesljivost in veljavnost vprašalnika

Kakovost merilnega modela se običajno ocenjuje glede na njegovo vsebinsko in konstruktno veljavnost ter zanesljivost (Hulland, 1999; Straub, et al., 2004). Ker smo v tej doktorski disertaciji uporabili dve orodji – SPSS in SmartPLS, smo pri obeh izvedli preverjanje zanesljivosti in veljavnosti.

Prvi korak pri oceni reflektivnega merilnega modela vključuje pregled *faktorskih uteži* (priloga 7). Vrednosti nad 0,70 so priporočljive, saj kažejo, da konstrukt pojasnjuje več kot 50 % variance, kar zagotavlja sprejemljivo zanesljivost elementov (Hair, et al., 2019a).

Drugi korak za oceno reflektivnega merilnega modela zadeva merilo *notranje skladnosti*, ki ocenjuje stopnjo, do katere so odgovori skladni z elementi vprašalnika (Kline, 2015).

Zanesljivost meritev obravnava vprašanje, kako dobro elementi konstukta korelirajo med seboj (Straub, et al., 2004). Zanesljivost običajno ocenjujemo z dvema kazalnikoma: a) Crombach alfa (CA) ter b) Jöreskogovo (1971) *sestavljeno zanesljivostjo* ali Composite Reliability (CR). CA je merilo notranje skladnosti (angl. »*internal consistency*«) med vsemi elementi, ki se uporabljajo za en konstrukt. CR zadeva podoben koncept, vendar velja za strožje merilo zanesljivosti v kontekstu PLS-SEM (Chin, 1998; Raykov, 1998). Višje vrednosti CR pomenijo višjo stopnjo zanesljivosti. Vrednosti med 0,60 in 0,70 veljajo za sprejemljive v eksploratornih raziskavah, vrednosti med 0,70 in 0,90 pa zadovoljive oz. dobre. Vrednosti 0,95 in višje so problematične, saj nakazujejo, da so elementi odveč in s tem zmanjšujejo veljavnost konstrukta (Diamantopoulos, et al., 2012).

Tretji korak ocene reflektivnega merilnega modela obravnava *konvergentno veljavnost*, ki se nanaša na obseg do katerega merilni element pozitivno korelira z alternativnim elementom enakega konstrukta. Konvergentna veljavnost je obseg, do katerega konstrukt konvergira, da pojasni varianco svojih postavk. Metrika, ki se uporablja za ocenjevanje konvergentne veljavnosti konstrukta je AVE za vse elemente v vsakem konstruktu ter faktorske uteži z mejo 0,70. Sprejemljiva vrednost AVE je 0,50 ali več, kar pomeni, da konstrukt pojasnjuje vsaj 50 % variance svojih elementov (Hair, et al., 2019a).

Kazalniki zanesljivosti konstruktov v naši raziskavi so prikazani v Tabeli 9. V Prilogi 8 so natančneje prikazane vrednosti CA vsakega elementa posebej. Najnižja CR znaša 0,885, CA pa 0,884, pri čemer so vse vrednosti višje od priporočene minimalne vrednosti, t.j. 0,7 za CA (Bagozzi & Yi, 1988; Gefen, et al., 2000), in višja od 0,80 za CR (Chin, 2010). Rezultati kažejo, da so meritve pri merjenju vseh konstruktov zanesljive. Iz Tabele 9 je razvidno, da so vrednosti faktorskih uteži pri štirih elementih pod 0,70 (najmanjša znaša 0,564 za PCM4) in da AVE za vsak konstrukt presega 0,50 (Hair, et al., 2013), kar kaže, da je konvergentna veljavnost za vse elemente konstruktov sprejemljiva.

Tabela 9: Rezultati veljavnosti in zanesljivosti

Element	Uteži	CA	CR (rho_a)	CR (rho_c)	AVE
ATB1	0,857				
ATB2	0,906	0,913	0,914	0,913	0,778
ATB3	0,883				
SN1	0,826				
SN2	0,867	0,884	0,885	0,884	0,719
SN3	0,849				
NB1	0,811				
NB2	0,853	0,893	0,897	0,894	0,739
NB3	0,913				
PBC1	0,990				
PBC2	0,912	0,939	0,945	0,939	0,838
PBC3	0,838				
BI1	0,944				
BI2	0,942	0,960	0,960	0,960	0,889
BI3	0,942				
PCM1	0,934				
PCM2	1,085	0,903	0,956	0,899	0,703
PCM3	0,666				
PCM4	0,564				
RM1	0,924				
RM2	1,006	0,926	0,943	0,928	0,813
RM3	0,757				
SETA1	0,974				
SETA2	0,859	0,909	0,924	0,909	0,717
SETA3	0,862				
SETA4	0,664				
TMC1	0,941				
TMC2	0,941	0,969	0,969	0,969	0,887
TMC3	0,918				
TMC4	0,967				
MON1	0,968				
MON2	0,965	0,952	0,956	0,952	0,870
MON3	0,862				
ISK1	0,990				
ISK2	0,936	0,927	0,941	0,928	0,812
ISK3	0,762				
ISKS1	1,042				
ISKS2	0,935	0,947	0,959	0,945	0,814
ISKS3	0,750				
ISKS4	0,858				
PO1	0,824				
PO2	0,870				
PO3	0,984	0,943	0,953	0,943	0,771
PO4	0,976				
PO5	0,708				
SO1	0,880				
SO2	0,903				
SO3	0,934	0,939	0,947	0,940	0,760
SO4	0,930				
SO5	0,687				

Četrti korak je ocena diskriminantne veljavnosti, ki se nanaša na obseg, v katerem se konstrukti razlikujejo od drugih. Za testiranje diskriminantne veljavnosti poznamo številne tehnike (Straub, et al., 2004). Na stopnji elementov jo ocenjujemo z analiziranjem uteži elementov, na konstruktnem nivoju pa se diskriminantna veljavnost analizira s primerjavo korelacij med konstrukti in kvadratnim korenom AVE vsakega posameznega konstrukta (Fornell & Larcker, 1981; Hulland, 1999). Gre za obseg, v katerem se konstrukt empirično razlikuje od drugih konstruktov v strukturnem modelu. Fornell in Larcker (1981) trdita, da je potrebno AVE vsakega konstrukta primerjati s kvadratom korelacije med konstrukti (kot merilo skupne variance) istega konstrukta in vseh drugih reflektivno izmerjenih konstruktov v strukturnem modelu. Diskriminantna veljavnost je podprta, v kolikor je kvadratni koren konstruktov AVE višji od korelacije konstruktov z vsemi drugimi konstrukti (Fornell & Larcker, 1981; Hulland, 1999). Tabela 10 prikazuje Fornell-Lackerjev kriterij. Kvadratni koren vsake AVE je večji kot absolutna vrednost korelacije med konstrukti, kar nakazuje na dobro diskriminantno veljavnost za vse konstrukte v merilnem modelu.

Kot zamenjavo Fornell-Larckerjevevemu kriteriju, Henseler, et al. (2015) ter Voorhees, et al. (2016) predlagajo izvedbo izračuna razmerja korelacij med in znotraj konstruktov, t.j. HTMT. Ta je opredeljen kot povprečna vrednost korelacij elementov med konstrukti glede na geometrično sredino povprečnih korelacij za elemente, ki merijo isti konstrukt. V kolikor so vrednosti HTMT testa pod 0,90, velja, da je diskriminantna veljavnost vzpostavljena med dvema konstruktoma. Težave z diskriminantno veljavnostjo so prisotne, ko so vrednosti HTMT visoke. Henseler, et al. (2015) predlagajo mejno vrednost 0,90 za strukturne modele s konstrukti, ki so konceptualno zelo podobni (npr. kognitivno zadovoljstvo, afektivno zadovoljstvo in lojalnost). V takšnem primeru vrednost HTMT nad 0,90 pomeni, da diskriminantna veljavnost ni prisotna. Ko pa so konstrukti konceptualno bolj različni, je predlagana nižja in konzervativnejša vrednost praga, to je 0,85 (Henseler, et al., 2015). Iz Tabele 11 je razvidno, da je v našem primeru diskriminantna veljavnost vzpostavljena.

Tabela 10: Fornell-Lackerjev kriterij

	ATB	BI	ISK	ISKS	MON	NB	PBC	PCM	PO	RM	SETA	SN	SO	TMC
ATB	0,882													
BI	0,674	0,943												
ISK	-0,109	-0,145	0,901											
ISKS	-0,057	-0,137	0,697	0,902										
MON	-0,071	-0,134	0,730	0,716	0,933									
NB	0,619	0,713	-0,210	-0,203	-0,211	0,859								
PBC	0,290	0,386	-0,147	-0,092	-0,121	0,328	0,915							
PCM	-0,166	-0,168	0,570	0,558	0,590	-0,247	-0,105	0,839						
PO	-0,260	-0,195	0,304	0,386	0,282	-0,343	-0,083	0,471	0,878					
RM	-0,063	-0,108	0,666	0,644	0,749	-0,238	-0,088	0,689	0,349	0,902				
SETA	-0,122	-0,171	0,663	0,734	0,719	-0,297	-0,172	0,689	0,411	0,769	0,847			
SN	0,646	0,661	-0,146	-0,177	-0,168	0,711	0,327	-0,219	-0,265	-0,168	-0,215	0,847		
SO	-0,164	-0,226	0,484	0,594	0,495	-0,406	-0,099	0,591	0,696	0,555	0,648	-0,294	0,872	
TMC	-0,122	-0,148	0,711	0,720	0,745	-0,237	-0,152	0,648	0,385	0,752	0,745	-0,187	0,589	0,942

Tabela 11: HTMT (razmerja korelacij med in znotraj konstrukti)

	ATB	BI	ISK	ISKS	MON	NB	PBC	PCM	PO	RM	SETA	SN	SO	TMC
ATB														
BI	0,674													
ISK	0,105	0,142												
ISKS	0,055	0,136	0,709											
MON	0,070	0,134	0,736	0,721										
NB	0,619	0,714	0,210	0,201	0,211									
PBC	0,290	0,386	0,148	0,093	0,121	0,328								
PCM	0,154	0,158	0,597	0,586	0,627	0,244	0,109							
PO	0,259	0,193	0,307	0,390	0,283	0,342	0,082	0,478						
RM	0,063	0,107	0,679	0,658	0,759	0,238	0,089	0,733	0,354					
SETA	0,120	0,169	0,678	0,749	0,731	0,292	0,178	0,722	0,410	0,785				
SN	0,646	0,660	0,144	0,176	0,169	0,713	0,327	0,212	0,263	0,167	0,211			
SO	0,163	0,224	0,493	0,601	0,498	0,406	0,103	0,608	0,701	0,563	0,653	0,292		
TMC	0,122	0,148	0,717	0,723	0,746	0,237	0,152	0,676	0,387	0,763	0,757	0,187	0,590	

3.4 POTEK RAZISKAVE IN SOGLASJA

Raziskava je potekala v petih delih. Pri tem smo se oprli na proces, ki sta ga opredelila Polit in Beck (2008). V prvem delu (koncept raziskave) smo pregledali obstoječo literaturo, oblikovali in omejili raziskovalni problem, izvedli preliminarno kvalitativno raziskavo, definirali pojme, spremenljivke ter raziskovalne cilje in hipoteze. V drugem delu smo izbrali raziskovalni dizajn, izdelali načrt, dopolnili že obstoječi merski instrument, identificirali populacijo, izdelali načrt vzorčenja, specifikacijo metode za merjenje spremenljivk, razvili protokol za zaščito podatkov, pridobljenih med raziskavo (priloga 9) in dopolnili raziskovalni načrt. V tretjem, empiričnem delu je potekalo zbiranje podatkov (tudi pilotno testiranje). V četrtem, analitičnem delu smo analizirali podatke in se opredelili do zastavljenih hipotez. V petem, zadnjem delu, tj. razširitev podatkov, smo razpravljali o dobljenih rezultatih in le-te predstavili javnosti na 14. Kongresu zdravstvene in babiške nege Slovenije.

Za izvedbo raziskave smo pridobili naslednja soglasja:

- za izvedbo preliminarne kvalitativne raziskave (priloga 2), z dne 11. 11. 2019;
- udeležencev v preliminarni kvalitativni raziskavi (za izvedbo in snemanje intervjuja) (priloga 2);
- Zbornice zdravstvene in babiške nege Slovenije – Zveze strokovnih društev medicinskih sester, babic in zdravstvenih tehnikov Slovenije (v nadaljevanju Zbornica – Zveza) za sodelovanje v raziskavi (priloga 10), z dne 22. 5. 2020, sklep št. UO 615/45;
- Komisije RS za medicinsko etiko (priloga 11), z dne 25. 2. 2021, št. 0120-583/2020/7;
- primarnih avtorjev merskega instrumenta (priloga 12), z dne 15. 11. 2019.

Zbornica – Zveza je posredovala e-novice, skupaj s povezavo do spletne ankete, na več kot 12.000 elektronskih naslovov. Cilj je bil povezavo do spletne ankete deliti med čim večje število zaposlenih v zdravstveni negi. Povezava do spletne ankete je bila posredovana v sklopu e-novic, sedemkrat. Povabilo do sodelovanja v raziskavi je bilo objavljeno tudi v informativnem biltenu Utrip (Mikuletič, 2021). Zbornica – Zveza je dvakrat posredovala poziv k sodelovanju v raziskavi preko elektronskega sporočila

zdravstvenim ustanovam in povezavo do spletne ankete objavila na svojem socialnem omrežju Facebook. Prošnjo za sodelovanje smo posredovali vsem regijskim društvom, ki delujejo pod okriljem Zbornice – Zveze. Od enajstih sta se odzvala dva in anketo objavila na svoji spletni strani. Zbiranje podatkov je potekalo v več etapah od aprila 2021 do marca 2022. Časovni potek zbiranja podatkov je prikazan v Tabeli 12.

Tabela 12: Časovni potek zbiranja podatkov

Datum objave	Način objave
6. 4. 2021	e-novice št. 83, april 2021
12. 4. 2021	e-novice št. 84, april 2021
21. 4. 2021	e-novice št. 85, april 2021
7. 5. 2021	e-novice št. 86, maj 2021
24. 5. 2021	e-novice št. 88, maj 2021
24. 5. 2021	Objava poziva k sodelovanju v raziskavi, skupaj s povezavo do spletne ankete na socialnem omrežju Facebook (objava Zbornice – Zveze).
Junij	Zbornica – Zveza posredovala zdravstvenim ustanovam zaprosilo za sodelovanje
Junij–julij 2021	Objava poziva k sodelovanju v raziskavi, skupaj z navedbo dostopa do spletne ankete v reviji Utrip (junij–julij 2021) na strani 29.
2. 8. 2021	Poslana prošnja za sodelovanje v raziskavi društvom, ki delujejo pod okriljem Zbornice–Zveze. Potrdili Ljubljana in Koroška.
8. 10. 2021	Objava poziva k sodelovanju v raziskavi, skupaj s povezavo do spletne ankete na socialnem omrežju Facebook (objava Zbornice–Zveze).
11. 10. 2021	e-novice št. 96, oktober 2021
29. 10. 2021	e-novice št. 97, oktober 2021

3.5 OBDELAVA PODATKOV

Argumentacijo za izbiro analiz in interpretacijo podatkov smo v nadaljevanju, v podpoglavju *Obdelava podatkov* in poglavju *Rezultati*, zaradi kompleksnosti predstavili ločeno. Podatke pridobljene z vprašalnikom smo analizirali s statističnim orodjem IBM SPSS Statistics 22.0 (IBM Software Group, 2013) in SmartPLS 4.0.8.3 (Ringle, et al., 2022).

3.5.1 Izvedene statistične analize

Za analizo zbranih podatkov in ugotavljanje različnih zvez med njimi smo uporabili naslednje opisne statistične analize: predstavitev velikosti vzorca (N), odstotke (%), frekvence (f), minimalne (Min), maksimalne (Max) in srednje vrednosti. V nadaljevanju smo uporabili inferenčne statistične analize, s katerimi smo ocenili in preverili naše domneve in hipoteze.

Najprej smo izvedli univariatno analizo podatkov (izračun frekvenc, relativnih frekvenc, povprečja (M), standardnih odklonov (SD), mediane (M_E), kvartilov oz. interkvartilnega ranga – IQR). Preverili smo koeficient asimetrije (angl. »*skewness*« – KA) in sploščenosti (angl. »*kurtosis*« – KS) ter porazdelitve podatkov preverili tudi grafično, s pomočjo diagrama škatla z brki. Rezultati so pokazali, da podatki odstopajo od normalne porazdelitve, zato smo v nadaljevanju uporabili neparametrične teste, ki jih imata na voljo obe omenjeni orodji. Za preverjanje hipotez H1–H6 smo uporabili program SmartPLS 4.0.8.3, medtem ko smo za preverjanje hipoteze H7 (a, b, c, d, e in f) uporabili IBM SPSS Statistics 22.0, kjer smo preverjali razlike v zaznavanju dimenzij informacijske varnostne kulture glede na starost, delovno dobo, spol, stopnjo izobrazbe, organizacijo zaposlitve in raven zdravstvenega varstva, v katerem so zaposleni respondenti (Mann-Whitneyev U test, Kruskal-Wallisov H test). V sklopu multivariatne statistične analize smo izvedli faktorsko analizo.

Metoda ponovnega vzorčenja (angl. »*Bootstrap*« ali »*Bootstrapping*«), ki jo izvaja program SmartPLS 4.0.8.3 je neparametrični postopek, ki omogoča preverjanje statistične pomembnosti različnih rezultatov ter ocene statističnih parametrov iz katerih lahko ocenimo intervale zaupanja, pridobljene z metodo PLS-SEM. Namen metoode ponovnega vzorčenja, kot že pove njeno ime, je ponovno vzorčenje podatkov znotraj naključnega vzorca. Pri bootstrappingu se ustvarijo podvzorci z naključno izbranimi opazovanji iz prvotnega nabora podatkov. Podvzorec (angl. »*subsamples*«) se nato uporabi za oceno PLS poti modela. Ta postopek se ponavlja, dokler ni ustvarjen velik nabor naključnih podvzorcev (Ringle, et al., 2022). Začetna nastavitev pred obdelavo podatkov naloge je 5.000 podvzorcev. Ostale nastavitve analiz v programu SmartPLS 4.0.8.3 so prikazane v Tabeli 13.

Tabela 13: Nastavitve analiz v programu SmartPLS 4.0.8.3

Analiza	Nastavitve
CCA	*PLS-SEM algorithm: initial weights – 1.0; max. number of iterations – 3000; stop criterion - 10^{-7}; use Lohmoeller settings – no; weighting scheme – factor, stop criterion changes: algorithm converged in 6 iterations.*
Merilni model	*PLS-SEM algorithm: initial weights – 1.0; max. number of iterations: 3000; stop criterion:10^{-7}; type of results: standardized; Lohmoeller settings? No; weighting scheme: factor.*

Analiza	Nastavitve
Izločitev spremenljivke družbena zaželjenost ter učinek kontrolnih spremenljivk	*Consistent PLS-SEM algorithm: initial weights – 1.0; max. number of iterations – 3000; stop criterion - 10^{-7}; use Lohmoeller settings – no; weighting scheme – path.* *Consistent PLS-SEM algorithm, bootstrapping: complexity – most important (faster); confidence interval method – percentile bootstrap; parallel processing – yes; samples – 5000; seed - fixed seed; significance level – 0.05; test type – two tailed.*
PLSpredict	*No. of repetitions – 10; number of folds – 10; seed – fixed seed.*
Strukturni model	*Consistent PLS-SEM algorithm settings: initial weights – 1.0; max. number of iterations – 3000; stop criterion – 10^{-7}; type of results – standardized; Lohmoeller settings? – no; weighting scheme – path.* *Consistent PLS-SEM algorithm, bootstrapping: complexity – most important (faster); confidence interval method – percentile bootstrap; parallel processing – yes; samples – 5000; seed – fixed seed; significance level – 0.05; test type – two tailed.*

3.5.2 SEM in PLS-SEM

Kombiniranje elementov faktorske analize, regresijske analize in elementov analize poti združujemo v metodo, znano pod imenom SEM. Gre za multivariatno tehniko, ki obravnava kompleksne probleme, ki vključujejo analiziranje endogenih in eksogenih spremenljivk in daje oceno hipotetičnih povezav med spremenljivkami v teoretičnem modelu (Milfelner, et al., 2006).

Za opravljanje analiz, ki temeljijo na SEM je na voljo več orodij. V nadaljevanju je podrobneje razdelana metoda, ki smo jo uporabili za analiziranje podatkov v doktorski disertaciji.

Švedski ekonometrik Herman Wold (1975, 1982) je kot prvi razvil statistično podlago za PLS-SEM. Metoda je bila dolgo poznana in jo včasih še vedno poimenujejo »*PLS path modeling*« (Hair, et al., 2011). Model strukturnih enačb omogoča specifikacijo zapletenih medsebojnih odnosov med opazovanimi in latentnimi spremenljivkami.

Pristop z uporabo metode PLS-SEM (Khan, et al., 2019; Hwang, et al., 2020) je pred kratkim pridobil množično uporabo v poslovnih raziskavah in drugih znanstvenih področjih (Sarstedt, 2019). PLS-SEM se obravnava kot alternativa Jöreskogovem (1971) CB-SEM-u (Hair, et al., 2011).

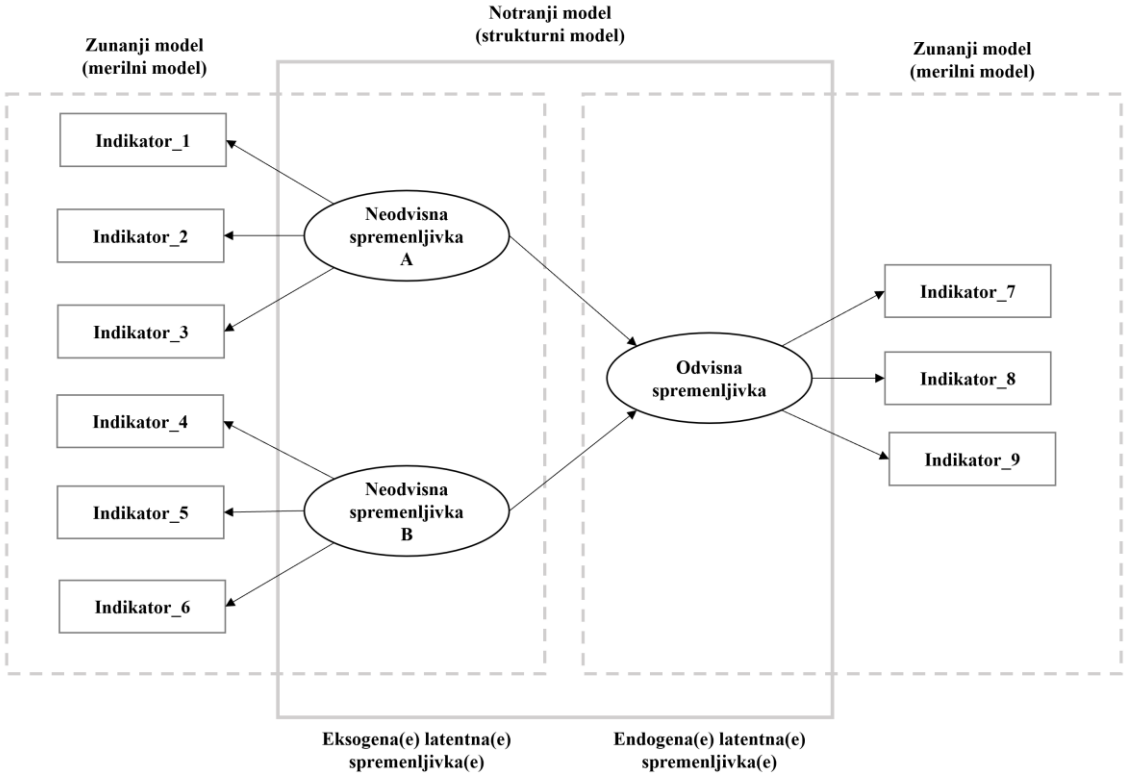
Uporaba PLS-SEM je za številne raziskovalce zelo privlačna, saj omogoča ocenjevanje zapletenih modelov s številnimi konstrukti, spremenljivkami in strukturnimi potmi, ne glede na to, kakšna je porazdelitev podatkov. Še pomembneje pa je, da je PLS-SEM vzročno-napovedni pristop, ki poudarja napovedovanje pri ocenjevanju statističnih modelov, katerih strukture so zasnovane tako, da zagotavljajo vzročne razlage (Hair, et al., 2019b).

V zadnjem desetletju je potekala precejšnja razprava o tem, katere situacije so bolj ali manj primerne za uporabo PLS-SEM metode (Marcoulides, et al., 2009, 2012; Goodhue, et al., 2012; Henseler, et al., 2014; Rigdon, 2014a; Khan, et al., 2019). Hair, et al. (2019a) so podali sklop priporočil. PLS-SEM je primeren, ko:

- želimo z analizo testirati teoretični okvir z vidika napovedi;
- je strukturni model zapleten in vključuje številne konstrukte, indikatorje in/ali povezave v modelu;
- je cilj bolje razumeti naraščajočo kompleksnost z raziskovanjem teoretičnih razširitev že poznanih teorij (eksplorativna raziskava za nadgradnjo teorije);
- v modelu je en ali več formativno merjenih konstruktov;
- raziskava temelji na sekundarnih ali arhivskih podatkih in le-ta nima celovite teoretične zasnove;
- imamo na voljo majhno populacijo oz. ko njena velikost omejuje velikost samega vzorca (npr. raziskave znotraj podjetij);
- se pojavljajo težave s porazdelitvijo podatkov.

3.5.3 Smernice za uporabo PLS-SEM

Kot večina statističnih metod, ima tudi PLS-SEM osnovna pravila, ki služijo kot smernice za vrednotenje rezultatov modela. Pri analizi rezultatov smo sledili smernicam za opisovanje merilnega in strukturnega modela z reflektivnimi konstrukti (Hair, et al., 2019a; Wong, 2019; Sarstedt, et al., 2021). Da bi lažje razumeli komponente PLS-SEMa, smo le-te predstavili na Sliki 10.



Slika 10: Komponente PLS-SEM: notranji (strukturni) in zunanji (merilni model)
(Wong, 2019)

V prvem koraku, ki se nanaša na *Predhodna vprašanja, povezana z vidiki uporabe PLS-SEM*, smo izračunali ustrezno velikost vzorca ter preverili porazdelitev podatkov. V drugem koraku *Ocena merilnega modela z reflektivnimi konstrukti*, smo ocenili CA, CR, AVE, Fornell-Lackerjev kriterij, HTMT itd. V tretjem koraku *Ocena strukturnega modela* smo ocenili faktor inflacije variance (angl. »*Variance Inflation Scores*«, v nadaljevanju VIF), pojasnjevalno in napovedno moč modela ter relevantnost in statistično značilnost poti v modelu (Hair, et al., 2019a). Prav tako smo ocenili napovedno moč modela zunaj vzorca z uporabo postopka PLSpredict (Sarstedt & Cheah, 2019; Shmueli, et al., 2016, 2019). Dodatni korak pri interpretaciji rezultatov PLS-SEM vključuje še izvajanje enega ali več preverjanj robustnosti, ki dodatno podprejo stabilnosti rezultatov. Ustreznost teh preverjanj je odvisna od raziskovalnega konteksta, kot sta cilj analize in razpoložljivost podatkov (Hair, et al., 2019a).

3.5.3.1 Predhodna vprašanja, povezana z vidiki uporabe PLS-SEM (velikost vzorca, porazdelitev podatkov, koncept prileganja modela)

Za izračun velikosti vzorca smo se osredotočili na zahteve za uporabo SEM, saj od vseh predvidenih statističnih analiz, le-ta zaradi svoje kompleksnosti zahteva kar največji vzorec. Določanje ustrezne velikosti vzorca je prvi korak, pri katerem je potrebno upoštevati ozadje modela, porazdelitvene značilnosti podatkov, psihometrične lastnosti spremenljivk in obseg njihovih odnosov (Wong, 2019). Metoda PLS-SEM ponuja rešitev pri majhnih vzorcih ter večjemu številu konstruktov in elementov (Hair, et al., 2017; Willaby, et al., 2015). Algoritem omenjene statistične metode omogoča rešitve z ločenim izračunavanjem razmerij med merilnimi in strukturnimi modeli. Vendar pa tako kot druge multivariatne metode, tudi ta metoda ne more spremeniti slabega (npr. nereprezentativnega) vzorca v ustreznega, da bi lahko zagotovila veljavno oceno modela. PLS-SEM se vsekakor lahko uporablja pri majhnih vzorcih, vendar narava populacije določa situacije, v katerih je majhna velikost vzorca še sprejemljiva (Rigdon, 2016). Ob predpostavki, da so vse ostale situacijske značilnosti enake, je ob heterogeni populaciji potrebna večja velikost vzorca, da se lahko doseže še sprejemljivo vzorčno napako (Cochran, 1977 cited in Hair, et al., 2019a).

Za izhodišče smo vzeli:

- Priporočilo desetih enot vzorca na merjeno spremenljivko (Wolf, et al., 2013), kar je v našem primeru *50 merjenih spremenljivk x 10 enot vzorca na spremenljivko = 500 enot.*
- Tabachnick in Fidell (2018) navajata enačbo za izračun priporočene velikosti vzorca: $50 + 8x$, kjer je x število merjenih spremenljivk. Skladno s predlagano enačbo priporočena velikost vzorca znaša: $50 + 8 \cdot 50 = 450$.
- »*A-priori*« izračun za velikost vzorca z zahtevno statistično močjo 0,8 in pragom statistične značilnosti 0,05, kar smo izračunali s pomočjo kalkulatorja *»A-priori Sample Size Calculator for Structural Equation Models«* (Soper, 2020). Upoštevali smo, da ima naš predlagani raziskovalni model 50 merjenih in 15 latentnih spremenljivk. Kot osnovo za velikost učinka smo vzeli primerljivo raziskavo (Nasir, et al., 2019a), kjer so identificirali razmeroma veliko velikost učinka (R^2 = 0,445). Raziskovalni model omenjenih raziskovalcev ima 44

merjenih in 14 latentnih spremenljivk. Vendar, ker nismo imeli zagotovila, da bomo v naši raziskavi dobili podobno velikost učinka, smo se raje odločili za srednjo vrednost velikosti učinka (R^2 = 0,3), ki da najmanjšo velikost vzorca – 212 enot.

Iz predlaganih izhodišč smo izbrali največjo predlagano velikost vzorca, in sicer 500 enot.

Pred izvedbo analiz smo preverili normalnost porazdelitve podatkov. Rezultati so pokazali, da se podatki ne porazdeljujejo normalno (tabela 14). Številni raziskovalci navajajo, da je odstopanje podatkov od normalne porazdelitve eden glavnih razlogov za izbiro PLS-SEM (Hair, et al., 2012; Nitzl, 2016). Čeprav gre za eno od prednosti rabe v družboslovnih študijah, sama po sebi še vedno ni zadostna utemeljitev. Odstopanje od normalne porazdelitve lahko deluje tudi na same rezultate PLS-SEM, četudi ta deluje z ekstremnimi vrednostmi (Sarstedt, et al., 2016). Nastale težave omili postopek bootstrappinga s popravkom in pospeškom (angl. »*Bias-corrected and accelerated bootstrapping – Bca*«*).* Ta prilagodi intervale zaupanja v primeru asimetrične porazdelitve podatkov. Sama izbira PLS-SEM zaradi porazdelitve podatkov torej v večini primerov ne zadostuje, vsekakor pa predstavlja tehten argument v kombinaciji z drugimi razlogi za uporabo PLS-SEM (Hair, et al., 2019a).

Tabela 14: Preverjanje normalnosti porazdelitve podatkov za dimenzije informacijske varnostne kulture ter TPB konstrukte – opisna statistika (n = 527)

Konstrukti	M	SD	KA	KS
ATB	1,33	0,85	3,97	18,87
SN	1,71	1,05	1,80	3,64
PBC	2,52	2,03	1,06	-0,35
BI	1,61	1,08	2,18	5,12
NB	1,51	0,91	2,53	7,89
PO	6,17	1,23	-2,30	6,01
SO	5,89	1,20	-1,39	2,53
PCM	5,68	1,34	-1,42	1,97
RM	5,09	1,38	-0,53	-0,08
SETA	5,34	1,45	-0,90	0,16
TMC	5,11	1,49	-0,55	-0,26
MON	4,82	1,67	-0,52	-0,67
ISK	4,98	1,42	-0,47	-0,06
ISKS	4,95	1,46	-0,55	-0,32

Legenda: analiza iz povprečja posameznih dimenzij, kurtosis (koeficient sploščenosti – KS), skewness (koeficient asimetrije – KA)

PLS-SEM metoda se ne zanaša na validacijo modela, t.j. prileganje modela (angl. »*Goodness-of-Fit*«, v nadaljevanju GoF) (Hair, et al., 2019b) in naj se tudi ne bi uporabljal kot merilo za kakovost GoF (SmartPLS GmbH, 2023). Zaradi tega se tudi napačno sklepa, da PLS-SEM ni uporabna metoda za testiranje in potrjevanje teorij (Westland, 2015). Kljub temu, da so nekateri metodologi potrdili meritve za GoF pri PLS-SEM metodi (Henseler, et al., 2016), je potrebna pozornost pri odločanju o uporabnosti teh meritev (Henseler & Sarstedt, 2013; Hair, et al., 2019b), saj celovita ocena le-teh doslej še ni bila izvedena. Zaradi tega je potrebno vse prage in smernice, ki jih navaja literatura, obravnavati z določeno mero preudarnosti. Priporočljivo je osredotočanje na napovedno vrednotenje modela, ki je v skladu z vzročno-napovedno naravo PLS-SEM (Sharma, et al., 2019a). Postavlja se vprašanje, ali je koncept GoF, kot se uporablja v okviru raziskav CB-SEM, sploh koristno uporabiti v PLS-SEM (Rigdon, 2012). PLS-SEM se namreč osredotoča predvsem na medsebojno delovanje med napovedovanjem in testiranjem teorije, rezultate pa je potrebno ustrezno potrditi (Shmueli, 2010). V tem kontekstu so raziskovalci pred kratkim predlagali nove postopke vrednotenja, ki so zasnovani posebej za napovedno usmerjeno naravo PLS-SEM (Shmueli, et al., 2016). Kot navajajo Wong (2019) ter Dash in Paul (2021), je bilo izračunavanje GoF do sedaj redko izvedeno in poročano, vendar je z razvojem »*Partial Least Square Consistent-SEM*« (v nadaljevanju PLSc) to mogoče. PLSc trenutno omogoča ugotavljanje, ali se model dobro ali slabo prilega (Henseler, et al., 2014) in odkriva napačne specifikacije merilnega ter strukturnega modela (Dijkstra & Henseler, 2015). Uporabimo ga takrat, ko želimo razumeti neskladja med opazovanimi ali približnimi vrednostmi odvisnih spremenljivk in vrednostmi, ki jih napoveduje PLS model. Zaradi zgoraj opisanih dejstev smo se odločili, da rezultatov prileganja modela ne bomo poročali.

3.5.3.2 Ocena merilnega modela z reflektivnimi konstrukti

Ocena merilnega modela je opisana v poglavju *Zanesljivost in veljavnost vprašalnika* kjer smo podrobneje predstavili CA, CR, AVE, Fornell-Lacker kriterij ter HTMT.

3.5.3.3 Ocena strukturnega modela z reflektivnimi konstrukti

VIF

Koeficienti strukturnega modela odnosov med konstrukti izhajajo iz ocenjevanja niza regresijskih enačb. Pred ocenjevanjem strukturnih odnosov je potrebno preveriti kolinearnost, saj ima lahko le-ta učinek na rezultate regresije (Hair, et al., 2019a). Postopek je podoben ocenjevanju formativnih merilnih modelov. Za izračun VIF se uporabijo ocene latentnih spremenljivk napovednih konstruktov v delni regresiji (Hair, et al., 2019a). VIF nad 5 identificira težave s kolinearnostjo med napovednimi konstrukti, vendar se težave lahko pojavijo tudi pri nižjih vrednostih, t.j. 3–5 (Becker, et al., 2015). V idealnem primeru bi moral VIF znašati 3 ali celo nižje. Hair, et al. (2019a) navajata, da je v takem primeru najboljša izbira uporaba modela višjega reda, ki ga še lahko podpira teorija. Med drugim Kock in Lynn (2012) poudarjata, da se vrednosti VIF nad 5 pojavljajo ob uporabi algoritmov, ki vključujejo merilno napako. Kljub temu, da je pripomba podana v zvezi z algoritmi SEM, ki temeljijo na kovarianci, se nanaša tudi na algoritme PLS-SEM, ki temeljijo na faktorjih, saj obe vrsti algoritmov vključujeta merilno napako. Za reflektivne indikatorje so tako vrednosti VIF visoke in jih zato ni niti smiselno ocenjevati. V kolikor pa jih že, se poročajo vrednosti VIF za notranji (strukturni) model.

Pojasnjevalna in napovedna moč modela

R^2 meri varianco, ki je razložena v vsakem od endogenih konstruktov in je zato merilo za razlagalno moč modela (Shmueli & Koppius, 2011). Vrednosti R^2 se gibljejo od 0 do 1, kjer višje vrednosti kažejo na večjo razlagalno moč. Kot vodilo se vrednosti R^2 0,75; 0,50 in 0,25 štejejo za znatne, zmerne in šibke (Henseler, et al., 2009; Hair, et al., 2011). Henseler, et al. (2009) izpostavljajo strožji kriterij glede odstotkov pojasnjene variance, kot npr. Cohenova kategorizacija vrednosti R^2. Po Cohenu (1988) vrednosti f^2: 0,02; 0,15 in 0,35 kažejo, da ima eksogeni konstrukt majhen, srednji ali velik učinek na endogeni konstrukt. Sprejemljive vrednosti R^2 temeljijo na kontekstih in v nekaterih disciplinah že nizka vrednost, t.j. 0,10 velja za zadovoljivo (npr. pri napovedovanju donosnosti delnic) (Raithel, et al., 2012). R^2 je funkcija števila prediktorskih konstruktov – večje kot je število prediktorskih konstruktov, višji je R^2. Zato je potrebno R^2 vedno razlagati v

povezavi s kontekstom raziskave in na podlagi vrednosti R^2 iz sorodnih raziskav ter modelov podobne kompleksnosti. Pri merjenju koncepta, ki je sam po sebi predvidljiv (npr. fizični procesi) se lahko pojavijo vrednosti $R^2 = 0{,}90$. Podobne vrednosti so možne tudi v modelu, ki napoveduje človeški odnos, dojemanje in namero (Hair, et al., 2019a). Mogoče je ovrednotenje, kako odstranitev določenega napovedovalnega konstrukta deluje na vrednost R^2 endogenega konstrukta – v tem primeru govorimo o velikosti učinka (f^2). Velikost učinka nam pokaže, koliko eksogena latentna spremenljivka prispeva k vrednosti R^2 endogene latentne spremenljivke. Učinek ocenjuje velikost razmerja med latentnimi spremenljivkami. Chin, et al. (2003) navajajo, da je potrebno poleg statistično značilnih povezav med spremenljivkami poročati tudi o velikosti učinka med temi spremenljivkami. Vrstni red pomembnosti napovednih konstruktov pri razlagi odvisnega konstrukta v strukturnem modelu je pogosto enak, če primerjamo velikost koeficientov poti (β) in velikosti učinka (f^2) (Hair, et al., 2019a).

Napovedna ustreznost je še en vidik, ki ga je mogoče raziskati za notranji (strukturni) model. Matrike, ki jih PLS omogoča za preizkušanje napovedne ustreznosti poti modela (angl. »*path model's predictive relevance*«) sta *»the blindfolding-based* Q^2« in »*PLSpredict*« (Sarstedt & Cheah, 2019).

Q^2 (angl »*The Stone-Geisser's* Q^2 *values*«) (Geisser, 1974; Stone, 1974), združuje vidike napovedi izven vzorca in pojasnjevalne moči v vzorcu (Shmueli, et al., 2016; Sarstedt, et al., 2021). Izračun vrednosti Q^2 temelji na t. i. postopku »*blindfolding«*. Vrednosti Q^2 morajo biti za določen konstrukt višje od 0, saj lahko samo tako nakažejo napovedno ustreznost strukturnega modela za dotični konstrukt (Hair, et al., 2013). Vrednosti Q^2 višje od 0; 0,25 in 0,50 prikazujejo majhno, srednjo in veliko napovedno ustreznost modela. Podobno kot pri velikostih učinka f^2 je možno izračunati in interpretirati velikosti učinka q^2 (Hair, et al., 2019a).

Napovedna moč modela zunaj vzorca

Večina raziskovalcev interpretira vrednosti R^2 kot merilo napovedne moči modela. Gre za ne povsem pravilno interpretacijo, saj vrednost R^2 samo nakazuje pojasnjevalno moč modela v vzorcu – in ne pove ničesar o napovedni moči modela zunaj vzorca (Shmueli,

2010; Shmueli & Koppius, 2011; Dolce, et al., 2017). Zaradi opisanega so Shmueli, et al. (2016) predlagali nabor postopkov za napovedovanje zunaj vzorca. Ta nabor vključuje ocenjevanje modela na vzorcu za analizo in njegove napovedi na podatkih, ki niso vzorec za analizo, kar imenujemo zadržani vzorec. Programska oprema SmartPLS omogoča izvedbo analize *PLSpredict*. Omenjena izračunava napovedno moč modela, ki temelji na zadržanem vzorcu (Hair, et al., 2019a). *PLSpredict* izvaja *k*-kratno navzkrižno preverjanje. Zgib je podskupina celotnega vzorca in *k* je število podskupin. Celoten nabor podatkov je naključno razdeljen na *k* enako velikih podnaborov podatkov. Na primer navzkrižna validacija na podlagi $k = 5$ razdeli vzorec na pet enako velikih podnaborov podatkov (tj. skupin podatkov). *PLSpredict* nato združi $k - 1$ podnaborov v en sam vzorec analize, ki se uporablja za napovedovanje preostalega petega podnabora podatkov. Peti podnabor podatkov je zadržani vzorec za prvo navzkrižno preverjanje. Ta postopek navzkrižnega preverjanja se nato ponovi *k*-krat (v tem primeru petkrat), pri čemer je vsaka od petih podmnožic enkrat uporabljena kot zadržani vzorec. Tako ima vsak primer v vsakem zadržanem vzorcu predvideno vrednost, ocenjeno z vzorcem, v katerem ta primer ni bil uporabljen za oceno parametrov modela (Hair, et al., 2019a). Shmueli, et al. (2019) priporočajo nastavitev $k = 10$, vendar je pri tem potrebno zagotoviti, da vzorec za analizo za vsako podskupino (zgib) ustreza smernicam za minimalno velikost vzorca.

Pri oceni napovedne moči modela, ki temelji na *PLSpredic*t, je na voljo več analiz, ki kvantificirajo napovedne napake. Ena od njih je povprečna absolutna napaka (angl. »*the Mean Absolute Error*«, v nadaljevanju MAE) in pa povprečna kvadratna napaka (angl. »*the Root Mean Squared Error*«, v nadaljevanju RMSE). MAE meri povprečno velikost napak v nizu napovedi brez upoštevanja njihove smeri in je povprečna absolutna razlika med napovednimi in dejanskimi opazovanji, pri čemer imajo vse posamezne razlike enako težo (Hair, et al., 2019a). RMSE je definirana kot kvadratni koren povprečja kvadratov razlik med napovedmi in dejanskimi opazovanji. Ker RMSE kvadrira napake pred povprečenjem, statistika pripiše večjo težo večjim napakam, zaradi česar je še posebej uporabna, ko velike napake niso zaželene (Hair, et al., 2019a). Pri interpretaciji rezultatov *PLSpredict* je potrebna osredotočenost na ključni endogeni konstrukt v modelu, v nasprotju s preučevanjem napovednih napak za vse indikatorje vseh endogenih konstruktov. Ko je izbran ključni konstrukt, je potrebno ovrednotenje Q^2 (Shmueli, et al., 2019). Ovrednotenju Q^2 sledi analiza napovedne statistike. Zaželeno je poročanje

vrednosti RMSE; v kolikor je porazdelitev napovednih napak zelo nesimetrična, je MAE ustreznejša napovedna statistika (Shmueli, et al., 2019). Napovedna statistika je odvisna od merilnih lestvic indikatorjev in njihove surove vrednosti nimajo večjega pomena. Zaradi tega je potrebno primerjati vrednosti RMSE (ali MAE) s primerjalnim merilom. Primerjalno merilo uporablja linearni regresijski model (LM) za ustvarjanje napovedi manifestnih spremenljivk, na način, da izvede linearno regresijo vsakega indikatorja odvisnega konstrukta na indikatorjih eksogenih latentnih spremenljivk v PLS poti modela (Danks & Ray, 2018).

V primerjavi vrednosti RMSE ali MAE z vrednostmi LM veljajo naslednje smernice (Shmueli, et al., 2019):

- Če analiza s primerjalnim merilom LM prinese večje napake v napovedi RMSE ali MAE za vse kazalnike, to pomeni, da model nima napovedne moči.
- Če večina indikatorjev odvisnih konstruktov v analizi povzroči večje napake v napovedi v primerjavi s primerjalnim merilom LM, to pomeni, da ima model nizko napovedno moč.
- Če manjšina (ali enako število) indikatorjev v analizi povzroči večje napake v napovedi v primerjavi s primerjalnim merilom LM, slednje kaže na srednjo napovedno moč.
- Če nobeden od indikatorjev v analizi nima višjih vrednosti RMSE ali MAE v primerjavi s primerjalnim merilom LM, ima model visoko napovedno moč.

Statistična značilnost in relevantnost koeficientov poti

Po analizi razlagalne in napovedne moči modela je zadnji korak ocena statistične pomembnosti in ustreznosti koeficientov poti. PLSc-SEM izvaja popravek korelacije reflektivnih konstruktov, da postanejo rezultati skladni s faktorskim modelom (Dijkstra, 2010, 2014; Dijkstra & Schermelleh-Engel, 2014; Dijkstra & Henseler, 2015). Proces metode ponovnega vzorčenja daje analizo statistične značilnosti koeficientov poti in njihove vrednosti, ki imajo razpon od - 1 do + 1. Omenjeni proces metode omogoča izračunavanje tako posrednega učinka konstrukta na določen ciljni konstrukt prek enega ali več vmesnih konstruktov ter skupni učinek. Skupni učinek je opredeljen kot vsota posrednih in vseh neposrednih učinkov in reflektira kumulativni učinek enega konstrukta

na drugega v strukturnem modelu (Hu, et al., 2012). Gre za perspektivo, ki pokaže vzročni učinek posameznega konstrukta na osrednjo preučevano spremenljivko. Posredni učinek je pomemben pri ocenjevanju mediacijskih učinkov (Nitzl, 2016). Po pregledu koeficientov poti za notranji model sledi pregled zunanjega modela s preverjanjem T-statistike (Wong, 2019).

3.5.4 Pristranost zaradi skupne metode zbiranja podatkov in varianca skupne metode

Medtem ko velja anketa kot najpogosteje uporabljena metoda zbiranja podatkov, predstavlja tudi potencialno nevarnost pojava CMV ter CMB, ki lahko imata učinek na zanesljivost in veljavnost empiričnih rezultatov (Kock, et al., 2021).

CMV je opredeljena kot sistematična napaka variabilnosti in izhaja iz skupne metode, rabljene za merjenje konstruktov (Podsakoff, et al., 2003). Ko ima CMV učinek na razmerje med merjenimi spremenljivkami, govorimo o prisotnosti CMB (Jakobsen & Jensen, 2015). Slednja se pojavi, ko so tako neodvisne kot tudi odvisne spremenljivke merjene znotraj iste ankete, pri čemer se uporablja enaka (tj. skupna) metoda merjenja (npr. ordinalna lestvica). Skupna metoda merjenja neodvisnih in odvisnih spremenljivk je ena od virov sistematičnih napak merjenja, ki izkrivljajo prave odnose med spremenljivkami in vodijo v merilne napake (Bagozzi & Yi, 1990). Omenjene vključujejo tako naključne kot tudi sistematične komponente. CMB ima lahko učinek na parametersko ocenjevanje hipotetičnih odnosov med konstrukti. Ta učinek lahko bodisi zmanjša bodisi poveča moč povezav med spremenljivkami in vodi do napake tipa I in II. Metaanaliza avtorjev Dolnicar, et al. (2014) je pokazala, da je CMB skrb vzbujajoča v raziskavah, ki preučujejo povezave med zadovoljstvom in namero ponovnega potovanja oz. obiska določenega kraja. Ugotovitve omenjenih raziskovalcev so pokazale, da prisotnost CMB poveča moč obstoječe povezave med konstruktoma, kar vodi do napačnih sklepanj (Dolnicar, et al., 2015).

Viri CMB lahko izhajajo iz respondentov (skupni učinki respondenta, značilnosti respondentov) ali iz merilnega instrumenta (značilnost merilnih elementov, kontekst merjenja) (Kock, et al., 2021).

Skupni učinki respondenta kažejo na sistematično napako variance (angl. »*systematic error variance*«), ki se pojavi, ko isti respondent oceni tako neodvisno kot odvisno spremenljivko (Podsakoff, et al., 2003). Omenjeni učinki vključujejo nagnjenost respondenta k odgovarjanju vprašanj na družbeno sprejemljiv način, kar je v nasprotju z izražanjem resničnih občutkov (družbena zaželenost), nagnjenost k nestrinjanju ali strinjanju (pristranskost pritrjevanja) ter poskus odgovarjanja na vsa vprašanja ankete na dosleden način (motiv doslednosti). Skupni učinki, ki jih povzroči isti respondent, lahko privedejo do napačnih zaključkov glede obstoječih odnosov med spremenljivkami (Podsakoff, et al., 2003).

Atributi elementov merilnega instrumenta zadevajo kompleksne ali nejasne formulacije vprašanj, ki lahko vodijo k stiliziranemu odgovarjanju respondentov in predstavljajo vir sistematične napake variance. Vrste merilne lestvice, kot je npr. ordinalna lestvica, predstavlja vir pristranosti v odgovorih (Dolnicar, 2020). Kontekstualne značilnosti merskih elementov prav tako predstavljajo potencialen vir CMB. Omenjene značilnosti izhajajo iz oblikovanja merskega instrumenta. Na primer vrstni red vprašanj, ki merijo neodvisne in odvisne spremenljivke lahko nakazuje vzročno povezavo med njimi in s tem vodi respondente, da se z odgovarjanjem podvržejo predpostavljenim odnosom med spremenljivkami. Pri oblikovanju merilnega instrumenta je pomembno upoštevati dolžino končnega vprašalnika. Uporaba dolgih vprašalnikov lahko povzroči utrujenost respondenta, kar zmanjšuje motivacijo pri odgovarjanju na vprašanja. Merilni kontekst lahko privede do CMB, če se neodvisne in odvisne spremenljivke merijo na istem mestu in v istem trenutku (Podsakoff, et al., 2003).

Poznamo več preverjanj prisotnosti CMB, ki jih razdelimo na dve vrsti: in sicer postopkovna in statistična preverjanja. Postopkovna preverjanja se izvajajo pred zbiranjem podatkov (ex ante), medtem ko se statistične izvajajo po zbiranju podatkov (ex post). Po temeljitem preverjanju združimo ex ante in ex post (Kock, et al., 2021). Postopkovna preverjanja je pomembno uvesti že v zelo zgodnjih fazah oblikovanja merskega instrumenta, saj raba statističnih rešitev šele v kasnejši fazi ni dovolj (Kock, et al., 2021).

Postopkovna preverjanja se nanašajo na ukrepe, ki so namenjeni zmanjševanju ali odpravljanju CMB s pomočjo temeljitega oblikovanja merskega instrumenta (razvoj jasnih navodil za respondente; seznanitev respondentov, da ni pravilnih odgovorov in da bodo vsi odgovori ostali anonimni; uporaba nasprotnih trditev namesto obrnjenih vprašanj) (Weijters & Baumgartner, 2012).

Ločevanje virov za neodvisne in odvisne spremenljivke lahko pomaga omiliti učinke CMB. Neodvisna spremenljivka se tako pridobi iz enega vira (respondenta), odvisna spremenljivka pa iz drugega ali sekundarnega vira podatkov (Jakobsen & Jensen, 2015), vendar v mnogih primerih takšna ločitev ni mogoča. Zato so na voljo tudi druge tehnike, kot je npr. časovna ločitev. Ta se nanaša na zbiranje podatkov od istega vira, vendar v različnih časovnih točkah. Ta tehnika pomaga izboljšati natančnost odgovorov (Podsakoff, et al., 2012). Ločevanje lahko temelji na metodologiji ali bližini (raba različnih lestvic ali oblik merilnih elementov odvisnih in neodvisnih spremenljivk ali merjenje le-teh v različnih delih ankete) (Viswanathan & Kayande, 2012).

Statistična preverjanja predstavljajo drugo skupino ukrepov za ugotavljanje CMB in se uporabljajo po zaključenem zbiranju podatkov (*ex post*). Namenjene so identifikaciji in ne preprečevanju CMB (Kock, et al., 2021). Harmanov enofaktorski test (angl. »*Harman's single factor tes*t« ali »*Harman's one-factor test*«) predstavlja najpogosteje uporabljeno tehniko preverjanja prisotnosti CMB (Fuller, et al., 2016). Test zajema uporabo nerotirane EFA ob predpostavki obstoja samo enega faktorja. CMB je prisotna takrat, ko en faktor pojasni več kot 50 % variance (Fuller, et al., 2016). Možnost za ugotavljanje prisotnosti CMB daje še nekaj tehnik. V doktorski nalogi smo poleg rezultatov Harmanovega enofaktorskega testa predstavili še rezultate dveh drugih analiz.

V poglavju *Razvoj merskega instrumenta* je podrobneje razdelan proces uporabljenih postopkovnih preverjanj. Verjetnost pristranosti zaradi družbene zaželenosti anketirancev smo zmanjšali tako, da smo respondentom zagotovili anonimnost in izpostavili, da ni pravilnih ali napačnih odgovorov. Respondente smo prosili, da na vprašanja odgovarjajo iskreno. Nadzor pristranosti nad odzivom na družbeno zaželenost respondentov smo izvedli z neposrednim merjenjem omenjenih spremenljivke družbena zaželjenost in delnim izločanjem učinkov omenjene spremenljivke na napovedno in kriterijsko

spremenljivko (Hays, et al., 1989). Slednjo smo uporabili pri izračunu CMV (Podsakoff,, et al., 2003). Gre za teoretično nepovezano spremenljivko s konstrukti in okvirom raziskave. Raziskave poudarjajo uporabo vsaj štirih merilnih elementov spremenljivke družbena zaželjenost in njihovo implementacijo na konec ankete. Chin, et al. (2013) navajajo, da se na tak način CMV zmanjša tudi za 70 %. Spremembe v R^2 po vpeljavi omenjene spremenljivke v model ne smejo biti višje od 10 % (Podsakoff, et al., 2003). Rezultati analize izločitve spremenljivke družbena zaželenost so prikazani v Tabeli 15. V njih ni zaznati pomembnih sprememb po uvedbi spremenljivke družbena zaželenost (spremembe v R^2 so pod 10 %). V vzorcu raziskave torej ni zaznati CMV. Podoben rezultat je pokazala tudi analiza z uporabo merjene in nemerjene latentne spremenljivke. Bistvenih sprememb v R^2 ne gre zaznati, kar nakazuje, da v vzorcu raziskave ni prisotnosti CMV.

Tabela 15: Izločitev spremenljivke družbena zaželenost

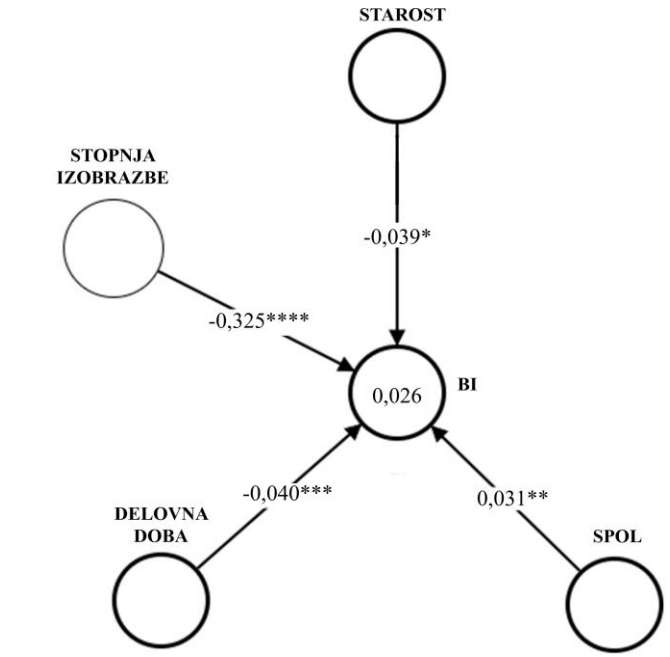
Odvisna spremenljivka	β pred uvedbo marker spremenljivke	β po uvedbi marker spremenljivke	R^2 pred uvedbo marker spremenljivke	R^2 po uvedbi marker spremenljivke	Sprememba R^2 v %
ATB → BI	0,306	0,301	0,091	0,158	6,7
SN → BI	0,161	0,158	0,098	0,149	5,1
NB → BI	0,369	0,326	0,184	0,251	6,7
PBC → BI	0,124	0,109	0,050	0,102	5,2
BI			0,623	0,638	1,5

Po avtorjih Podsakoff, et al. (2003) smo preverili, ali obstaja možnost za CMB tako, da smo izračunali nerotirano EFA ob predpostavki obstoja samo enega faktorja. V našem primeru en takšen faktor pojasni 37,6 % variance (priloga 13). Ker je omenjena vrednost pod 50 %, CMB ni prisotna.

Kot navajajo Dunning, et al. (2004), je samoocenjevanje podvrženo pristranskosti, v primeru informacijske varnosti pa smo pričakovali celo družbeno zaželene odgovore. Samoocena predstavlja posameznikovo zaznavo lastnega vedenja na različnih dimenzijah (Eckert, et al., 2000). Ne glede na to, da številni avtorji v takih primerih predlagajo še dodatne načine zbiranja podatkov (npr. intervjuji, fokusne skupine, opazovanje), se pristranosti ne moremo povsem izogniti. Že sama prisotnost raziskovalca oz. samo zavedanje preiskovancev, da so opazovani, izkrivi dejanski fenomen.

3.5.5 Učinek kontrolnih spremenljivk

Kontrolne spremenljivke »*spol«*, »*stopnja izobrazbe«*, »*delovna doba«* in »*starost«* smo v raziskovalni model dodali z namenom ugotavljanja, ali bi katera od naštetih lahko imela učinek na odvisno spremenljivko BI. Slednje smo izvedli s pomočjo programa SmartPLS 4. Prav tako smo kontrolne spremenljivke v nadaljevanju preučili v povezavi s hipotezami H7, ki se nanašajo na povezanost kontrolnih spremenljivk na spremenljivki ATB in BI (a–f). Slednje smo izvedli s pomočjo programa SPSS. V prvem delu smo analizirali učinek kontrolnih spremenljivk na spremenljivko BI; ker se koeficienti poti in R^2 drugače obnašajo v večjih modelih, smo v drugem delu analize kontrolne spremenljivke vnesli v celotni model. Slika 11 prikazuje rezultate koeficientov poti, statistično značilnost povezav in učinke med kontrolnimi spremenljivkami in konstruktom BI. Rezultati kažejo, da obstaja le ena šibka povezanost med kontrolno spremenljivko *»stopnja izobrazbe«* in BI (β = -0,325), vendar je ta statistično značilna (p = 0,002). Ostale kontrolne spremenljivke niso statistično značilno povezane z BI.



*p = 0,588, f^2= 0,001; **p = 0,838, f^2= 0,000; ***p = 0,562, f^2= 0,001; ****p = 0,002, f^2= 0,021

Slika 11: Povezanost kontrolnih spremenljivk na BI (β in R^2)

Tabela 16: Rezultati povezanosti kontrolnih spremenljivk z BI

Povezanost	***t***	***β***	***p***	f^2	f^2 **učinek**
Delovna doba → BI	0,580	-0,040	0,562	0,001	Ne
Spol → BI	0,204	0,031	0,838	0,000	Ne
Starost → BI	0,542	-0,039	0,588	0,001	Ne
St. izobrazbe → BI	3,121	-0,325	0,002	0,021	Zanemarljiv

V drugem delu analize, ko smo kontrolne spremenljivke vnesli v celotni model, rezultati niso potrdili prisotnosti statistično značilne povezanosti med kontrolnimi spremenljivkami in BI. Rezultati v Tabeli 17 kažejo, da spremenljivke *»spol«*, *»starost«*, *»delovna doba«* in *»stopnja izobrazbe«* nimajo učinka na odvisno spremenljivko BI. Kontrolne spremenljivke smo v nadaljevanju uporabili pri analiziranju H7, vendar smo jih iz končnega strukturnega modela izločili.

Tabela 17: Rezultati povezanosti kontrolnih spremenljivk z BI (celotni model)

Povezanost	***t***	***β***	***p***	f^2	f^2 **učinek**
Delovna doba → BI	1,413	-0,070	0,158	0,004	Neznaten
Spol → BI	1,820	-0,032	0,069	0,007	Neznaten
Starost → BI	0,841	0,148	0,400	0,002	Neznaten
St. izobrazbe → BI	0,466	0,043	0,641	0,021	Neznaten

4 REZULTATI

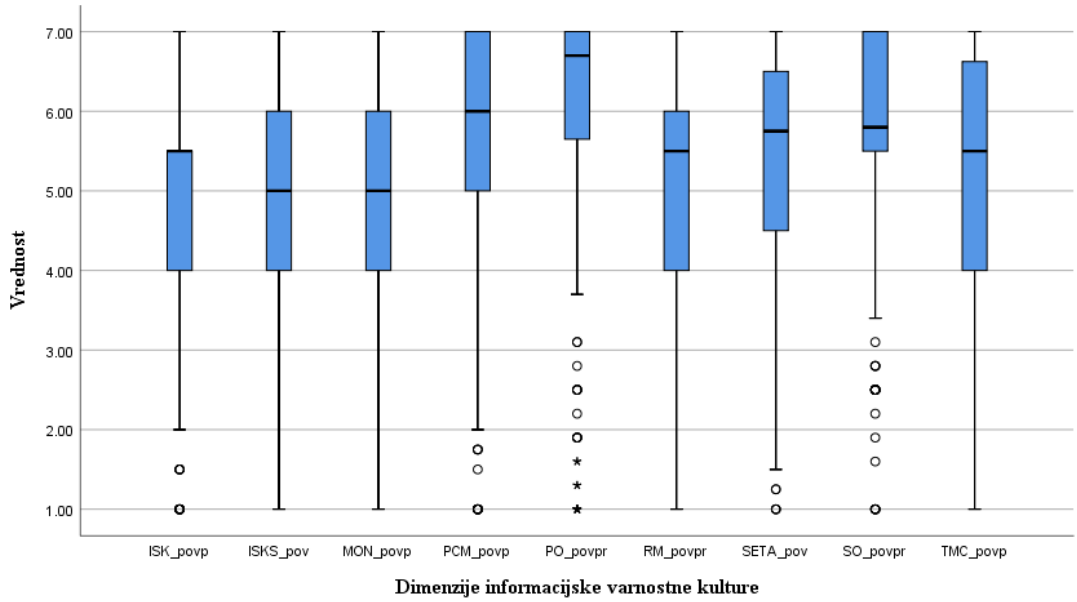
4.1 REZULTATI OPISNE STATISTIKE DIMENZIJ

Tabela 18 prikazuje opisno statistiko posameznih dimenzij informacijske varnostne kulture. Iz omenjene tabele razberemo vrednost mediane za vsak posamezen konstrukt. Najnižja vrednost mediane je pri dimenziji MON in ISKS (5,0). Najvišja vrednost mediane je pri dimenziji PO (6,70). Slika 12 prikazuje diagram škatla z ročaji za omenjene dimenzije.

Tabela 18: Opisna statistika posameznih dimenzij (n = 527)

Dimenzije	M	SD	Me	Q1	Q3
PO	6,18	1,23	6,70	5,50	7,00
SO	5,89	1,20	5,80	5,50	7,00
PCM	5,69	1,34	6,00	5,00	7,00
RM	5,10	1,39	5,50	4,00	6,00
SETA	5,34	1,45	5,75	4,50	6,50
TMC	5,11	1,50	5,50	4,00	6,63
MON	4,82	1,67	5,00	4,00	6,00
ISK	4,98	1,42	5,50	4,00	5,50
ISKS	4,96	1,46	5,00	4,00	6,00

Legenda: M – povprečna vrednost, SD standardni odklon, Me – mediana, Q1 – 1. kvartil, Q3 – 3. kvartil



Slika 12: Diagram škatla z ročaji – vrednosti median za dimenzije informacijske varnostne kulture

4.1.1 Izračun razlik v zaznavanju dimenzij glede na starost udeležencev

Tabela 19 prikazuje povezanost med starostjo zaposlenih v zdravstveni negi in zaznavanjem dimenzij informacijske varnostne kulture. Slednja kaže na izredno šibko, pozitivno povezavo med starostjo udeležencev in dimenzijo RM ($r_s = 0{,}211;\ n = 527;\ p < 0{,}001$). Povezave med starostjo udeležencev in dimenzijami PCM ($r_s = 0{,}157;\ n = 527;\ p < 0{,}001$), SETA ($r_s = 0159;\ n = 527,\ p < 0{,}001$), TMC ($r_s = 0{,}164;\ n = 527;\ p < 0{,}001$) in MON ($r_s = 0{,}150;\ n = 527;\ p = 0{,}001$) so navkljub statistični značilnosti neznatne.

Tabela 19: Izračun Spearmanovega koeficienta korelacije rangov za ugotavljanje povezave med dimenzijami in starostjo udeležencev (n = 527)

Dimenzije informacijske varnostne kulture	r_s	p
PO	-0,011	0,801
SO	0,012	0,778
PCM	0,157**	< 0,001
RM	0,211**	< 0,001
SETA	0,159**	< 0,001
TMC	0,164**	< 0,001
MON	0,150**	0,001
ISK	0,075	0,085
ISKS	0,098*	0,024

*p = 0,05; **p < 0,01

4.1.2 Izračun razlik v zaznavanju dimenzij glede na delovno dobo udeležencev

Tabela 20 (glej še prilogo 15) prikazuje povezanost med delovno dobo zaposlenih v zdravstveni negi in zaznavanjem dimenzij informacijske varnostne kulture. Slednja kaže na neznatne ali izredno šibke, pozitivne povezave med delovno dobo udeležencev in dimenzijami PCM ($r_s = 0{,}167;\ n = 527;\ p < 0{,}001$), RM ($r_s = 0{,}123;\ n = 527;\ p = 0{,}005$) in SETA ($r_s = 0142;\ n = 527;\ p < 0{,}001$).

Tabela 20: Izračun Spearmanovega koeficienta korelacije rangov za ugotavljanje povezave med dimenzijami in delovno dobo udeležencev

Dimenzije informacijske varnostne kulture	r_s	p
PO	-0,011	0,804
SO	-0,011	0,809
PCM	0,167**	< 0,001
RM	0,123**	0,005
SETA	0,142**	0,001

Dimenzije informacijske varnostne kulture	r_s	*p*
TMC	0,105*	0,016
MON	0,117**	0,007
ISK	0,063	0,151
ISKS	0,056	0,196

*$p = 0,05$; **$p < 0,01$

4.1.3 Izračun razlik v zaznavanju dimenzij glede na spol udeležencev

Tabela 21 prikazuje opisno statistiko v zaznavanju dimenzij informacijske varnostne kulture glede na spol zaposlenih v zdravstveni negi.

Tabela 21: Opisna statistika za dimenzije glede na spol udeležencev

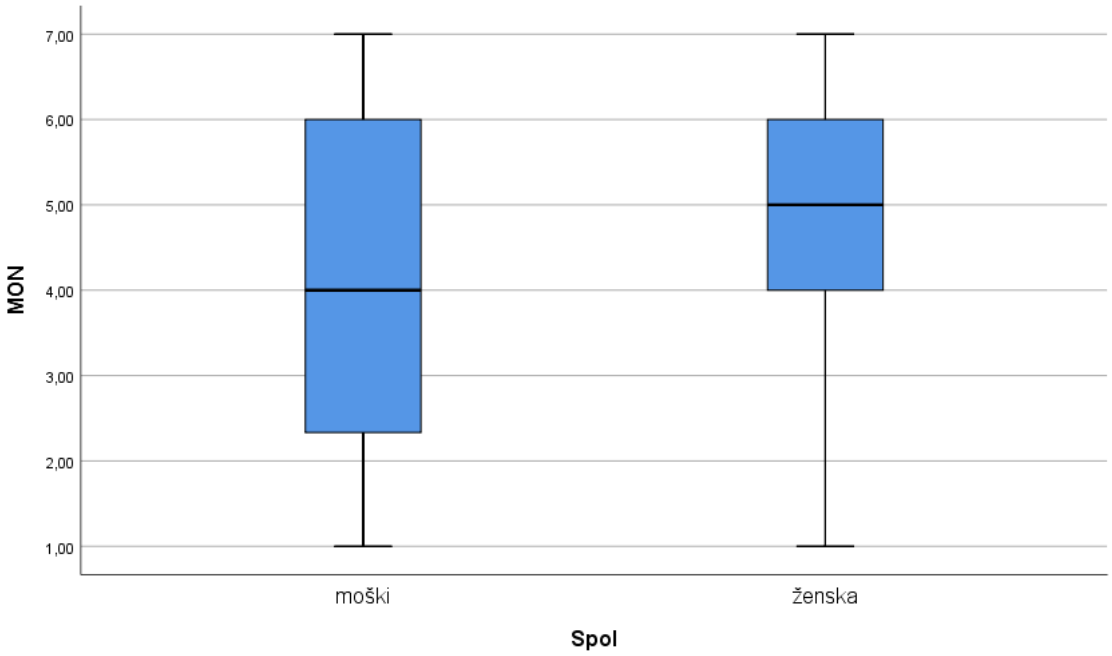
Spol	Dimenzije	n	M	SD	Me	Q1	Q3
moški	PO	70	6,14	1,22	6,40	5,80	7,00
	SO	70	5,74	1,23	5,65	5,20	7,00
	PCM	70	5,41	1,46	5,75	5,00	6,25
	RM	70	4,84	1,52	5,00	4,00	6,00
	SETA	70	5,05	1,58	5,50	4,00	6,50
	TMC	70	4,76	1,57	4,94	3,63	5,88
	MON	70	4,12	1,95	4,00	2,33	6,00
	ISK	70	4,61	1,56	4,50	4,00	5,50
	ISKS	70	4,47	1,61	4,50	3,50	5,75
ženski	PO	457	6,18	1,24	6,70	5,50	7,00
	SO	457	5,92	1,20	5,80	5,50	7,00
	PCM	457	5,73	1,32	6,00	5,25	7,00
	RM	457	5,14	1,36	5,50	4,00	6,00
	SETA	457	5,38	1,43	5,75	4,50	6,50
	TMC	457	5,16	1,48	5,50	4,00	6,63
	MON	457	4,93	1,60	5,00	4,00	6,00
	ISK	457	5,04	1,39	5,50	4,00	5,50
	ISKS	457	5,03	1,42	5,25	4,00	6,00

Legenda: M – povprečna vrednost, SD – standardni odklon, Me – mediana, Q1 – 1. kvartil, Q3 – 3. kvartil

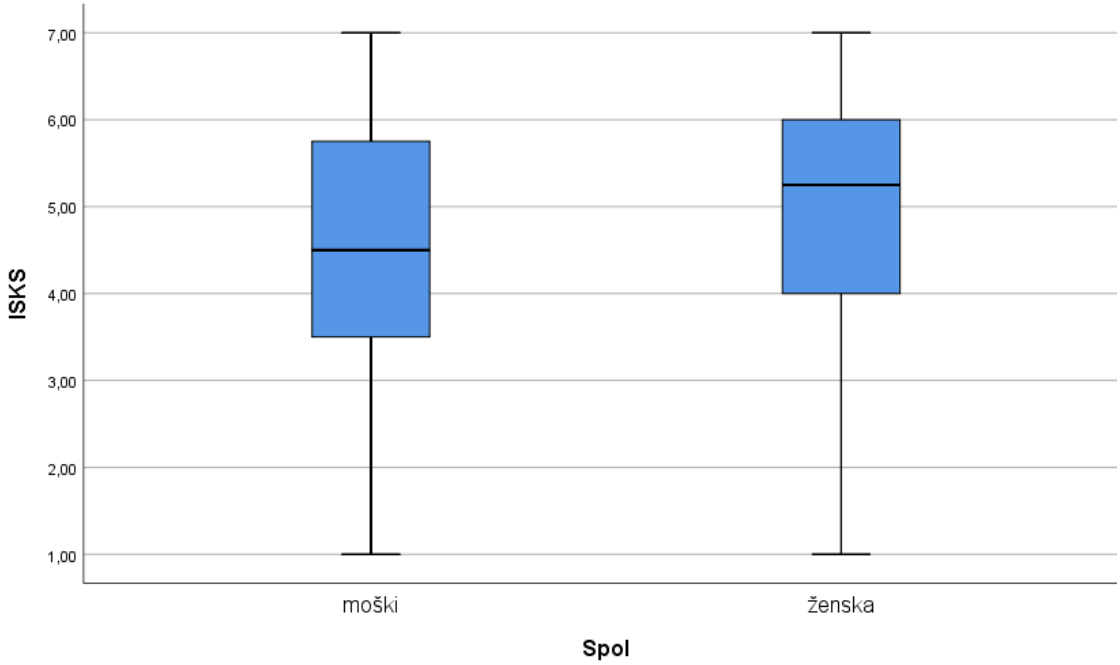
Tabela 22 prikazuje rezultate Mann-Whitneyevega U testa za razlike v zaznavanju dimenzij informacijske varnostne kulture med spoloma (glej prilogo 16). Identificirane so statistično značilne razlike v povprečnih rangih med moškimi in ženskami za dimenziji MON ($U\ (n_{moški} = 70, n_{ženski} = 457) = 1.2069{,}5; Z = -3{,}330; p = 0{,}001$) in ISKS ($U\ (n_{moški} = 70\ , n_{ženski} = 457) = 1.2762{,}5; Z = -2{,}739; p = 0{,}006$). Vrednost mediane pri dimenziji MON pri ženskah znaša 5 (*IQR = 2*), medtem ko pri moških znaša 4 (*IQR = 3,67*) (tabela 22, slika 13). *IQR* = Q3–Q1. Vrednost mediane pri dimenziji ISKS pri ženskah znaša 5,25 (*IQR = 2*), medtem ko pri moških znaša 4,5 (*IQR = 2,25*) (tabela 22, slika 14).

Tabela 22: Rezultati Mann-Whitneyevega U testa za razlike v zaznavanju dimenzij med spoloma (n = 527)

Dimenzije	U	Wilcoxon W	Z	p
PO	15282,0	17767,0	-0,637	0,524
SO	14454,5	16939,5	-1,341	0,180
PCM	13619,0	16104,0	-2,027	0,043
RM	13976,0	16461,0	-1,730	0,084
SETA	13995,0	16480,0	-1,697	0,090
TMC	13126,0	15611,0	-2,456	0,014
MON	12069,5	14554,5	-3,330	0,001
ISK	13378,5	15863,5	-2,248	0,025
ISKS	12762,5	15247,5	-2,739	0,006



Slika 13: Diagram škatla z ročaji za dimenzijo MON, glede na spol



Slika 14: Diagram škatla z ročaji za dimenzijo ISKS, glede na spol

4.1.4 Izračun razlik v zaznavanju dimenzij glede na stopnjo izobrazbe udeležencev

Tabela 23 prikazuje opisno statistiko za posamezne dimenzije informacijske varnostne kulture glede na stopnjo dosežene izobrazbe.

Tabela 23: Opisna statistika za dimenzije glede na stopnjo dosežene izobrazbe na področju zdravstvene nege

Stopnja dosežene izobrazbe	Dimenzije	n	M	SD	Me	Q1	Q2
SMS/ZT/TZN	PO	124	6,11	1,31	6,70	5,50	7,00
	SO	124	5,97	1,19	5,80	5,50	7,00
	PCM	124	5,78	1,22	6,00	5,25	7,00
	RM	124	5,08	1,38	5,50	4,00	5,50
	SETA	124	5,34	1,41	5,75	4,50	6,25
	TMC	124	4,95	1,46	5,50	4,00	5,50
	MON	124	4,95	1,58	5,33	4,00	6,00
	ISK	124	4,94	1,31	5,00	4,00	5,50
	ISKS	124	5,03	1,38	5,00	4,00	6,00

Stopnja dosežene izobrazbe	Dimenzije	n	M	SD	Me	Q1	Q2
VIŠ. MED. SES./VIŠ. MED. TEH	PO	19	6,19	1,45	7,00	5,50	7,00
	SO	19	5,93	1,97	5,50	5,20	7,00
	PCM	19	5,64	1,42	6,00	5,25	6,50
	RM	19	5,29	1,08	5,00	4,50	5,50
	SETA	19	5,36	1,57	6,00	4,50	7,00
	TMC	19	5,24	1,58	5,50	4,38	7,00
	MON	19	5,12	1,79	5,67	4,00	7,00
	ISK	19	4,92	1,44	5,50	4,00	5,50
	ISKS	19	4,76	1,64	5,25	3,50	6,00
DIPL. M. S./DIPL. ZN	PO	308	6,18	1,22	6,70	5,80	7,00
	SO	308	5,84	1,22	5,80	5,35	7,00
	PCM	308	5,66	1,37	6,00	5,00	7,00
	RM	308	5,08	1,37	5,50	4,00	6,00
	SETA	308	5,35	1,43	5,63	4,50	6,50
	TMC	308	5,15	1,45	5,50	4,00	6,63
	MON	308	4,73	1,70	5,00	4,00	6,00
	ISK	308	4,97	1,44	5,50	4,00	5,50
	ISKS	308	4,92	1,44	5,00	4,00	6,00
MAG. ZDR. NEGE	PO	76	6,26	1,11	6,85	5,95	7,00
	SO	76	5,99	1,24	6,25	5,50	7,00
	PCM	76	5,64	1,44	6,00	5,25	6,50
	RM	76	5,14	1,54	5,50	4,00	6,50
	SETA	76	5,30	1,59	5,50	4,50	6,50
	TMC	76	5,17	1,71	5,50	4,00	7,00
	MON	76	4,91	1,69	5,33	4,00	6,00
	ISK	76	5,11	1,52	5,50	4,00	6,50
	ISKS	76	5,05	1,62	5,50	4,00	6,00

Legenda: M – povprečna vrednost, SD –standardni odklon, Me – mediana, Q1 – 1. kvartil, Q3 – 3. kvartil, SMS/ZT/TZN – srednja medicinska sestra/zdravstveni tehnik/tehnik zdravstvene nege, VIŠ. MED. SES./VIŠ. MED. TEH – višja medicinska sestra/višji medicinski tehnik, DIPL. M. S./DIPL. ZN – diplomirana medicinska sestra/diplomirani zdravstvenik, MAG. ZDR. NEGE – magister/magistrica zdravstvene nege

Rezultati Kruskal-Wallisovega H testa so pokazali, da ni statistično značilnih razlik v povprečnih vrednostih rangov dimenzij informacijske varnostne kulture glede na stopnjo izobrazbe (tabela 24).

Tabela 24: Kruskal-Wallis H test za razlike v zaznavanju dimenzij glede na stopnjo dosežene izobrazbe na področju zdravstvene nege

Dimenzije	χ^2	*p*
PO	1,005	0,800
SO	2,243	0,524
PCM	0,455	0,929
RM	0,457	0,928
SETA	0,084	0,994
TMC	2,347	0,504
MON	2,407	0,492
ISK	1,105	0,776
ISKS	1,668	0,644

Izvedli smo dodatno analizo. Spremenljivko stopnjo izobrazbe smo rekodirali v dve skupini. S tem smo udeležence razdelili v dve večji skupini glede na doseženo stopnje izobrazbe (brez diplome in z diplomo). Tabela 25 prikazuje opisno statistiko za posamezne dimenzije informacijske varnostne kulture glede na udeležence z diplomo in brez diplome.

Tabela 25: Opisna statistika za dimenzije glede na posedovanje diplome

Izobrazba	Dimenzije	n	M	SD	Me	Q1	Q2
	PO	143	6,12	1,32	6,70	5,50	7,00
	SO	143	5,97	1,16	5,80	5,50	7,00
brez diplome	PCM	143	5,76	1,25	6,00	5,25	7,00
SMS/ZT/TZN in	RM	143	5,11	1,34	5,50	4,00	5,50
VIŠ. MED.	SETA	143	5,34	1,43	5,75	4,50	6,25
SES./VIŠ. MED.	TMC	143	4,99	1,47	5,50	4,00	5,50
TEH	MON	143	4,97	1,60	5,33	4,00	6,00
	ISK	143	4,93	1,32	5,00	4,00	5,50
	ISKS	143	4,99	1,42	5,00	4,00	6,00
	PO	384	6,20	1,20	6,70	5,80	7,00
	SO	384	5,87	1,22	5,80	5,50	7,00
z diplomo	PCM	384	5,66	1,38	6,00	5,00	7,00
DIPL. M.	RM	384	5,09	1,40	5,50	4,00	6,00
S./DIPL. ZN in	SETA	384	5,34	1,46	5,50	4,50	6,50
MAG. ZDR.	TMC	384	5,15	1,51	5,50	4,00	6,63
NEGE	MON	384	4,77	1,70	5,00	4,00	6,00
	ISK	384	5,00	1,45	5,50	4,00	5,75
	ISKS	384	4,95	1,48	5,00	4,00	6,00

Legenda: M – povprečna vrednost, SD – standardni odklon, Me – mediana, Q1 – 1. kvartil, Q3 – 3. kvartil

Izvedli smo Mann-Whitneyev U test, da bi identificirali razlike v zaznavanju dimenzij informacijske varnostne kulture med dvema skupinama udeležencev. Rezultati so pokazali, da ni statistično značilnih razlik v zaznavanju dimenzij informacijske varnostne kulture glede na omenjeni skupini (tabela 26).

Tabela 26: Rezultati Mann-Whitneyevega U testa za razlike v zaznavanju dimenzij med posameznimi stopnjami izobrazbe – z visokošolsko diplomo oz. več in ostale

Dimenzije	U	Wilcoxon W	Z	p
PO	26682,0	36978,0	-0,527	0,598
SO	26467,0	100387,0	-,0514	0,607
PCM	26667,0	100587,0	-0,514	0,607
RM	27305,5	37601,5	-0,098	0,922
SETA	27348,0	37644,0	-0,070	0,944
TMC	25635,5	35931,5	-1,189	0,234
MON	25669,0	99589,0	-1,157	0,247
ISK	26271,0	36567,0	-,0777	0,437
ISKS	27116,0	101036,0	-0,220	0,826

4.1.5 Izračun razlik v zaznavanju dimenzij glede na organizacijo zaposlitve udeležencev

Tabela 27 prikazuje opisno statistiko za posamezne dimenzije informacijske varnostne kulture glede na organizacijo, v kateri so zaposleni udeleženci v zdravstveni negi. Rezultati Kruskal-Wallisovega H testa so pokazali, da ni statistično značilnih razlik v povprečnih vrednostih rangov dimenzij informacijske varnostne kulture med organizacijami (tabela 28).

Tabela 27: Opisna statistika za dimenzije glede na tip organizacije, v kateri so zaposleni udeleženci

Tip organizacije	Dimenzije	n	M	SD	Me	Q1	Q2
Zdravstveni dom	PO	128	6,00	1,50	6,70	5,50	7,00
	SO	128	5,86	1,33	6,10	5,35	7,00
	PCM	128	5,64	1,24	6,00	5,00	6,50
	RM	128	5,11	1,40	5,50	4,00	6,00
	SETA	128	5,41	1,40	5,75	4,75	6,50
	TMC	128	5,09	1,51	5,50	4,00	6,63
	MON	128	4,81	1,64	5,00	4,00	6,00
	ISK	128	5,02	1,34	5,50	4,00	5,50
	ISKS	128	4,89	1,52	5,00	4,00	6,00
Splošna bolnišnica	PO	100	6,23	1,16	6,70	5,80	7,00
	SO	100	5,94	1,21	6,10	5,35	7,00
	PCM	100	5,83	1,36	6,00	5,50	7,00
	RM	100	5,06	1,48	5,50	4,00	6,00
	SETA	100	5,34	1,52	5,75	5,00	6,25
	TMC	100	5,19	1,51	5,50	4,00	6,44
	MON	100	5,04	1,66	5,50	4,00	6,33
	ISK	100	5,02	1,33	5,50	4,00	5,50
	ISKS	100	4,97	1,42	5,00	4,00	6,00
Specialistična bolnišnica	PO	24	6,10	1,15	6,55	5,50	7,00
	SO	24	5,70	1,42	5,80	5,20	7,00
	PCM	24	5,55	1,31	5,50	4,63	7,00
	RM	24	5,00	1,29	5,50	4,50	5,50
	SETA	24	4,76	1,59	5,13	4,00	5,75
	TMC	24	5,05	1,09	5,13	4,19	5,50
	MON	24	4,74	1,38	4,67	4,00	5,67
	ISK	24	4,85	1,46	5,00	4,00	5,50
	ISKS	24	4,75	1,22	4,75	4,00	5,75
Klinični center (vključno s klinikami)	PO	109	6,23	1,12	6,70	5,80	7,00
	SO	109	5,95	1,08	5,80	5,50	7,00
	PCM	109	5,67	1,51	6,00	5,25	7,00
	RM	109	5,21	1,36	5,50	4,00	6,00
	SETA	109	5,50	1,49	6,00	4,50	7,00
	TMC	109	5,14	1,46	5,50	4,00	6,63
	MON	109	4,83	1,74	5,33	4,00	6,00
	ISK	109	5,11	1,35	5,50	4,00	5,50
	ISKS	109	5,01	1,49	5,50	4,00	6,00

Tip organizacije	Dimenzije	n	M	SD	Me	Q1	Q2
Klinika (samostojna)	PO	16	6,59	0,67	7,00	5,95	7,00
	SO	16	6,18	0,93	6,40	5,50	7,00
	PCM	16	5,89	1,53	6,13	6,00	6,88
	RM	16	5,53	1,36	5,50	4,00	7,00
	SETA	16	5,53	1,44	5,75	4,88	6,75
	TMC	16	5,10	1,71	5,50	4,19	6,44
	MON	16	5,10	1,95	6,00	4,00	6,50
	ISK	16	5,09	1,78	5,25	4,00	6,75
	ISKS	16	5,27	1,60	6,00	4,75	6,00
Inštitut	PO	7	5,63	1,20	5,50	4,60	7,00
	SO	7	5,41	1,23	5,20	4,00	7,00
	PCM	7	5,14	0,98	5,00	4,50	6,25
	RM	7	4,29	1,19	4,50	3,00	5,50
	SETA	7	4,57	1,43	5,00	3,50	6,00
	TMC	7	3,46	1,18	4,00	2,88	4,00
	MON	7	3,90	1,07	4,00	3,00	4,67
	ISK	7	3,71	0,86	4,00	2,50	4,50
	ISKS	7	3,54	1,01	3,75	2,75	4,25
Socialnovarstveni zavod	PO	125	6,22	1,17	6,70	5,80	7,00
	SO	125	5,82	1,20	5,80	5,50	7,00
	PCM	125	5,67	1,28	6,00	5,00	6,50
	RM	125	4,99	1,36	5,00	4,00	5,50
	SETA	125	5,24	1,38	5,50	4,50	6,25
	TMC	125	5,10	1,51	5,50	4,00	5,88
	MON	125	4,67	1,63	5,00	4,00	6,00
	ISK	125	4,84	1,50	5,50	4,00	5,50
	ISKS	125	4,97	1,41	5,25	4,00	6,00
Drugo	PO	17	6,49	1,12	7,00	6,40	7,00
	SO	17	6,31	0,84	6,70	5,50	7,00
	PCM	17	5,60	1,47	5,75	5,25	7,00
	RM	17	5,35	1,39	5,50	5,00	6,50
	SETA	17	5,44	1,52	6,00	4,50	6,75
	TMC	17	5,48	1,71	5,50	5,13	7,00
	MON	17	4,82	2,14	5,67	3,00	6,33
	ISK	17	5,21	1,90	5,50	4,50	7,00
	ISKS	17	5,49	1,63	6,00	4,50	7,00

Legenda: M – povprečna vrednost, SD – standardni odklon, Me – mediana, Q1 – 1. kvartil, Q3 – 3. kvartil

Tabela 28: Kruskal-Wallis H test za razlike v zaznavanju dimenzij glede na tip organizacije, v kateri so zaposleni udeleženci

Dimenzije	χ^2	s. p.	p
PO	8,182	7	0,317
SO	5,373	7	0,615
PCM	7,752	7	0,355
RM	7,094	7	0,419
SETA	11,160	7	0,132
TMC	10,711	7	0,152
MON	7,753	7	0,355
ISK	9,313	7	0,231
ISKS	12,840	7	0,076

4.1.6 Izračun razlik v zaznavanju dimenzij glede na nivoje zdravstvenega varstva, v katerih so zaposlenih udeleženci

Izvedli smo dodatno analizo, kjer smo spremenljivko tip organizacije rekodirali v nivoje zdravstvenega varstva ter socialno varstveni zavod. S tem smo udeležence razdelili v štiri večje skupine. Tabela 29 prikazuje opisno statistiko za posamezne konstrukte informacijske varnostne kulture glede na zaposlitev v nivojih zdravstvenega varstva in socialno varstvenih zavodih.

Tabela 29: Opisna statistika za dimenzije glede na nivoje zdravstvenega varstva

Nivoji zdravstvenega varstva	Dimenzije	n	M	SD	Me	Q1	Q2
I (zdravstveni dom)	PO	128	6,00	1,50	6,70	5,50	7,00
	SO	128	5,86	1,33	6,10	5,35	7,00
	PCM	128	5,64	1,24	6,00	5,00	6,50
	RM	128	5,11	1,40	5,50	4,00	6,00
	SETA	128	5,41	1,40	5,75	4,75	6,50
	TMC	128	5,09	1,51	5,50	4,00	6,63
	MON	128	4,81	1,64	5,00	4,00	6,00
	ISK	128	5,02	1,34	5,50	4,00	5,50
	ISKS	128	4,89	1,52	5,00	4,00	6,00
II (splošna in specialistična bolnišnica)	PO	124	6,20	1,15	6,70	5,80	7,00
	SO	124	5,89	1,25	5,95	5,20	7,00
	PCM	124	5,77	1,35	6,00	5,25	7,00
	RM	124	5,05	1,44	5,50	4,00	5,75
	SETA	124	5,23	1,55	5,50	4,75	6,25
	TMC	124	5,16	1,43	5,50	4,00	6,25
	MON	124	4,98	1,61	5,17	4,00	6,00
	ISK	124	4,99	1,35	5,25	4,00	5,50
	ISKS	124	4,93	1,38	5,00	4,00	6,00
III (klinični center (vključno s klinikami), klinika samostojna, inštitut)	PO	132	6,24	1,09	6,70	5,65	7,00
	SO	132	5,95	1,07	5,80	5,50	7,00
	PCM	132	5,67	1,48	6,00	5,13	7,00
	RM	132	5,20	1,36	5,50	4,00	6,00
	SETA	132	5,45	1,49	6,00	4,50	7,00
	TMC	132	5,05	1,52	5,13	4,00	6,25
	MON	132	4,82	1,74	5,00	4,00	6,00
	ISK	132	5,04	1,41	5,50	4,00	5,50
	ISKS	132	4,96	1,52	5,00	4,00	6,00
Socialno-varstveni zavodi	PO	125	6,22	1,17	6,70	5,80	7,00
	SO	125	5,82	1,20	5,80	5,50	7,00
	PCM	125	5,67	1,28	6,00	5,00	6,50
	RM	125	4,99	1,36	5,00	4,00	5,50
	SETA	125	5,24	1,38	5,50	4,50	6,25
	TMC	125	5,10	1,51	5,50	4,00	5,88
	MON	125	4,67	1,63	5,00	4,00	6,00
	ISK	125	4,84	1,50	5,50	4,00	5,50
	ISKS	125	4,97	1,41	5,25	4,00	6,00

Nivoji zdravstvenega varstva	Dimenzije	n	M	SD	Me	Q1	Q2
Drugo	PO	17	6,49	1,12	7,00	6,40	7,00
	SO	17	6,31	0,84	6,70	5,50	7,00
	PCM	17	5,60	1,47	5,75	5,25	7,00
	RM	17	5,35	1,39	5,50	5,00	6,50
	SETA	17	5,44	1,52	6,00	4,50	6,75
	TMC	17	5,48	1,71	5,50	5,13	7,00
	MON	17	4,82	2,14	5,67	3,00	6,33
	ISK	17	5,21	1,90	5,50	4,50	7,00
	ISKS	17	5,49	1,63	6,00	4,50	7,00

Legenda: M – povprečna vrednost, SD – standardni odklon, Me – mediana, Q1 – 1. kvartil, Q3 – 3. kvartil

Rezultati Kruskal-Wallisovega H testa so pokazali, da ni statistično značilnih razlik v povprečnih vrednostih rangov dimenzij informacijske varnostne kulture glede na nivoje zdravstvenega varstva (tabela 30).

Tabela 30: Kruskal-Wallis H test za razlike v zaznavanju dimenzij glede na nivo zdravstvenega varstva

Dimenzije	χ^2	p
PO	2,974	0,562
SO	2,169	0,705
PCM	2,438	0,656
RM	2,651	0,618
SETA	3,887	0,422
TMC	2,150	0,708
MON	2,558	0,634
ISK	2,008	0,734
ISKS	3,310	0,507

4.2 REZULTATI, KI SE NANAŠAJO NA SMERNICE PLS-SEM

Nekateri rezultati, ki se nanašajo na PLS-SEM so že predstavljeni v poglavju *Predhodna vprašanja, povezana z vidiki uporabe PLS-SEM* (velikost vzorca, porazdelitev podatkov, GoF) ter poglavju *Ocena merilnega modela z reflektivnimi konstrukti* (CA, CR, AVE, Fornell-Lackerjev kriterij ter HTMT). V nadaljevanju so predstavljeni rezultati *Ocene strukturnega modela*. Rezultati statistična značilnost in relevantnost koeficientov poti se navezujejo na potrjevanje hipotez. Za lažjo interpretacijo rezultatov smo za vse domnevne povezave izračunali velikosti učinka (f^2) in intervale zaupanja (CI: 2,5–97,5 %) (Dziak, et al., 2020).

4.2.1 Kolinearnost modela

V Tabeli 31 je prikazana kolinearna statistika za notranji (strukturni) model z reflektivnimi konstrukti. Iz tabele je razvidno, da najvišja vrednost VIF znaša 3,830. Vrednost po nekaterih avtorjih presega priporočeno vrednost 3,3 – vendar pa nobena od njih ne presega ravno tako priporočene mejne vrednosti 5. Prav tako smo se oprli na navedbo Kock in Lynn (2012), ki navajata, da se višje vrednosti pojavljajo ob uporabi algoritmov, ki vključujejo merilno napako. Glede na zgoraj navedena dejstva, lahko zaključimo, da multikolinearnost med konstrukti ne dosega kritičnih ravni.

Tabela 31: Kolinearnost – VIF vrednosti za notranji model

	ATB	BI	ISK	ISKS	MON	NB	PBC	PCM	PO	RM	SETA	SN	SO	TMC
ATB		1,892												
BI														
ISK	2,698					2,698	2,698					2,698		
ISKS	3,023					3,023	3,023					3,023		
MON	3,418					3,418	3,418					3,418		
NB		2,250												
PBC		1,149												
PCM	2,416					2,416	2,416					2,416		
PO	2,027					2,027	2,027					2,027		
RM	3,544					3,544	3,544					3,544		
SETA	3,830					3,830	3,830					3,830		
SN		2,377												
SO	2,953					2,953	2,953					2,953		
TMC	3,499					3,499	3,499					3,499		

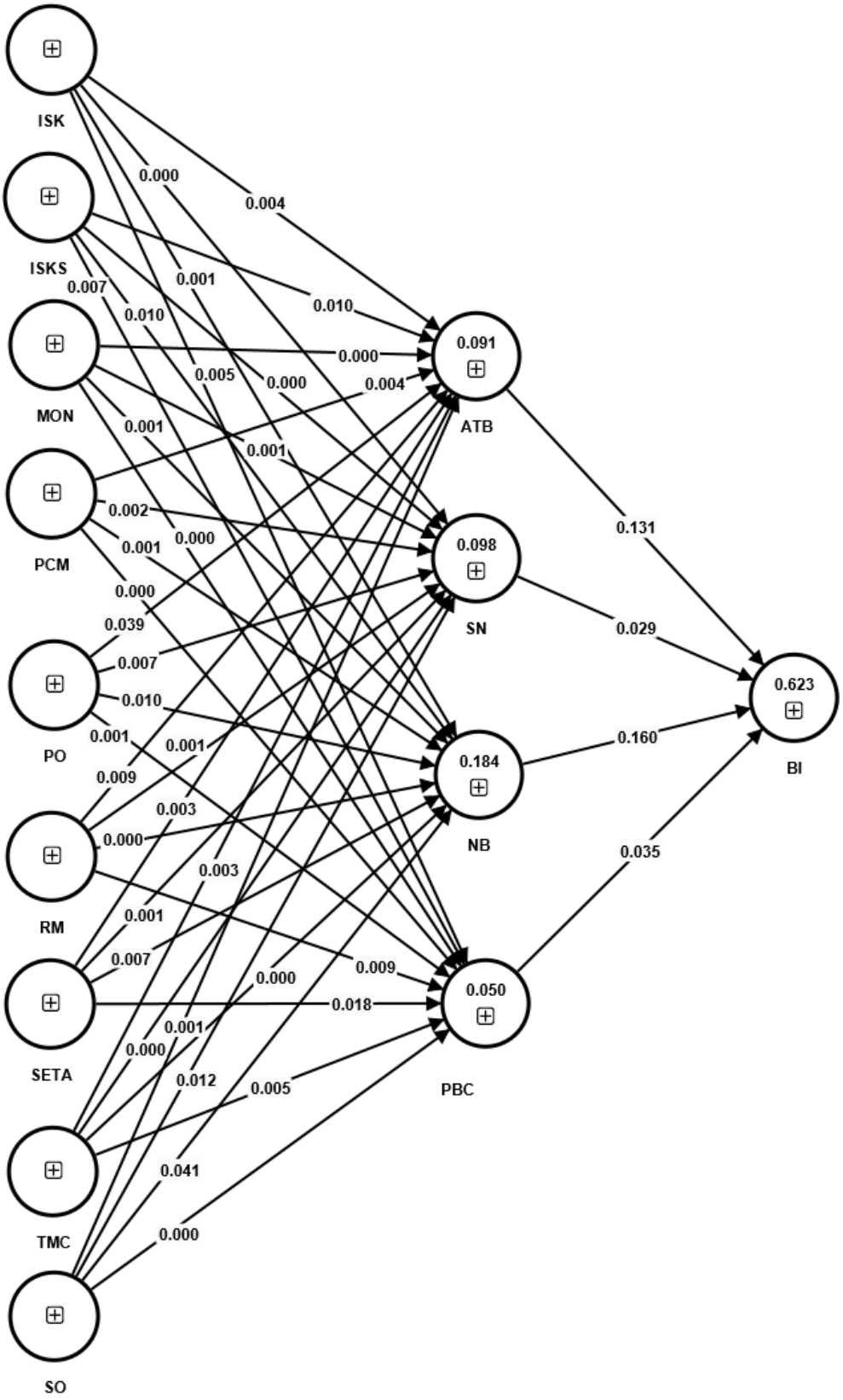
4.2.2 Pojasnjevalna in napovedna moč modela

V Tabeli 32 so prikazane vrednosti R^2, f^2 in Q^2. Rezultati kažejo, da so vse vrednosti R^2 nad 0,1, zato govorimo o vzpostavljeni pojasnjevalni sposobnosti modela. Vrednost Q^2 nad 0 kaže, da ima model napovedno relevantnost, t.j. prediktorni pomen endogenega konstrukta.

Tabela 32: Izračun vrednosti R^2, f^2 in Q^2

Prediktor	Odvisna spremenljivka	R^2	f^2	Q^2
SO			0,001	
PO			0,039	
PCM			0,004	
RM			0,009	
SETA	ATB	0,091	0,003	0,020
TMC			0,003	
ISKS			0,010	
MON			0,000	
ISK			0,004	
SO			0,012	
PO			0,007	
PCM			0,002	
RM			0,001	
SETA	SN	0,098	0,001	0,042
TMC			0,000	
ISKS			0,000	
MON			0,001	
ISK			0,000	
SO			**0,041**	
PO			0,010	
PCM			0,001	
RM			0,000	
SETA	NB	0,184	0,007	0,111
TMC			0,000	
ISKS			0,010	
MON			0,001	
ISK			0,001	
SO			0,000	
PO			0,001	
PCM			0,000	
RM			0,009	
SETA	PBC	0,050	0,018	0,002
TMC			0,005	
ISKS			0,007	
MON			0,000	
ISK			0,005	
ATB			**0,131**	
SN	BI	0,623	**0,029**	0,025
NB			**0,160**	
PBC			**0,035**	

Iz Slike 15 je razvidno, da je R^2 vrednost za BI (endogena latentna spremenljivka) 0,623, kar pomeni, da štiri latentne spremenljivke – ATB, SN, NB in PBC pojasnijo 62,3 % variance BI. Notranji model prikazuje, da imajo NB največji učinek ($f^2 = 0,160$) na BI. Sledijo mu ATB ($f^2 = 0,131$), PBC ($f^2 = 0,035$) in SN ($f^2 = 0,029$).



Slika 15: Ocenjevanje strukturnega modela – R^2 in f^2

4.2.3 Napovedna moč modela zunaj vzorca

V Tabeli 33 je prikazan povzetek napovedne moči modela. Vse vrednosti Q^2 so nad 0; vrednosti PLS-SEM RMSE in PLS-SEM MAE pa so višje napram vrednostim LM RMSE in LM MAE, razen za elemente PBC2 in PBC3, vendar vrednost Q^2 rangira nekaj nad 0. Glede na vrednosti lahko zaključimo, da ima model razmeroma dobro napovedno moč z zelo malo napake.

Tabela 33: PLSpredict

Latentne spremenljivke – napoved				**Manifestne spremenljivke – napoved**					
	Q²predict	RMSE	MAE		Q²predict	PLS-SEM RMSE	PLS-SEM MAE	LM RMSE	LM MAE
				ATB1	0,016	0,967	0,537	0,984	0,566
ATB	0,020	1,021	0,576	ATB2	0,021	0,876	0,475	0,899	0,510
				ATB3	0,007	0,920	0,502	0,937	0,541
				BI1	0,021	1,110	0,817	1,132	0,828
BI	0,025	1,000	0,722	BI2	0,017	1,098	0,791	1,123	0,808
				BI3	0,028	1,126	0,824	1,147	0,826
				NB1	0,065	0,783	0,478	0,806	0,498
NB	0,111	0,956	0,624	NB2	0,092	1,163	0,814	1,205	0,830
				NB3	0,108	0,926	0,581	0,968	0,618
				PBC1	0,015	2,154	1,807	2,220	1,816
PBC	0,002	1,003	0,834	PBC2	-0,003	2,177	1,834	2,223	1,825
				PBC3	-0,008	2,119	1,745	2,188	1,777
				SN1	0,036	1,216	0,949	1,266	0,967
SN	0,042	0,988	0,744	SN2	0,032	1,148	0,880	1,183	0,886
				SN3	0,033	1,075	0,770	1,097	0,774

4.2.4 Statistična značilnost in relevantnost koeficientov poti

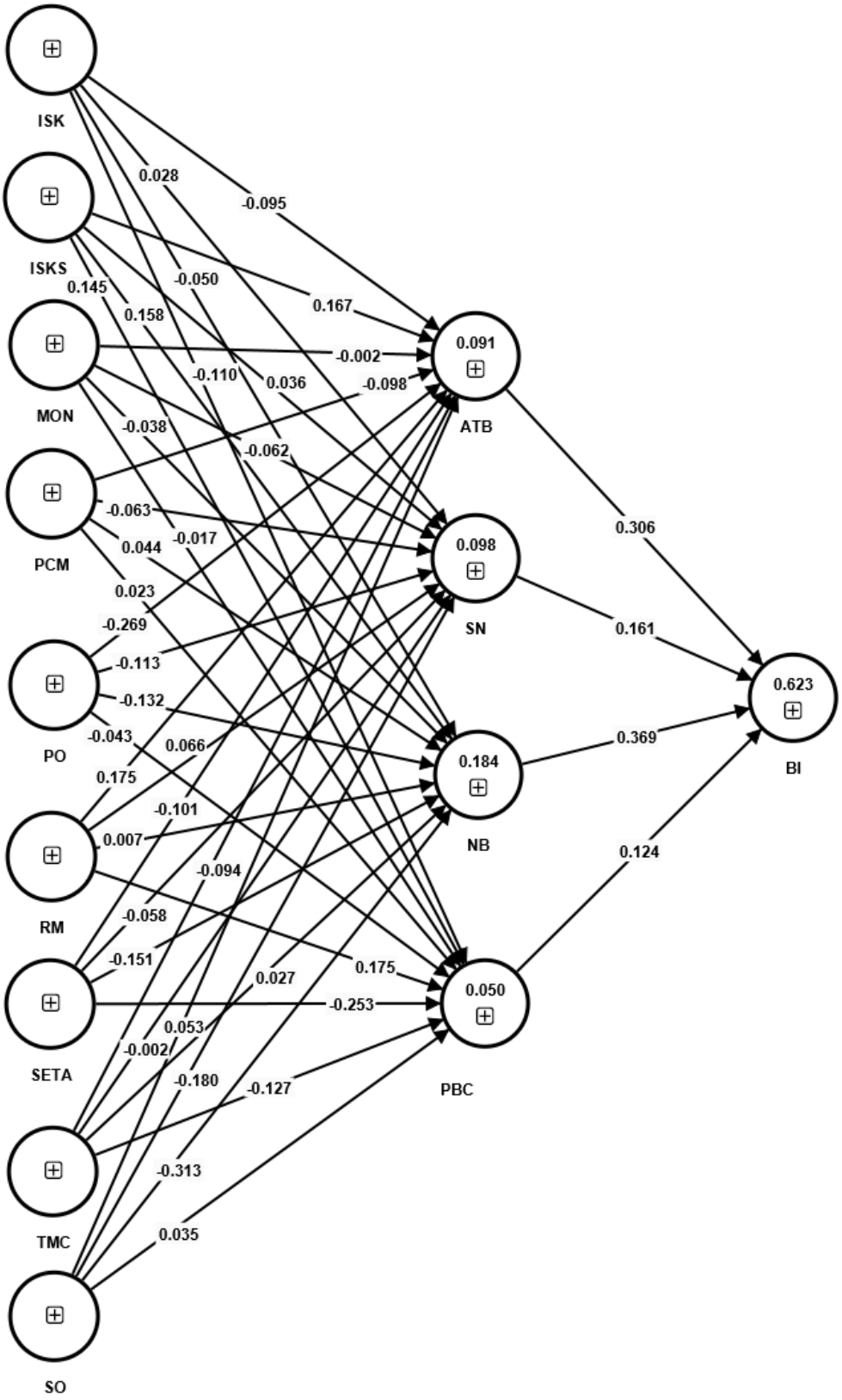
Na Sliki 16 in 17 so prikazani koeficienti poti in njihova statistična značilnost. Zeleno obarvane povezave so statistično značilne. Rezultati analize, prikazani v Tabeli 32 in Tabeli 34 ter na Sliki 17 kažejo, da imajo negativno povezanost z ATB dimenzije PO, PCM, SETA, TMC, MON in ISK. Izmed naštetih pa ima statistično značilno povezanost z ATB samo PO (*β = -0,269; f^2 = 0,039; t = 2,118; p = 0,034; 97,5 % CI [-0,525; -0,029]*). Za obratno se je kot pozitivna povezanost z ATB, ki je obenem tudi statistično značilna (*β = 0,167; f^2 = 0,010; t = 2,385; p = 0,017; 97,5 % CI [0,030; 0,304]*) pokazala dimenzija ISKS.

Rezultati analize, prikazani v Tabeli 32 in Tabeli 34 ter na Sliki 17 kažejo, da imajo negativno povezanost s SN dimenzije SO, PO, PCM, SETA, TMC in MON, vendar nobena izmed njih ni statistično značilna. Negativno povezanost z NB imajo dimenzije PO, SETA, MON in SO. Izmed naštetih pa ima statistično značilno povezanost z NB le dimenzija SO (*β = -0,313; f^2 = 0,041; t = 3,320; p = 0,001; 97,5 % CI [-0,490; -0,117]*).

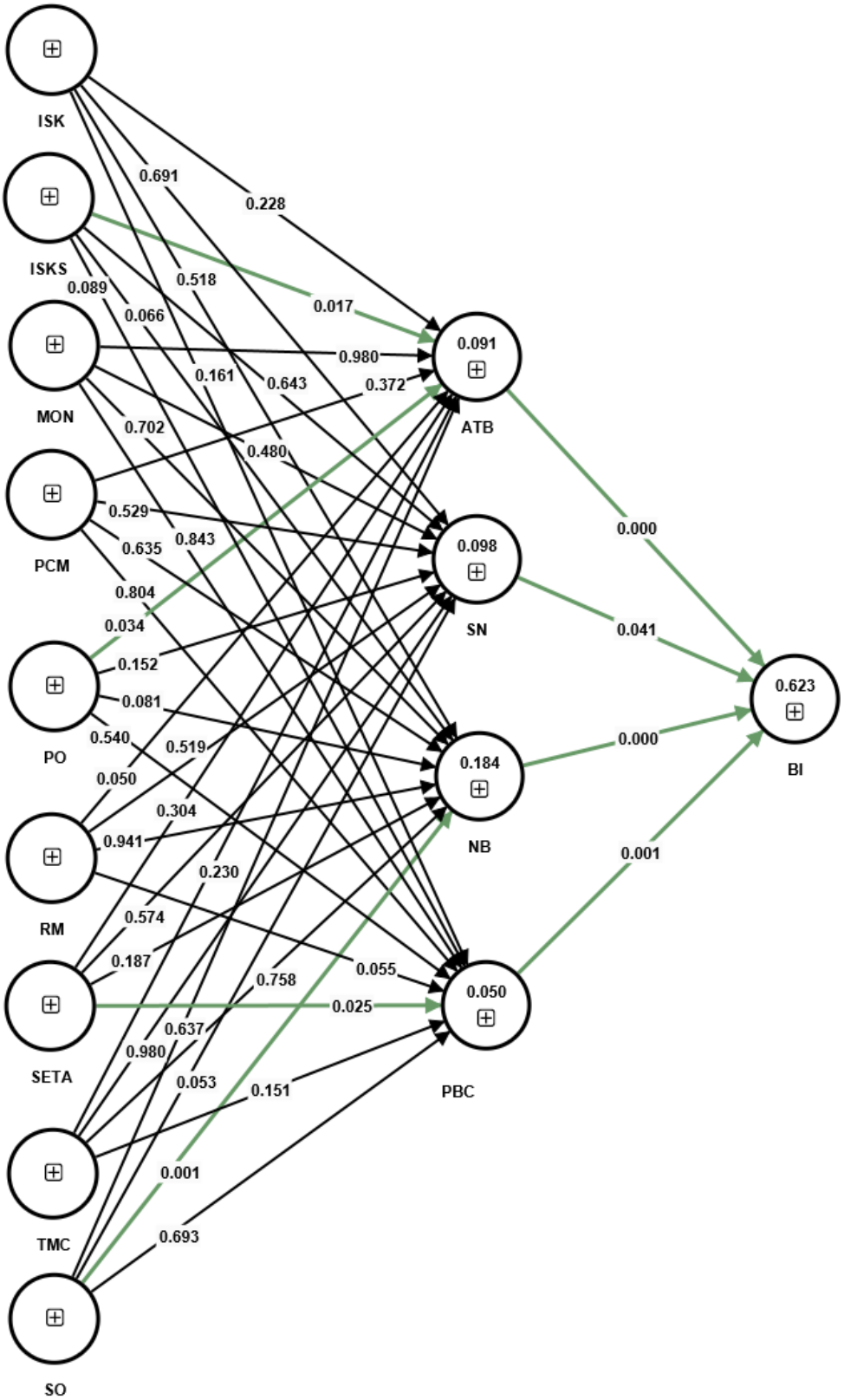
Rezultati analize, prikazani v Tabeli 32 in Tabeli 34 ter na Sliki 17 kažejo, da imajo negativno povezanost s PBC dimenzije PO, SETA in TMC. Izmed naštetih ima samo SETA statistično značilno povezanost s PBC (*β = -0,253; f^2=0,018; t = 2,235; p = 0,025; 97,5% CI [-0,471; -0,032]*).

Rezultati v Tabeli 32 in Tabeli 34 ter na Sliki 17 kažejo, da je povezanost ATB z BI pozitivna in statistično značilna (*β = 0,306; f^2=0,131; t = 3,865; p < 0,001; 97,5 % CI [0,168; 0,481]*). Povezanost SN in BI je pozitivna in statistično značilna (*β = 0,161; f^2 = 0,029; t = 2,046; p = 0,041; 97,5 % CI [0,000; 0,307]*) in prav tako je povezanost NB z BI pozitivna in statistično
značilna (*β = 0,369; f^2= 0,160; t = 3,615; p < 0,001; 97,5 % CI [0,163; 0,570]*).

Povezanost PBC z BI je pozitivna in statistično značilna (*β = 0,124; f^2= 0,035; t =3,272; p = 0,001; 97,5 % CI [0,049; 0,193]*).



Slika 16: Ocenjevanje strukturnega modela – R^2 in koeficienti poti



Slika 17: Ocenjevanje strukturnega modela – statistična značilnost in relevantnost koeficientov poti

Tabela 34: Rezultati relevantnosti in statistične značilnosti – rezultati metode ponovnega vzorčenja koeficientov poti in njihovih t-statistik (notranji model)

Pot	SD	*t*	*p*	2,50 %	97,5 %	*β*
SO → ATB	0,112	0,472	0,637	-0,160	0,278	0,053
SO → SN	0,093	1,935	0,053	-0,353	0,012	-0,180
SO → NB	0,094	3,320	**0,001**	-0,490	-0,117	-0,313
SO → PBC	0,088	0,395	0,693	-0,138	0,209	0,035
PO → ATB	0,127	2,118	**0,034**	-0,525	-0,029	-0,269
PO → SN	0,079	1,434	0,152	-0,278	0,029	-0,113
PO → NB	0,076	1,744	0,081	-0,282	0,014	-0,132
PO → PBC	0,071	0,613	0,540	-0,193	0,088	-0,043
PCM → ATB	0,110	0,894	0,372	-0,320	0,102	-0,098
PCM → SN	0,100	0,630	0,529	-0,250	0,128	-0,063
PCM → NB	0,093	0,475	0,635	-0,134	0,228	0,044
PCM → PBC	0,093	0,248	0,804	-0,158	0,210	0,023
RM → ATB	0,089	1,960	0,050	-0,004	0,352	0,175
RM → SN	0,102	0,644	0,519	-0,141	0,258	0,066
RM → NB	0,094	0,074	0,941	-0,180	0,184	0,007
RM → PBC	0,091	1,920	0,055	-0,016	0,350	0,175
SETA → ATB	0,098	1,028	0,304	-0,289	0,095	-0,101
SETA → SN	0,103	0,562	0,574	-0,255	0,146	-0,058
SETA → NB	0,114	1,321	0,187	-0,364	0,085	-0,151
SETA → PBC	0,113	2,235	**0,025**	-0,471	-0,032	-0,253
TMC → ATB	0,078	1,201	0,230	-0,252	0,056	-0,094
TMC → SN	0,094	0,025	0,980	-0,189	0,180	-0,002
TMC → NB	0,088	0,308	0,758	-0,152	0,193	0,027
TMC → PBC	0,089	1,437	0,151	-0,303	0,044	-0,127
ISKS → ATB	0,070	2,385	**0,017**	0,030	0,304	0,167
ISKS → SN	0,077	0,464	0,643	-0,123	0,188	0,036
ISKS → NB	0,086	1,841	0,066	-0,012	0,325	0,158
ISKS → PBC	0,085	1,703	0,089	-0,030	0,302	0,145
MON → ATB	0,092	0,025	0,980	-0,189	0,180	-0,002
MON → SN	0,088	0,706	0,480	-0,234	0,113	-0,062
MON → NB	0,099	0,383	0,702	-0,234	0,159	-0,038
MON → PBC	0,088	0,198	0,843	-0,191	0,155	-0,017
ISK → ATB	0,079	1,205	0,228	-0,252	0,062	-0,095
ISK → SN	0,070	0,397	0,691	-0,114	0,165	0,028
ISK → NB	0,078	0,647	0,518	-0,201	0,101	-0,050
ISK → PBC	0,079	1,402	0,161	-0,256	0,049	-0,110
ATB → BI	0,079	3,865	**0,000**	0,168	0,481	0,306
SN → BI	0,079	2,046	**0,041**	0,000	0,307	0,161
NB → BI	0,102	3,615	**0,000**	0,163	0,570	0,369
PBC → BI	0,038	3,272	**0,001**	0,049	0,193	0,124

Izračunali smo tudi skupni učinek (tabela 35) ter skupni posredni učinek (tabela 36) eksogenih spremenljivk na endogene. Rezultati so pokazali, da ima največji učinek na BI dimenzija PO (*t = 2,346, p = 0,019*). Posredni učinek za BI imata dimenziji ISKS (*t = 2,155, p = 0,031, β = 0,133*) in PO (*t = 2,346, p = 0,019, β = 0,154*).

Tabela 35: Skupni učinek

Pot	SD	*t*	*p*
ATB → BI	0,079	3,865	**< 0,001**
SN → BI	0,079	2,046	**0,041**
NB → BI	0,102	3,615	**< 0,001**
PBC → BI	0,038	3,272	**0,001**
PO → ATB	0,127	2,118	**0,034**
PO → SN	0,079	1,434	0,152
PO → NB	0,076	1,744	0,081
PO → PBC	0,071	0,613	0,540
PO → BI	0,066	2,346	**0,019**
SO → ATB	0,112	0,472	0,637
SO → SN	0,093	1,935	0,053
SO → NB	0,094	3,320	**0,001**
SO → PBC	0,088	0,395	0,693
SO → BI	0,076	1,620	0,105
PCM → ATB	0,110	0,894	0,372
PCM → SN	0,100	0,630	0,529
PCM → NB	0,093	0,475	0,635
PCM → PBC	0,093	0,248	0,804
PCM → BI	0,085	0,247	0,805
RM → ATB	0,089	1,960	0,050
RM → SN	0,102	0,644	0,519
RM → NB	0,094	0,074	0,941
RM → PBC	0,091	1,920	0,055
RM → BI	0,074	1,193	0,233
SETA → ATB	0,098	1,028	0,304
SETA → SN	0,103	0,562	0,574
SETA → NB	0,114	1,321	0,187
SETA → PBC	0,113	2,235	**0,025**
SETA → BI	0,081	1,565	0,118
TMC → ATB	0,078	1,201	0,230
TMC → SN	0,094	0,025	0,980
TMC → NB	0,088	0,308	0,758
TMC → PBC	0,089	1,437	0,151
TMC → BI	0,064	0,546	0,585
MON → ATB	0,092	0,025	0,980
MON → SN	0,088	0,706	0,480
MON → NB	0,099	0,383	0,702
MON → PBC	0,088	0,198	0,843
MON → BI	0,074	0,362	0,718
ISK → ATB	0,079	1,205	0,228
ISK → SN	0,070	0,397	0,691
ISK → NB	0,078	0,647	0,518
ISK → PBC	0,079	1,402	0,161
ISK → BI	0,059	0,963	0,336
ISKS → ATB	0,070	2,385	**0,017**
ISKS → SN	0,077	0,464	0,643
ISKS → NB	0,086	1,841	0,066
ISKS → PBC	0,085	1,703	0,089
ISKS → BI	0,062	2,155	**0,031**

Tabela 36: Skupni posredni učinek – rezultati relevantnosti in statistične značilnosti – rezultati metode ponovnega vzorčenja koeficientov poti in njihovih t-statistik

Pot	SD	*t*	*p*	2,50 %	97,5 %	*β*
PO → BI	0,066	2,346	**0,019**	-0,288	-0,025	-0,154
SO → BI	0,076	1,620	0,105	-0,271	0,031	-0,124
PCM → BI	0,085	0,247	0,805	-0,187	0,138	-0,021
RM → BI	0,074	1,193	0,233	-0,054	0,235	0,088
SETA → BI	0,081	1,565	0,118	-0,282	0,034	-0,127
TMC → BI	0,064	0,546	0,585	-0,166	0,085	-0,035
MON → BI	0,074	0,362	0,718	-0,176	0,116	-0,027
ISK → BI	0,059	0,963	0,336	-0,169	0,061	-0,057
ISKS → BI	0,062	2,155	**0,031**	0,007	0,248	0,133

Kot je razvidno iz Tabele 37, so vse vrednosti nasičenja (angl. »*loadings*«) zunanjega modela statistično značilne, saj so t-vrednosti višje od 1,96.

Tabela 37: T-statistika nasičenja zunanjega modela

	SD	*t*	*p*
ATB1 ← ATB	0,053	16,275	< **0,001**
ATB2 ← ATB	0,039	22,935	< **0,001**
ATB3 ← ATB	0,056	15,762	< **0,001**
SN1 ← SN	0,041	19,833	< **0,001**
SN2 ← SN	0,033	26,570	< **0,001**
SN3 ← SN	0,040	21,313	< **0,001**
NB1 ← NB	0,033	25,758	< **0,001**
NB2 ← NB	0,035	23,590	< **0,001**
NB3 ← NB	0,024	37,955	< **0,001**
PBC1← PBC	0,035	28,380	< **0,001**
PBC2 ← PBC	0,042	21,392	< **0,001**
PBC3 ← PBC	0,046	18,453	< **0,001**
BI1 ← BI	0,019	49,646	< **0,001**
BI2 ← BI	0,029	32,813	< **0,001**
BI3 ← BI	0,020	46,981	< **0,001**
PO1 ← PO	0,085	9,660	< **0,001**
PO2 ← PO	0,072	12,129	< **0,001**
PO3 ← PO	0,059	16,554	< **0,001**
PO4 ← PO	0,044	22,105	< **0,001**
PO5 ← PO	0,092	7,657	< **0,001**
SO1 ←SO	0,052	16,942	< **0,001**
SO2 ←SO	0,050	17,947	< **0,001**
SO3 ←SO	0,040	23,558	< **0,001**
SO4 ←SO	0,041	22,799	< **0,001**
SO5 ←SO	0,064	10,693	< **0,001**
PCM1 ←PCM	0,091	10,276	< **0,001**
PCM2 ←PCM	0,076	14,273	< **0,001**
PCM3 ←PCM	0,126	5,288	< **0,001**
PCM4 ←PCM	0,134	4,207	< **0,001**
RM1 ←RM	0,086	10,817	< **0,001**
RM2 ←RM	0,072	13,988	< **0,001**
RM3 ←RM	0,102	7,380	< **0,001**

	SD	***t***	***p***
SETA1 ←SETA	0,075	13,046	< **0,001**
SETA2 ←SETA	0,081	10,604	< **0,001**
SETA3 ←SETA	0,079	10,878	< **0,001**
SETA4 ←SETA	0,099	6,704	< **0,001**
TMC1 ←TMC	0,067	14,126	< **0,001**
TMC2 ←TMC	0,043	21,712	< **0,001**
TMC3 ←TMC	0,058	15,810	< **0,001**
TMC4 ←TMC	0,066	14,601	< **0,001**
MON1 ←MON	0,081	11,909	< **0,001**
MON2 ←MON	0,078	12,342	< **0,001**
MON3 ←MON	0,065	13,224	< **0,001**
ISK1 ←ISK	0,116	8,520	< **0,001**
ISK2 ←ISK	0,074	12,660	< **0,001**
ISK3 ←ISK	0,112	6,806	< **0,001**
ISKS1 ←ISKS	0,099	10,515	< **0,001**
ISKS2 ←ISKS	0,087	10,782	< **0,001**
ISKS3 ←ISKS	0,121	6,219	< **0,001**
ISKS4 ←ISKS	0,090	9,579	< **0,001**

4.3 REZULTATI PREVERJANJA HIPOTEZ

V nadaljevanju sledi predstavitev rezultatov preverjanja hipotez, rezultatov, ki se navezujejo na cilj 3 ter raziskovalno vprašanje doktorske disertacije. Rezultati preverjanja hipotez H1–H6 so prikazani v Tabeli 32 in Tabeli 34 ter na Sliki 17.

4.3.1 Rezultati preverjanja hipotez

H1 se glasi: »Dimenzije informacijske varnostne kulture so negativno povezane z ATB zaposlenih v zdravstveni negi glede izvedbe nepooblaščenega dostopa do zdravstvenih podatkov«. Rezultati kažejo, da ima negativno statistično značilno povezanost z ATB samo dimenzija PO (*β = -0,269; f^2 = 0,039; t = 2,118; p = 0,034; 97,5 % CI [-0,525; -0,029]*). Pozitivno statistično značilno povezanost (*β = 0,167; f^2 = 0,010; t = 2,385; p = 0,017; 97,5 % CI [0,030; 0,304]*) z ATB ima dimenzija ISKS. H1 lahko samo delno potrdimo.

H2 se glasi: »Dimenzije informacijske varnostne kulture so s SN oz. NB zaposlenih v zdravstveni negi glede izvedbe nepooblaščenega dostopa do zdravstvenih podatkov negativno povezane«. Niti ena dimenzija informacijske varnostne kulture nima statistično značilne povezanosti s SN. Negativno statistično značilno povezanost z NB ima le

dimenzija SO (*β = -0,313; f^2 = 0,041; t = 3,320; p = 0,001; 97,5 % CI [-0,490; -0,117]*). H2 lahko zato potrdimo le delno.

H3 se glasi: »Dimenzije informacijske varnostne kulture so negativno povezane s PBC zaposlenih v zdravstveni negi glede izvedbe nepooblaščenega dostopa do zdravstvenih podatkov«. Negativno povezanost s PBC ima samo dimenzija SETA (*β = -0,253; f^2=0,018; t = 2,235; p = 0,025; 97,5 % CI [-0,471; -0,032]*). H3 lahko zato potrdimo le delno.

H4 se glasi: »ATB zaposlenih v zdravstveni negi do izvedbe nepooblaščenega dostopa do zdravstvenih podatkov so pozitivno povezana z BI glede izvedbe omenjene kršitve«. To hipotezo potrdimo, saj je povezanost ATB pozitivna in statistično značilna (*β = 0,306; f^2 = 0,131; t = 3,865; p < 0,001; 97,5 % CI [0,168; 0,481]*).

H5 se glasi: »SN in NB zaposlenih v zdravstveni negi do izvedbe nepooblaščenega dostopa do zdravstvenih podatkov so pozitivno povezana z BI glede izvedbe omenjene kršitve«. To hipotezo potrdimo. Povezanost SN in BI je pozitivna in statistično značilna (*β = 0,161; f^2 = 0,029; t = 2,046; p = 0,041; 97,5 % CI [0,000–0,307]*) in prav tako je povezanost NB z BI pozitivna in statistično značilna (*β = 0,369; f^2 = 0,160; t = 3,615; p < 0,001; 97,5 % CI [0,163; 0,570]*).

H6 se glasi: »PBC zaposlenih v zdravstveni negi nad izvedbo nepooblaščenega dostopa do zdravstvenih podatkov je pozitivno povezana z BI glede izvedbo omenjene kršitve«. To hipotezo potrdimo. Povezanost PBC z BI je pozitivna in statistično značilna (*β = 0,124; f^2 = 0,035; t =3,272; p = 0,001; 97,5 % CI [0,049; 0,193]*).

Rezultati v Tabeli 38 kažejo, da ni statistično značilne povezave med spremenljivko starost ter ATB in BI, medtem ko sta spremenljivki ATB in BI med seboj statistično značilno povezani. Glede na dobljene rezultate H7a: »Spremenljivka starost zaposlenih v zdravstveni negi je negativno povezana z njihovimi ATB glede izvedbe nepooblaščenega dostopa do zdravstvenih podatkov.« ter H7b: »Spremenljivka starost zaposlenih v zdravstveni negi je negativno povezana z njihovo BI glede izvedbe nepooblaščenega

dostopa do zdravstvenih podatkov.« zavrnemo, saj ni statistično značilnih povezav med navedenimi spremenljivkami.

Tabela 38: Izračun Spearmanovega koeficienta korelacije rangov (r_s) za spremenljivke starost, ATB in BI (n = 527)

	r_s (p)	
	ATB	BI
Starost	-0,033 (0,454)	-0,031 (0,471)
ATB		0,682 (< 0,001)

Rezultati v Tabeli 39 kažejo, da obstaja statistično značilna povezanost med spremenljivko stopnja izobrazbe ATB in BI, vendar je ta izjemno šibka, saj sta obe vrednosti Spearman's rho koeficienta pod 0,3 (ATB -0,246 in BI -0,187). Gre za negativno povezanost, kar pomeni, da nižja kot je izobrazba, nižja so ATB in BI. Zato hipotezi H7c: »Spremenljivka izobrazba zaposlenih v zdravstven negi je negativno povezana z njihovimi ATB glede izvedbe nepooblaščenega dostopa do zdravstvenih podatkov.« ter H7d: »Spremenljivka izobrazba zaposlenih v zdravstveni negi je negativno povezana z njihovo BI glede izvedbe nepooblaščenega dostopa do zdravstvenih podatkov.« ovržemo.

Tabela 39: Izračun Spearmanovega koeficienta korelacije rangov (r_s) za spremenljivke stopnja dosežene izobrazbe, ATB in BI (n = 527)

	r_s (p)	
	ATB	BI
Stopnja dosežene izobrazbe	-0,246 (< 0,001)	-0,187 (< 0,001)
ATB		0,682 (< 0,001)

Rezultati v Tabeli 40 kažejo, da ni statistično značilne povezanosti med spremenljivko doba dela ter ATB in BI, zato H7e: »Spremenljivka delovna doba zaposlenih v zdravstveni negi je negativno povezana z njihovimi ATB glede izvedbe nepooblaščenega dostopa do zdravstvenih podatkov.« ter H7f: »Spremenljivka delovna doba zaposlenih v zdravstveni negi je negativno povezana z njihovo BI izvedbe nepooblaščenega dostopa do zdravstvenih podatkov« ovržemo.

Tabela 40: Izračun Spearmanovega koeficienta korelacije rangov (r_s) za spremenljivke doba dela v organizaciji, ATB in BI (n = 527)

	r_s (p)	
	ATB*	BI*
Doba dela	-0,012 (0,778)	-0,046 (0,295)
ATB		0,682 (< 0,001)

*p < 0,01

Rezultati preverjanja hipotez so povzeti v Tabeli 41.

Tabela 41: Povzetek preverjanja hipotez

Hipoteza		Povezanost	Rezultat
H1		Dimenzije > ATB	Delno potrjena.
H2		Dimenzije > SN in NB	Delno potrjena.
H3		Dimenzije > PBC	Delno potrjena.
H4		ATB > BI	Potrjena.
H5		SN in NB > BI	Potrjena.
H6		PBC > BI	Potrjena.
H7	a	Starost > ATB	Ovržena.
	b	Starost > BI	Ovržena.
	c	Stopnja izobrazbe > ATB	Ovržena.
	d	Stopnja izobrazbe > BI	Ovržena.
	e	Delovna doba > ATB	Ovržena.
	f	Delovna doba > BI	Ovržena.

4.3.2 Rezultati, ki zadevajo raziskovalno vprašanje

»V kolikšni meri so dimenzije informacijske varnostne kulture dober pokazatelj BI glede kršitev informacijske varnosti pri zaposlenih v zdravstveni negi?«

Posredni učinek na BI imata le dimenziji ISKS (*β = 0,133 ; t = 2,155; p = 0,031; 97,5 % CI [0,245; 0,133]*) in PO (*β = -0,154 ; t = 2,346; p = 0,019; 97,5 % CI [-0,288; 0,025]*) (tabela 36).

4.3.3 Rezultati, ki zadevajo tretji cilj

Ugotoviti, katere vzvode, ki se nanašajo na informacijsko varnostno kulturo lahko uporabijo zdravstvene in socialnovarstvene ustanove za zmanjšanje tveganja za kršitev zaupnosti zdravstvenih podatkov s strani zaposlenih v zdravstveni negi.

Povezave med dimenzijo PO, ISKS ter ATB; dimenzijo SO in NB; dimenzijo SETA in PBC; ATB, SN in PBC z BI imajo majhno velikost učinka, medtem ko ima povezava med NB in BI srednjo velikost učinka (tabela 32). Čeprav obstajajo statistično značilne povezave z dimenzijami informacijske varnostne kulture, te razlagajo relativno majhen delež variabilnosti v ATB, SN in PBC (R^2 < 0,10). R^2 vrednost za BI znaša 0,623, kar pomeni, da ATB, SN, NB in PBC pojasnijo 62,3 % variance v BI. Največji učinek na BI imajo NB ($f^2 = 0,160$). Sledijo ATB ($f^2 = 0,131$), PBC ($f^2 = 0,035$) ter SN ($f^2 = 0,029$).

5 RAZPRAVA

Pričakovali smo razmeroma močno statistično povezanost devetih dimenzij informacijske varnostne kulture z ATB, SN, NB ter PBC zaposlenih v zdravstveni negi, da preprečijo kršitve informacijske varnosti za področje nepooblaščenega dostopa. Prav tako smo pričakovali, da bodo ATB, SN, NB ter PBC skupaj z BI med seboj statistično značilno povezani konstrukti, skladno z zastavljenimi hipotezami. Predvidevali smo, da bodo dimenzije informacijske varnostne kulture statistično značilno povezane z BI preko ATB, SN, NB ter PBC zaposlenih v zdravstveni negi. V nadaljevanju poglavja *Razprava* so predstavljene ključne ugotovitve ter primerjave pridobljenih rezultatov s spoznanji drugih raziskav.

Naša raziskava, kakor tudi številne druge, je dokazala, da je pojem informacijske varnostne kulture razmeroma zapleten, saj zahteva poglobljeno razumevanje vedno večjega števila dimenzij, ki jih je potrebno uzreti z različnih zornih kotov.

5.1 RAZPRAVA O REZULTATIH, KI SE NANAŠAJO NA PRVI CILJ

Cilj 1: »*Preveriti koncept dimenzij in stanje informacijske varnostne kulture pri zaposlenih v zdravstveni negi v Republiki Sloveniji«.*

Rezultati raziskave so pokazali, da je najnižja vrednost mediane pri dimenziji MON in ISKS (Me = 5,0), medtem ko je najvišja pri dimenziji PO (Me = 6,70) (tabela 18). S tem rezultatom argumentiramo vnos novega konstrukta PO v že obstoječi model avtorjev Nasir, et al. (2019a). Nekateri avtorji predlagajo razvoj vsebin in metod, specifičnih za panoge, kot je npr. zdravstvo, ki se srečuje z dilemami med varnostjo zdravstvenih podatkov, strogimi predpisi in blaginjo pacientov (Hedström, et al., 2013; Karlsson, et al., 2017). Rezultati kažejo na razmeroma visoko stopnjo dojemanja in strinjanja o dimenziji PO za področje zdravstvene nege. Gre za dimenzijo, ki opredeljuje *usmerjenost k zagotavljanju zasebnosti* in se nanaša na zavezanost k poklicni molčečnosti, zavezi zagotavljanja zasebnosti pacientov, varovanju zasebnosti pacientov, zagovarjanju pravic pacientov do zasebnosti ter pravila »*Ne delaj drugim, kar ne želiš, da bi drugi naredili*

tebi.«, glede zasebnosti pacientov in vsebuje etično komponento. Ker je zdravstvena nega sama po sebi praksa etike in etičnega odločanja, je etično ravnanje medicinskih sester v zvezi z informacijsko varnostjo izjemnega pomena za spoštovanje idealov in etičnih norm poklica. Ta predstavlja posebnost zdravstvene nege. Zato ni presenetljivo, da ima poklicno specifična dimenzija informacijske varnostne kulture, ki je povezana s področjem etike v zdravstveni negi najvišjo mediano. Kar nekaj raziskav navaja, da so etične norme tesno povezane z na organizacijo osredotočenimi dimenzijami informacijske varnostne kulture (Martins & Eloff, 2002; Tarimo, et al., 2006; Da Veiga & Eloff, 2010; Hedström, et al., 2010; Alnatheer, 2014; Da Veiga, 2018). Z vidika zdravstvene nege in etike v zdravstveni negi dimenzije informacijske varnostne kulture temeljijo na deontoloških, utilitarističnih, na pravilih temelječih in intuicionističnih teorijah (angl. »intuitionist theories«) (Noureddine, 2001).

Po mnenju Ma, et al. (2015) imajo socialne (družbene) norme in tudi etične norme pomembno vlogo pri informacijski varnosti v delovnem okolju medicinskih sester, kjer ima etična ozaveščenost pomembno vlogo pri uveljavitvi teh norm v praksi (Lee & Seomun, 2021). Etična ozaveščenost omogoča medicinskim sestram, da prepoznajo etične posledice vseh dejanj v praksi in je pomemben sestavni del varne in kakovostne zdravstvene nege (Milliken, et al., 2019), kjer je varna uporaba zdravstvenih informacij izjemnega pomena (Saranto, et al., 2018).

Spoštovanje človekove pravice do dostojanstva je zato sestavni del zdravstvene nege (International Council of Nurses, 2021), ohranjanje zasebnosti informacij pa pomemben element pozornosti do dostojanstva pacientov (Jamalimoghadam, et al., 2019; Mohammadi, et al., 2020). Na žalost so v kliničnih okoljih pacienti ranljivi za izgubo dostojanstva glede informacijske zasebnosti (Mohammadi, et al., 2020). Zato je pomembno vzpostaviti organizacijsko kulturo, ki spodbuja dostojanstvo pacientov v klinični praksi (Baillie, 2009; Bidabadi, et al., 2019). Pozornost do pacientovega dostojanstva je neločljiv del poklica zdravstvene nege (International Council of Nurses, 2021; Kearns, 2017). Ena od definicijskih lastnosti dostojanstva je spoštovanje, ki ga sestavlja več razsežnosti: samospoštovanje, spoštovanje drugih, spoštovanje zasebnosti ljudi, zaupnost ter vera vase in vera v druge (Griffin-Heslin, 2005). Od naštetih je

spoštovanje zasebnosti in zaupnosti ljudi, zlasti pacientov, še posebej pomembno z vidika varnosti informacij.

Dimenzije informacijske varnostne kulture, specifične za poklic, ki so opredeljene v naši raziskavi, niti niso tako nepričakovane. Npr. Alnatheer (2014) je v svojem pregledu literature identificiral pet raziskav, ki vključujejo etiko in njene izpeljanke kot konstrukte informacijske varnostne kulture *(»ethical conduct«, »ethics«, »ethical«*). Ko upoštevamo posebnosti zdravstvene nege, se koncept informacijske varnostne kulture razširi na poklicno-specifične dimenzije, ki temeljijo na etičnih načelih poklica. Z drugimi besedami, etična dimenzija, ki je bila prej latentna, tako postane eksplicitna.

V skladu z dolžnostnim pristopom (angl. »*duty-based*«) k moralnemu odločanju je varovanje pacientove zasebnosti in zaupnosti pomembna zaveza medicinskih sester (Kearns, 2017), pomembna pa je tudi s pravnega vidika (U. S. Department of Labor, 2004; GDPR, 2016). Pozornost na zasebnost in zaupnost pacientov predstavlja korak dlje od samega obstoja teh pravnih aktov, saj prispeva k njihovemu izvajanju v praksi.

Z vidika zdravstvene nege je najbolj konfliktna situacija, s katero se srečujejo medicinske sestre zaposlene v enotah intenzivne nege – kršitev zasebnosti. Neuspeh pri ohranjanju zaupnih pacientovih podatkov z delitvijo s tretjimi osebami ali osebami, ki niso neposredno vključene v oskrbo pacienta se zgodi vsaj enkrat letno (Pishgooie, et al., 2019). Hansson in Fröding (2021) trdita, da se pri uporabi na posameznika osredotočene oskrbe srečamo s celo dvanajstimi vrstami etičnih konfliktov, od katerih dva zadevata tudi zasebnost ter varnost informacijske tehnologije (v nadaljevanju IT).

Razsežnost vključitev občutljivih osebnih podatkov, ki jih morajo zdravniki in zaposleni v zdravstveni negi, ki se ukvarjajo z oskrbo, osredotočeno na pacienta zapisati v zdravstveno dokumentacijo, je ogromna (Munthe, et al., 2012). Je pa nujna zaradi vodenja pacientovega stanja in predajanja ustreznih informacij kolegom. A kot ugotavljajo Munthe, et al. (2012, p. 235): *»Več informacij, kot je vnesenih v kakršenkoli sistem (spomin, papirnata dokumentacija, digitalna baza podatkov), večje je tveganje, da bodo nekatere občutljive informacije pricurljale na dan«*. Z vidika varnosti IT je prednost

vključiti čim manj občutljivih informacij v elektronske zbirke podatkov. Zato obstaja potencialen etični konflikt med varnostjo IKT in zdravstveno dokumentacijo pacienta (Hansson & Fröding, 2021). V procesu odločanja je zato potrebno posebno pozornost nameniti tudi prepoznavi omenjenih konfliktov; prepoznavanje problemov za procese odločanja olajša razvijanje sistematičnih in integriranih poti (klinične poti) v organizaciji (Svantesson, et al., 2021).

Medtem ko je na voljo obsežna literatura o pozitivnih učinkih *institucionalizacije etike* v organizacijski kulturi, raziskava informacijske varnostne kulture avtorjev Ruighaver, et al. (2010) ni identificirala nobenih dokazov v prid spodbujanja organizacij pri etičnih odločanjih, ki zadevajo informacijsko varnost. Kot navajajo omenjeni avtorji, veliko organizacij še vedno uporablja etični kodeks, ki temelji na *deontološki etiki* – od zaposlenih se namreč pričakuje, da so njihova dejanja na delovnem mestu prava. Na deontološko varnostno etiko se v praksi zanašajo varnostne politike, ki temeljijo na mehanizmu »odvračanja«. Spremembe v etičnih prepričanjih iz generacije »babyboomer« v »generacijo X« in »generacijo Y« pomenijo, da se mlajše generacije počutijo manj dolžne spoštovati pravila. Moralnosti svojih dejanj ne ocenjujejo na podlagi pravil, temveč na podlagi zaznanih posledic. Vsi zaposleni niso pripravljeni vedno postaviti interesov organizacije nad lastne interese (Ruighaver, et al., 2010).

Organizacije si morajo prizadevati za pozitivno kulturo med svojimi zaposlenimi, da bi lahko vzpostavili varnost podatkov (Farzandipour, et al., 2010). Ruighaver, et al. (2010) so mnenja, da bi morale organizacije v primeru ogrožene informacijske varnosti spodbujati etiko. Spoštovanje etike lahko postane kultura med zaposlenimi, kar vodi v varstvo podatkov (Farzandipour, et al., 2010). Številne grožnje varnosti in zasebnosti bi lahko preprečili, če bi uporabniki računalnikov upoštevali tudi etične standarde drugih sodelujočih strani (de Lusignan, et al., 2007; Zakariya & Kahn, 2015). D'Arcy, et al. (2009) predlagajo etično vedenje zaposlenih kot pomemben predpogoj za informacijsko varnost.

Po navedbah de Lusignan, et al. (2007) bi morale organizacije svojim zaposlenim zagotoviti usposabljanje za spodbujanje etičnih praks. Omenjeni navajajo, da bi

marsikatero etično kršitev lahko preprečili z usposabljanjem zaposlenih. Usposabljanje zaposlenih oblikuje in krepi etično kulturo v organizaciji, ima učinek na zaposlene, da delujejo etično in se počutijo odgovorne za zaščito informacij.

Pri tem se pojavi zanimivo vprašanje. Hipotetično, če bi bile v organizaciji dimenzije informacijske varnostne kulture popolnoma izključene (npr. PCM, MON, TMC), ali bi identificirana dimenzija PO, specifična za poklic zdravstvene nege, zadostovala za preprečitev morebitnih kršitev varnosti informacij?

Najnižjo mediano ima dimenzija informacijske varnostne kulture ISKS (tabela 18). Rezultati kažejo, da izmenjava znanja o informacijski varnosti med zaposlenimi v zdravstveni negi ni tako pomembna oz. je okrnjena ali pa ne poteka. Predhodne raziskave z drugih področij so pokazale ISKS (Safa, et al., 2016; Nasir, et al., 2019a) in prav tako tudi SETA (Chen, et al., 2015; Nasir, et al., 2019a) kot relevantni dimenziji informacijske varnostne kulture. Domnevamo lahko, da prenos znanja in veščin informacijske varnosti zaposleni v zdravstveni negi ne dojemajo kot prioriteto, ki bi jo bilo treba vključiti v stalno usposabljanje in izobraževanje, ali kot ključni element v procesu izmenjave znanja. Rezultati so presenetljivi, saj medicinske sestre predstavljajo populacijo, ki dojema nenehno usposabljanje, izobraževanje (Price & Reichert, 2017) ter izmenjavo znanja (Yoo, et al., 2019) kot ključnega pomena za njihov poklic in razvoj kariere.

Obenem smo identificirali še statistično značilne razlike v povprečnih rangih med moškimi in ženskami za dimenzijo ISKS (tabela 22). Vrednost mediane pri dimenziji ISKS pri ženskah znaša 5,25 (*IQR = 2*), medtem ko pri moških znaša 4,5 (*IQR = 2,25*) (tabela 21).

Poleg dimenzije ISKS ima najnižjo mediano dimenzija MON (tabela 21), kar kaže, da se zaposleni ne zavedajo ali celo ne poznajo posledic kršenja varovanja osebnih podatkov pacienta. Obenem so bile za dimenzijo MON identificirane statistično značilne razlike v povprečnih vrednostih med moškimi in ženskami. Povprečna vrednost je bila višja pri ženskah (tabela 22).

Farzandipour, et al. (2010) navajajo, da varnostno spremljanje zaposlenih deluje na varnost informacij v organizacijah. Izvajajo ga organizacije z namenom ugotavljanja, ali zaposleni upoštevajo organizacijska pravila in predpise. Po D'Arcy, et al. (2009) varnostno spremljanje in nadzor zaposlenih zmanjšata verjetnost kršitve varnosti tako, da poveča zaznavanje zaposlenih o morebitnih posledicah – kaznih za takšno vedenje. Da bi odkrili in popravili nesprejemljivo vedenje zaposlenih, vodi varnostno spremljanje do odvračanja problematičnega vedenja, vključno s kršitvami varnosti. Spremljani zaposleni težko prevzamejo tveganje v zvezi z razkritjem občutljivih informacij in raje prevzemajo skrb za svojo odgovornost v zvezi z informacijsko varnostjo (Zafar, 2013). Farzandipour, et al. (2010), Zafar (2013) in Peikari, et al. (2018) navajajo, da je varnostno spremljanje eden od ključnih faktorjev, ki oblikujejo zaupanje pacientov. Dojemanje pacientov o varnostnemu spremljanju zaposlenih je povezano z zaupanjem v bolnišnico in pomisleke glede kršitev varnosti.

Z našo nalogo smo potrdili, da obstaja povezanost, pa četudi šibka, pozitivna, med starostjo in delovno dobo zaposlenih v zdravstveni negi ter zaznavanjem dimenzije RM (tabela 19 in tabela 20).

Z RM identificiramo in analiziramo pomembna tveganja za doseganje ciljev, ki tvorijo osnovo za določanje, kako je treba tveganja obvladovati. Je eden najpomembnejših vidikov kliničnega vodenja in pristopov, predstavljenih v literaturi, katerega namen je izvedba celovitih analiz za odkrivanje temeljnih vzrokov neželenih dogodkov (Cagliano, et al., 2011). Sale (2005) navaja, da je cilj kliničnega upravljanja zagotoviti, da pacienti prejmejo najboljšo kakovost oskrbe in vključuje sisteme in procese za spremljanje in izboljševanje storitev, obvladovanje tveganja, klinično presojo, programe klinične učinkovitosti, izobraževanje in kontinuirano usposabljanje za osebni razvoj ter uporabo informacij za podporo izvajanja zdravstvenega varstva.

Med različnimi vidiki kliničnega upravljanja je obvladovanje tveganj ključnega pomena, saj obravnava klinično tveganje, ki vpliva na paciente. Ismail, et al. (2010) trdijo, da učinkovito obvladovanje tveganja izboljša uspešnost organizacije in hkrati pomaga pri doseganju ciljev organizacije. Obvladovanje tveganj vključuje procese, povezane z

načrtovanjem obvladovanja tveganj, identifikacijo, analizo, odzivom, spremljanjem in nadzorom (Cagliano, et al., 2011). Donaldson, et al. (2000) npr. opredeljujejo klinično tveganje kot verjetnost, da pacienta prizadene neželeni dogodek, ki ga prostovoljno ali neprostovoljno povzroči zdravljenje. Vendar klinično tveganje ni le posledica medicinskih aktivnosti, ki neposredno vplivajo na paciente, ampak je odvisno od večjega nabora dejavnosti in strokovnjakov. Določajo ga številni dejavniki v zvezi s sistemom, okoljem in medsebojnim delovanjem posameznikov, ki delujejo v procesih, povezanih z zagotavljanjem oskrbe.

Rezultati raziskave so pokazali, da obstajajo izredno šibke pozitivne povezave med delovno dobo zaposlenih v zdravstveni negi ter dimenzijami PCM ($r_s = 0,167; n = 527; p < 0,001$) in SETA ($r_s = 0142; n = 527; p < 0,001$) (tabela 20). Iz rezultatov lahko sklepamo, da delovne izkušnje zaposlenih lahko zmanjšajo tveganje za kršitve varnosti podatkov. Zaposleni, ki delujejo vrsto let v določeni organizaciji, bolje poznavajo varnostno politiko.

Roer in Petric (2018) navajata, da naj bi družbeni kontekst (npr. določeno delovno mesto) v kombinaciji s formalnim usposabljanjem, imel učinek na varnostno kulturo, medtem ko Metalidou, et al. (2014) trdijo, da samo formalno usposabljanje ne spreminja vedenja zaposlenih.

Neskladnost s politiko varnosti informacij in zloraba IS sta tesno povezana. Neskladnost definira namerno ali po nesreči neupoštevanje smernic in pravil s strani zaposlenih. Slednje pogosto vodi do zlorabe IS, kar lahko povzroči resne kršitve varnosti. Zloraba IS s strani zaposlenih je pogosto opredeljena kot »nepooblaščena, namerna interna zloraba sredstev organizacijskega IS« (Hedström, et al., 2013).

Trajanje delovne dobe je povezano s stališči do organizacijske varnosti. Večina zaposlenih izkazuje pretežno pozitivna stališča do organizacijskega nadzora. Najmanj pozitivna stališča pa imajo najmanj izkušeni zaposleni (60,5 %). Pri dimenziji skladnosti sta Roer in Petric (2018) identificirala več razlik, povezanih z leti zaposlitve v organizaciji. Večina zaposlenih z več kot pet let delovne dobe dobro pozna varnostne

procese. Zaposleni z manj delovne dobe so najmanj seznanjeni s komunikacijskimi kanali za hiter odziv na napade (55,3 %), veliko bolje pa so seznanjeni zaposleni z več kot 30 leti delovnih izkušenj (72,8 %).

Moody, et al. (2018) navajajo, da zaposleni ne upoštevajo vedno priporočil, predpisanih v varnostnih politikah, in da se vedejo precej nevarno, čeprav so seznanjeni z omenjenimi politikami, medtem ko Uchendu, et al. (2021) argumentirajo potrebo po jasnejših in lažje dostopnih politikah in postopkih. Greig, et al. (2015) navajajo, da nekateri zaposleni v maloprodajni organizaciji nikoli niso videli politik podjetja. Podobno velja pri raziskavi avtorja Olivos (2012), kjer varnostne politike niso bile posredovane zaposlenim, ker so bile le-te porazdeljene na več dokumentov. Vodstvo in IT oddelki morajo zagotoviti, da je poznavanje pravilnika zaposlenim na zahtevani ravni, posameznikom pa so na voljo posodobljeni in ustrezni pravilniki, ki zadevajo informacijsko varnost.

Rezultati doktorske disertacije so pokazali, da ni statistično značilnih razlik v povprečnih vrednostih rangov dimenzij informacijske varnostne kulture glede na stopnjo izobrazbe (tabela 24) ali vrste zdravstvenih organizacij (tabela 28). Rezultati so zanimivi, saj bi lahko zaradi različnih organizacijskih ustrojev med nivoji zdravstvenega varstva in socialnovarstvenimi zavodi ali velikostmi organizacij pričakovali različno organizacijsko kulturo in tudi informacijsko varnostno kulturo.

Vsaka organizacija ima svoje značilnosti, informacije, IT infrastrukturo ter določeno informacijsko varnostno prakso, ki je vključena v delovno okolje in bo postala del organizacijske kulture v organizaciji. Za značilnosti, kot sta razpoložljivost in celovitost informacij, si morajo organizacije prizadevati (Martins & Eloff, 2002).

Majhne in srednje velike organizacije pogosto predstavljajo pomemben delež organizacij. Tako npr. v Združenem kraljestvu predstavljajo 99,9 % vseh organizacij (Department for Business, Energy and Industrial Strategy – BEIS, 2020). Ling (2017) navaja, da je manjšim in srednje velikim organizacijam za bolj integriran in konsolidiran pogled koristnejše imeti dostop do informacij iz različnih oddelkov. Prav zaradi tega je informacijska varnost toliko bolj pomembna v manjših organizacijah. Raziskava Lloyd

(2020) je pokazala, da ima le 15 % malih organizacij formalen proces upravljanja kibernetskih incidentov, kar nakazuje na premajhen poudarek varnosti. Raziskava avtorjev Stavros, et al. (2016) je pokazala, da so bili zaposleni v manjših in srednje velikih organizacijah bolj odprti za spremembe, v kolikor so bili vključeni številni dejavniki, kot so komunikacija, vključenost in usposabljanje. To dodatno poudarja pomen organizacijske kulture in kako je kljub pristopu k izgradnji varnostne kulture izjemno pomembno vodenje zaposlenih (Uchendu, et al., 2021).

Raziskava avtorjev Saberi, et al. (2019), ki se nanaša predvsem na etične konflikte pri delu medicinskih sester, je namreč pokazala, da so bile medicinske sestre z magisterijem in zgodovino udeležbe na etičnih izobraževanjih bistveno bolj izpostavljene etičnim konfliktom kot ostale. Te izsledke lahko prenesemo tudi na področje etičnih konfliktov, ki nastajajo pri uporabi IKT in rokovanju z zdravstvenimi podatki.

5.2 RAZPRAVA O REZULTATIH, KI SE NANAŠAJO NA PLS-SEM

V prvem koraku *Predhodna vprašanja in vidiki, povezani z analizo SEM*, smo izračunali ustrezno velikost vzorca, t.j.500 enot in tako dosegli kriterije, ki jih določa analiza SEM. Preverili smo porazdelitev podatkov in podali argumente za izbiro SEM. V drugem koraku *Ocena merilnega modela z reflektivnimi konstrukti* smo ocenili CA, CR, AVE (tabela 9), Fornell-Lackerjev kriterij (tabela 10) ter HTMT (tabela 11). Vsi rezultati so izpolnili zahtevane kriterije. V tretjem koraku *Ocena strukturnega modela* smo analizirali VIF (tabela 31), pojasnjevalno (tabela 32) in napovedno moč (tabela 33), relevantnost in statistično značilnost poti v modelu (tabela 34). Primarni kazalniki kakovosti strukturnega modela so R^2 vrednosti endogenih spremenljivk, ki merijo kolikšen del variance v endogenem konstruktu je pojasnjeno z eksogenim konstruktom v modelu (Hulland, 1999). Rezultati so pokazali, da ima model dobro razlagalno moč. R^2 vrednost za odvisno spremenljivko BI znaša 0,623, kar pomeni, da spremenljivke v modelu pojasnijo kar 62,3 % variance v odvisni spremenljivki. Kriterij analize SEM je zagotovljen, saj je rezultat bistveno višji kot v primerljivih raziskavah, v katerih so uporabili podobne odvisne spremenljivke (42 % Herath & Rao, 2009a, 47 % 2009b; 35 % Bulgurcu, et al., 2010; 47 % Siponen & Vance, 2010; 45 % Nasir, et al., 2019a).

5.3 RAZPRAVA O REZULTATIH, KI SE NANAŠAJO NA HIPOTEZE

Cilj 2: »*Preveriti povezanost dimenzij informacijske varnostne kulture s konstrukti Teorije načrtovanega vedenja.*«

Preverjanje povezanosti dimenzij informacijske varnostne kulture s konstrukti TPB zadeva drugi cilj doktorske naloge. S potrditvijo ali zavrnitvijo hipotez smo pridobili novo sliko empiričnih dokazov in spoznali pomembne povezave. Zato si vsaka od hipotez zasluži individualno diskusijo. Potrjene so bile v celoti tri hipoteze, tri smo delno potrdili in tri ovrgli.

Hu, et al. (2012) v svojem delu navajajo, da obstoječa literatura organizacijskega konteksta in vedenja zaposlenih obravnava predvsem direktne povezave. Pri tem opominjajo, da je verjetnost, da kognitivna prepričanja posredujejo učinek kulture na vedenje pomembna in da si zasluži v prihodnjih raziskavah več pozornosti.

5.2.1 Vloga informacijske varnostne kulture (H1–H3)

Rezultati naše naloge kažejo, da so dimenzije informacijske varnostne kulture pomemben dejavnik, ki deluje na konstrukte prepričanj zaposlenih v zdravstveni negi v kontekstu informacijske varnosti, čeprav z različno stopnjo in signifikanco.

Rezultati v Tabeli 34 kažejo statistično značilno povezanost PO z ATB (*β = -0,269; f^2 = 0,039; t = 2,118; p = 0,034; 97,5 % CI [-0,525; -0,029]*); ISKS z ATB (*β = 0,167; f^2 = 0,010; t = 2,385; p = 0,017; 97,5 % CI [0,030; 0,304]*); SO s NB (*β = -0,313; f^2 = 0,041; t = 3,320; p = 0,001; 97,5 % CI [-0,490; -0,117]*); SETA s PBC (*β = -0,253; f^2 = 0,018; t = 2,235; p = 0,025; 97,5 % CI [-0,471; -0,032]*). H1–H3 smo zato le delno potrdili.

Presenetljivo je, da nismo zaznali nobene statistično značilne povezanosti katerekoli od dimenzij informacijske varnostne kulture s SN, za kar nimamo prav ustrezne razlage, medtem ko je to pri NB drugače. V zakup gre vzeti povezavo s tem, kako so bile SN opredeljene in merjene. V pričujoči raziskavi, kot v mnogih drugih, ki temeljijo na TPB,

SN merijo predvsem to, kako močno posameznik zaznava vpliv pomembnih drugih v njegovem ožjem krogu. Čeprav lahko kultura močno vpliva na stališča in prepričanja posameznih članov v organizaciji, ni nujno, da vpliva na to, kako zaposleni dojema vpliv svojih vrstnikov, nadrejenih in podrejenih (Hu, et al., 2012). Posameznike v vrhnjem managementu lahko npr. obravnavamo kot člane vplivnega družbenega ali strokovnega kroga. Le-ti pa lahko imajo močan in neposreden vpliv na SN zaposlenih.

Rezultati so pokazali na statistično značilno povezanost dimenzij PO z ATB (tabela 34). Dimenzijo PO predstavlja etičnost, poklicna molčečnost, zagotavljanje zasebnosti pacientov in njihova pravica do te zasebnosti. Najvišja mediana je bila identificirana prav za omenjeno dimenzijo (tabela 18).

Vzpostavljanje, izboljševanje in celo poslabšanje informacijske varnostne kulture pomeni organizacijsko spremembo. Razumevanje stališč glede podpore omenjene spremembe olajša poznavanje tradicij »od zgoraj navzdol« in »od spodaj navzgor« (Heyden, et al., 2017). Negativna povezava med PO in ATB nakazuje, da se stališča morda oblikujejo zaradi notranjih sil od »spodaj navzgor« usmerjenih dejavnikov organizacijske kulture (Heyden, et al., 2017). Osebna prepričanja, vrednote in etika posameznikov oblikujejo njihova ATB, kot je nepooblaščen dostop do zdravstvenih podatkov. Negativna povezanost SO z NB kaže, da družbeni vpliv morda izhaja iz tradicij organizacijskih praks varovanja podatkov od »zgoraj navzdol«, ki predpisuje, kako naj zaposleni ravna z varnostjo (Heyden, et al., 2017). Rezultat naše naoge nakazuje, da družbeni vpliv temelji na posameznikovi percepciji pomembnih organizacijskih vrednot, norm ter sprejetih načinov dela, kot jih določajo politike in pravni akti organizacije.

Dimenzija SO je pokazala statistično značilno povezanost z NB (β = *-0,313; t = 3,320; p = 0,001*) (tabela 34). Gre za dimenzijo, ki opredeljuje zaznavanje posameznika o prisotnosti dobre prakse varovanja podatkov v organizaciji in se nanaša na zaznavanje prisotnosti kulture za spodbujanje dobrih praks v organizaciji; na varnost podatkov kot pomembno vrednoto organizacije; zagotavljanje varnosti podatkov o pacientih kot sprejet način dela v organizaciji; zagotavljanje varnosti podatkov kot ključno normo v organizaciji ter kolektivno odgovornost za varnost podatkov o pacientih.

Vidna vedenja zaposlenih v organizaciji so tista, ki zagotavljajo opazne dele organizacijske kulture in spodbujajo novo-zaposlene in obstoječe zaposlene glede dejanj, ki so v organizaciji sprejemljiva (Cannoy & Salam, 2010). Vrednote, ki so ključne komponente Scheinovega (2019) modela organizacijske kulture, je težko spreminjati in so običajno distalni napovedovalec vedenja v organizaciji (Bruursema, 2007; Gatersleben, et al., 2014; Schein & Schein, 2019). Vendar Kessler, et al. (2020) navajajo, da je organizacijska klima učinkovitejša metoda neposrednega spreminjanja vedenja zaposlenih.

Kot navajajo Chen, et al. (2018), so bile v empiričnih raziskavah v različnih organizacijskih konceptih identificirane štiri vrste *organizacijskih varnostnih klim* – organizacijska varnostna klima usmerjena v skrb (angl. »*caring-oriented*«), usmerjena v zakon in pravila (angl. »*law-and-rule-oriented*«), v instrumentalizem (angl. »*instrumentalism-oriented*«) ter v neodvisnost (angl. »*independence-oriented*«).

Z utilitarnega vidika skrbno usmerjena organizacijska varnostna klima zagovarja načelo vzajemnosti. Zaposleni v takšni klimi dajejo prednost skrbi za koristi drugih pred rezultati svojega etičnega vedenja. V tem kontekstu sta skrb in upoštevanje drugih podprta s politikami, praksami in strategijami organizacije ter njenih vodilnih akterjev. Organizacijska varnostna klima, usmerjena v zakone in pravila, poudarja zunanje omejitve, kot so nacionalni zakoni in norme, standardi, pravila in predpisi, ki jih je določila organizacija. Zaposleni se v takšnem okolju načeloma nagibajo k etičnemu delovanju. Za organizacijsko klimo, usmerjeno v instrumentalizem, velja, da je lastni interes nad vsemi drugimi koristmi. V taki klimi je izhodišče posameznikovega odločanja namera uresničevanja osebnih interesov; učinek na druge ali na organizacijo pa ni pomemben. Za organizacijsko etično klimo, usmerjeno v neodvisnost, je znano posameznikovo prepričanje o tem, da se pri sprejemanju odločitev ravnajo po globoko utrjenih osebnih moralnih prepričanjih. V takšni klimi organizacija popolnoma zaupa presojam zaposlenih o etičnosti vprašanj. Etične odločitve posameznikov so nemotene s pravili ali družbenimi pritiski.

Medtem ko ugotovitve kažejo, da lahko obstajajo pomembni nepredvideni dogodki, *moderatorji* odnosov med prepričanji o (ne)skladnosti, le-ti niso bili kritično ocenjeni v literaturi. Pri tem Gwebu, et al. (2020) navajajo pomanjkanje raziskav, ki bi preučevale interakcijo med prepričanji in npr. *osebnimi normami.* Te vrste povezav z našo nalogo nismo preučevali. Moderatorji pogojev vključujejo tudi nevtralizacijo in *etično klimo*, v kateri se sprejemajo odločitve o (ne)skladnosti z ISP (Gwebu, et al., 2020).

Asgari, et al. (2019) navajajo, da je etična klima del organizacijske kulture, ki ne deluje le na etično dimenzijo zaposlenih, temveč tudi na njihovo delovno učinkovitost. Vsaka organizacija ima določene etične vrednote, ki so lahko rezultat njene etične klime. Etična klima je posameznikovo dojemanje obravnav etičnih vprašanj, ki se pojavljajo v delovnem okolju (Hojati & Azma, 2014; Hwang & Park, 2014). Zmanjšanje moralnega distresa oz. moralne stiske pri zdravstvenih delavcih je mogoče doseči s prilagoditvijo etičnih vrednot organizacije (Pauly, et al., 2009). Zaznavanje etične klime okolja je odvisno od interakcij med vrstniki, pacienti, managerji, bolnišnicami in zdravstvenim osebjem, ki se soočajo z etičnimi problemi (Asgari, et al., 2019).

Rezultati naše raziskave so pokazali na statistično značilno povezanost dimenzije SETA s PBC (tabela 34). Na področju socialne psihologije so bili programi ozaveščanja opredeljeni kot dejavniki, ki povečujejo norme in spreminjajo stališča do deviantnega vedenja (MacKinnon, et al., 1991). Zavedanje o obstoju takšnih programov in njihove vrednosti lahko pripomore k oblikovanju močne miselnosti o informacijski varnosti (Chen, et al., 2015). Ozaveščenost o SETA programih ima učinek na zaznavanje sankcij zaradi kršitev varnostnih politik (D'Arcy, et al., 2009) in spreminja stališča (Bulgurcu, et al., 2010). Raziskave se na tem področju osredotočajo na preučevanje razmerja med celovitimi izobraževalnimi programi in namero zaposlenih do upoštevanja varnostne politike (D'Arcy, et al., 2009) ter učinka komponent programov na učinkovitost strategij izvrševanja varnostne politike (Chen, et al., 2012). Rezultati raziskave avtorjev Chen, et al. (2012) so pokazali, da imajo SETA programi statistično značilen učinek na varnostno kulturo, na zavedanje zaposlenih o varnostni politiki ter da ima zavedanje o nadzoru oz. spremljanju varnosti učinek na varnostno kulturo.

Ocenjevanje znanja je lahko v nekaterih primerih koristno, vendar Fertig, et al. (2020) navajajo, da ni mogoče predvidevati, da ima znanje učinek na vedenje. Zaposleni so lahko seznanjeni s pravilniki, vendar seznanjenost ni povezana z njihovim aktualnim vedenjem. Bada, et al., (2019) so ugotovili, da se posamezniki pogosto ne ravnajo v skladu z varnostnimi politikami. Raziskave, ki so orientirane na preučevanje skladnosti, se fokusirajo na več vrst kompleksnih skladnosti z varnostno politiko (Cram, et al., 2019), za temelje pa imajo več vrst teorij in vedenjskih modelov (Moody, et al., 2018). Gre za izzive v zvezi z razumevanjem in ocenjevanjem vedenja zaposlenih – predvsem v smislu spremembe vedenja. Fertig, et al. (2020) so ugotovili, da za merjenje ozaveščenosti o varnosti informacij samo vprašalniki za ocenjevanje znanja niso dovolj. Kombinacija meritev vedenja in znanja je tista, ki daje zadostne ocene. Njihov sklep pa lahko uporabimo tudi za prenos na informacijsko varnostno kulturo.

Raziskavi avtorjev Alshaiki (2020) in Nasir, et al. (2020) so kot merilo za ocenjevanje vedenja zaposlenih in s tem razvoja informacijske varnostne kulture v preučevanje skladnosti vključile tudi komponente vedenja in poročanje o rezultatih odgovornim za skladnost.

Raziskave avtorjev Olivos (2012); Greig, et al. (2015) ter Ruhwanya in Ophoff (2019), ki vključujejo usposabljanje, metode opazovanja in okrogle mize, prikazujejo zanesljivejše podatke o tem, ali zaposleni v vsakodnevnih situacijah resnično kažejo ozaveščeno varnostno vedenje. Rantos, et al. (2012) navajajo, da je ključnega pomena dati prednost sejam, ki osvežujejo znanje zaposlenih, saj se tam naučijo potrebnega varnostnega vedenja. Nujno je s strani organizacij upoštevati, da je potrebno tako znanje kot vedenje testirati in opazovati. Pătrașcu (2019) ponazarja izobraževanje o kibernetski varnostni kulturi kot netrivialen proces. Raziskave so pokazale, da redna usposabljanja pogosto nimajo želenih rezultatov. Podatki kažejo, da se kar 50 % informacij iz izobraževanj za izboljšanje razumevanja varnosti izgubi v eni uri, 70 % v 24 urah in 90 % v enem tednu (Ghafir, et al., 2018).

Ozaveščenost o varnostnih politikah deluje na dojemanje, stališča in vedenje zaposlenih do informacijske varnosti (Straub & Welke, 1998; D'Arcy, et al., 2009; Herath & Rao,

2009a; Chen, et al., 2012). Rezultati naše raziskave niso pokazali statistično značilne povezanosti PCM s konstrukti TPB, kar nakazuje, da navodila in pravilniki na kognitivne konstrukte prepričanj nimajo učinka. Čeprav organizacijska kultura zagotavlja normativni okvir interpretacije, razumevanje in splošni pristop k reševanju problemov zaposlenih v organizacijskih okoljih, le-to ni dovolj, da bi lahko dosegla spremembe pri vedenju zaposlenih glede skladnega delovanja z varnostnimi politikami (Hu, et al., 2012). Omenjeni avtorji navajajo, da je učinek organizacijske kulture na vedenje posameznika v celoti posredovan preko notranjih kognitivnih procesov, ki zadevajo specifične naloge in kontekste, kar je skladno tudi s teoretično razlago avtorja Harris (1994), po kateri posameznik oblikuje svoj odziv na organizacijske dražljaje, na podlagi notranje mentalne sheme oz. kognitivnih struktur, v katerih se ohranja in organizira njegovo znanje. Harris (1994) trdi, da organizacijska kultura deluje na izražanje in aktivacijo specifičnih shem, iz katerih se oblikujejo posameznikovi odzivi. Hu, et al. (2012) v svojem delu navajajo, da naj bi bila ta posredniška funkcija v večini raziskav v organizacijskih kontekstih spregledana.

V kontekstu skladnosti z informacijsko varnostno politiko izstopajo vrednote »*usmerjenost na cilj*« in »*usmerjenost na pravila*«, ki oblikujejo vedenje, povezano z varnostjo. To pa zato, ker se vedenje nanaša na skladnost z obstoječimi politikami, uveljavljanje pravil in praks ter na doseganje cilja, ki je višja raven informacijske varnosti. Za večino zaposlenih takšno vedenje ne predstavlja temeljne aktivnosti, ki bi vodila do delovnih rezultatov. Takšno vedenje v večini primerov niti ni merjeno kot kazalnik uspešnosti in je le v redkih primerih nagrajeno kot individualni ali timski dosežek (Hu, et al., 2012). Skladnost z informacijsko varnostno politiko je vedenje »*upoštevanje pravil*«, ki ni značilno za spodbujanje ustvarjalnosti, miselnih procesov ali kritičnega razmišljanja (Hu, et al., 2012).

V literaturi je najpogosteje omenjen in v zadnjem desetletju najbolj obravnavan dejavnik podpora vrhnjega managementa. Uchendu, et al. (2021) menijo, da za to obstaja več razlogov. Eden od njih je, da se brez podpore vodstva pobude za informacijsko varnost zaposlenim morda ne zdijo pomembne v primerjavi s svojim vsakdanjim delom. S podporo vodstva je mogoče informacijski varnostni kulturi nameniti potrebno pozornost,

kar pomeni, da bodo zagotovljena sredstva usmerjena tja, kjer je to potrebno. Vodstvo zato ne sme usmerjati pozornosti zaposlenih le k prizadevanju za ustrezno informacijsko varnostno kulturo, ampak mora zagotoviti tudi ustrezno upravljanje virov (Uchendu, et al., 2021).

Izsledki raziskav kažejo na pomanjkanje zavezanosti in podpore managementa za izvajanje informacijske varnosti ter odsotnost usposabljanj za zaposlene. Razvoj politike, procesov, postopkov, zavesti, izobraževanj ter usposabljanj na tem področju je pri tem ključnega pomena. Da bi se med zaposlenimi oblikovala informacijska varnostna kultura, je potrebna visoka zaveza vodstva.

Deli avtorjev Chang & Lin (2007) ter Puhakainen & Siponen (2010) sta med redkimi raziskavami, ki sta preučevali vlogo vrhnjega managementa in organizacijske kulture z empiričnimi podatki v informacijskem varnostnem kontekstu. Puhakainen in Siponen (2010) sta podala neposredne dokaze o tem, kako ukrepi vrhnjega managementa pri podpori vzpostavitve informacijske varnostne politike, med opazovanjem zaposlenih, spremenijo njihova stališča in posledično privedejo do boljše skladnosti z informacijskimi varnostnimi politikami.

Ugotovitev avtorjev Puhakainen in Siponen (2010), da udeležba vrhnjega managementa neposredno deluje na vedenje zaposlenih, da so ti v skladu s predpisi je v nasprotju z argumentom avtorja Wylder (2003). Ta navaja, da zavezanost vrhnjega managementa do varnostnih politik nima učinka na odnos in zavezanost zaposlenih do varnostnih politik, saj je vrhnji management odmaknjen od vsakodnevnih dejavnosti. Do podobnih ugotovitev so prišli tudi Liu, et al. (2011). V večjih organizacijah na odnos zaposlenih do učenja in uporabe sistemov za načrtovanje virov organizacije bolj delujejo kolegi in neposredno nadrejeni kot pa bolj odmaknjeni zaposleni v vrhnjemu managementu (Liu, et al., 2011).

Hu, et al. (2012) navajajo, da ima sodelovanje vrhnjega managementa v pobudah za informacijsko varnost neposreden in posreden učinek na ATB, SN in PBC zaposlenih s skladnostjo informacijske varnostne politike. Učinek sodelovanja vrhnjega managementa

na BI zaposlenih je v celoti posredovan preko kognitivnih prepričanj zaposlenih, ki zadevajo skladnost s politikami informacijske varnosti (Hu, et al., 2012).

Medtem ko so Hu, et al. (2012) ter Puhakainen in Siponen (2010) dokazali, da je vrhnji management eden od ključnih prediktorijev z največjim učinkom na BI, smo v pričujoči raziskavi dobili povsem drugačne rezultate. Z doktorsko disertacijo smo poskušali dokazati, da je TMC za informacijsko varnost ključnega pomena in da je negativno povezana z ATB, SN in NB ter s PBC zaposlenih v zdravstveni negi do izvedbe nepooblaščenega dostopa do zdravstvenih podatkov. Rezultati so pokazali, da dimenzija TMC ni statistično značilno povezana z nobenim od konstruktov TPB. Statistično značilno nepovezanost lahko pojasnimo z relativno hierarhično distanco med vrhnjim managementom in zaposlenimi. Na podlagi Angst in Agarwal (2009) običajne metode delovanja na ATB zaposlenih vključujejo neposredne psihološke mehanizme (npr. posredovanje ustreznega sporočila prejemniku, prepričljivost, osebno prepričevanje z oblikovanjem argumentov in vpletenostjo ter učinkovito prenašanje prepričevanja in obenem tudi strasti). Zato je verjetno, da imata na ATB učinek osebna in neposredna komunikacija.

Hu, et al. (2012) ugotavljajo, da v nekaterih organizacijah, predvsem tistih, pri katerih IT ni njihova osnovna dejavnost, vrhnji management pogosto prenese odločitve in odgovornosti za informacijsko varnost na vodje IT nižje ravni. Ugotovitve raziskave zahtevajo aktivno in vidno sodelovanje vrhnjega managementa. Vrhnji management se mora dejavno in vidno vključiti v vzpostavitev, izvajanje in uveljavljanje politik in pravil informacijske varnosti.

Ozaveščenost o informacijski varnosti, znanje na tem področju in vedenje so trije najpomembnejši dejavniki, ki ustvarjajo informacijsko varnostno kulturo. Za omenjene dejavnike je potrebna visoka zaveza vrhnjega managementa, da se informacijska varnostna kultura oblikuje med zdravstvenimi delavci (Hassan, et al., 2017). Glede na organizacijsko strukturo in odgovorne za upravljanje informacij je naloga spreminjanja informacijske varnostne kulture odvisna od višjega ali izvršnega vodstva. Le-ta pa je del

upravljalnega odbora, ki skrbi za več nalog, od skladnosti, tveganj, etike do zasebnosti in IT (Da Veiga & Martins, 2017).

Podporo vrhnjega managementa smo merili s strani dojemanja zaposlenih. Vendar kot že prej omenjeno, lahko tako strukturne kot tudi fizične razdalje med vrhnjim managementom in zaposlenimi izkrivijo meritve. Možna je argumentacija, da podpora vrhnjega managementa zaposlenim na nižji ravni ni vidna. Ne glede na rezultate pa ne smemo sklepati, da podpora vrhnjega managementa nima učinka neposredno na ATB zaposlenih kar se tiče izvedbe nepooblaščenega dostopa do podatkov v vseh organizacijah. Za preučevanje tega pomembnega razmerja so potrebne raziskave z različnimi organizacijskimi velikostmi, strukturami, kulturo in stili vodenja.

5.2.2 Vloga individualnih kognitivnih prepričanj (H4–H6)

Obstoječa literatura (Taylor & Todd, 1995; Huang, et al., 2010; Seyal & Turner, 2013; Aigbefo, et al., 2022; Alanazi, et al., 2022; Hong & Furnell, 2022; Ma, 2022; Philip, et al., 2023; Vrhovec, et al., 2023) potrjuje obstoj povezanosti ATB, SN, in PBC na BI. Raziskovalne hipoteze, ki temeljijo na TPB (H4–H6) so bile potrjene (p = 0,001). Naši rezultati naše naloge dodatno potrjujejo ustreznost TPB pri napovedovanju vedenj posameznikov v različnih družbenih in organizacijskih kontekstih.

Učinek dimenzij na BI zaposlenih, ki je prediktor vedenja samega je v naši raziskavi v celoti posredovan z NB zaposlenih. NB lahko obravnavamo tudi kot prediktor SN (Fishbein & Ajzen, 2011).

Povezanost ATB z BI je pozitivna in statistično značilna (*β = 0,306; f^2=0,131; t = 3,865; p < 0,001; 97,5 % CI [0,168; 0,481]*). Prav tako je povezanost SN z BI pozitivna in statistično značilna (*β = 0,161; f^2 = 0,029; t = 2,046; p = 0,041; 97,5 % CI [0,000; 0,307]*) ter povezanost NB z BI (*β = 0,369; f^2 = 0,160; t = 3,615; p < 0,001; 97,5 % CI [0,163; 0,570]*) in PBC z BI pozitivna in statistično značilna (*β = 0,124; f^2 = 0,035; t =3,272; p = 0,001; 97,5 % CI [0,049; 0,193]*) (tabela 34). R^2 vrednosti za BI znaša 0,623,

kar pomeni, da ATB, SN, NB in PBC pojasnijo 62,3 % variance BI. Največji učinek na BI imajo NB ($f^2 = 0,160$). Sledijo ATB ($f^2 = 0,131$), PBC ($f^2 = 0,035$) ter SN ($f^2 = 0,029$).

ATB je stabilen napovedovalec BI (Lee, et al., 2003; Bryan Foltz, et al., 2008; Zhang, et al., 2009; Hung, et al., 2012; Glegg, et al., 2013; Seyal & Turner, 2013; Ma, et al., 2015). Predhodne raziskave (Chau & Hu, 2002; Hung, et al., 2012; Ryu, et al., 2003), ki so preučevale področje sprejemanja zdravstvene IT med zdravniki, so podprle povezanost ATB na BI. ATB se je izkazal kot najbolj kritičen napovedovalec BI pri uporabi elektronskih zdravstvenih zapisov s strani zdravnikov (Mohd & Syed Mohamad, 2005; Egea & González, 2011).

Rezultati raziskave Bulgurcu, et al. (2010) kažejo, da v organizacijskem kontekstu ATB posameznikov do informacijske varnosti niso tako pomembna, kakor so pomembne SN. Navedeni rezultati so v nasprotju z raziskavo avtorjev Dinev & Hu (2007) ter Pavlou & Fygenson (2006), kjer so ugotovili, da je učinek SN na individualne BI nepomemben. Razliko v rezultatih je moč pojasniti z argumentom, da sta bili raziskavi avtorjev Dinev & Hu (2007) ter Pavlou & Fygenson (2006) izvedeni v popolnoma drugačnem kontekstu. SN so bile merjene za proaktivno vedenje in z vidika vpliva družbenega kroga posameznika (prijatelji, sorodniki).

Predhodne raziskave na področju zdravstva so pokazale, da imajo SN učinek na BI. Socialni vpliv igra kritično vlogo pri medicinskih sestrah in BI varovanja zasebnosti elektronskih zdravstvenih zapisov (Ma, et al., 2015). Slednje potrjujejo tudi drugi raziskovalci (Herath & Rao, 2009a; Hung, et al., 2012; Seyal & Turner, 2013; Zhang, et al., 2009). Prepričanja medicinskih sester so odvisna od družbenih norm referenčnih skupin (sodelavcev in nadrejenih). SN so pod vplivom sodelavcev in pod vplivom njihovih nadrejenih. Vpliv sodelavcev je najmočnejši napovedovalec SN (Ma, et al., 2015).

V naši raziskavi je bil udeležencem predstavljen scenarij v zdravstveni organizaciji, za katerega so ocenjevali elemente konstrukta SN. Vsi elementi za konstrukt SN so se nanašali na »pomembne« in vplivne« ljudi, katerih mnenje zaposleni v zdravstveni negi

cenijo. Ločeno smo, prav tako z uporabo scenarija merili konstrukt NB, katerega elementi so odražali strokovni krog sodelavcev in nadrejenih, kar ima tudi za posledico močnejši učinek norm na individualne BI (Hu, et al., 2012).

Raziskave za področje organizacijske klime kažejo pomembnost neposredno nadrejenega in njegov večji učinek na vedenje zaposlenih, kot naj bi ga imel vrhnji management (Zohar & Luria, 2005; Zohar & Hofmann, 2012). Vrhnji management določa politike in postopke celotne organizacije, izvajanje le-teh pa poteka na nižjih ravneh organizacije, pogosto v obliki diskrecijske pravice nadzornika. Taka implementacija vodi dojemanje zaposlenih glede organizacijske klime in vedenje zaposlenih (Zohar & Luria, 2005).

Kot navajajo Hahn, et al. (2021) ter Tan in Conde (2021), imajo vodje močan vpliv na skupino zaposlenih v zdravstveni negi, za katero so odgovorni. Zato je ustrezna predanost in zgledno informacijsko varnostno ravnanje nadrejenega ključnega pomena za vzpostavitev informacijske varnostne kulture. To je v skladu z raziskavo Ma, et al. (2015), kjer ima nadrejeni pomemben vpliv na SN, povezane z informacijsko varnostjo. Kar pa ni presenetljivo, saj vodja (nadrejeni) predstavlja vzor ostalim zaposlenim v zdravstveni negi (Hughes, 2017). Ta pogled premakne fokus dimenzije iz načelno strateške na bolj operativno raven odločanja. Očitno je, da je potrebno sprejemljivo vedenje približati zaposlenim. Vedenje je potrebno obravnavati na treh različnih ravneh – organizacijski, skupinski in individualni (Martins & Eloff, 2002).

Rezultati naše raziskave so pokazali, da ima PBC statistično značilno povezanost z BI, kar so pokazali tudi rezultati drugih raziskav (Chau & Hu, 2001; Lee, et al., 2003; Ryu, et al., 2003; Lin, 2007; Herath & Rao, 2009b; Zhang, et al., 2009; Hung, et al., 2012; Seyal & Turner, 2013; Hsieh, 2015; Ma, et al., 2015), vendar je učinek PBC na BI najmanjši, kar je v nasprotju s Pavlou in Fygenson (2006); Dinev in Hu (2007); Bulgurcu, et al. (2010) ter Hu, et al. (2012). Med raziskavami se kažejo razlike v učinkih konstruktov TPB na BI (Bulgurcu, et al., 2010; Hu, et al., 2012). Večji kot je posameznikov PBC in je vedenje enostavno uveljaviti, večja je verjetnost, da se bo posameznik vedel npr. v skladu z varnostnimi politikami. Najučinkovitejši način za dosego tega želenega vedenja je usposabljanje zaposlenih. Usposabljanje pa ne sme biti usmerjeno le na politike in same

postopke, temveč mora zajeti tudi uporabo IT in veščine za njihovo uporabo (Hu, et al., 2012).

Pomembno je poudariti, da se identificirane povezave lahko spremenijo zaradi drugih vidikov, ki prihajajo v ospredje. Raziskave kažejo, da so *vedenjske težnje* zaposlenih pogosto spregledane, a zelo pomembne (Uchendu, et al., 2021). Ob preučevanju človeških vidikov Van't Wout (2019) navaja, da bi morale organizacije sprejeti prilagojen pristop k informacijski varnostni kulturi in predlaga, da se zaposlene v organizaciji ocenjuje s psihološkega vidika, pri čemer se upoštevajo koncepti, kot so osebnost, interesi, potrebe in motivacija.

Informacijska varnostna kultura je skupek eksplicitnih in/ali implicitnih sil, ki so odgovorne za oblikovanje stališč in vedenja zaposlenih do informacijske varnosti na daljši rok. Zaposleni pod vplivom varnostne kulture razvijajo način razmišljanja in vedenja, ki se dotika informacijske varnosti na naraven in samoumeven način. Primer tega je uporaba močnih gesel, čeprav nameščanje le-teh od zaposlenih zahteva dodaten napor (Chen, et al., 2015).

5.2.3 Vloga kontrolnih spremenljivk na stališča do vedenja in vedenjsko namero (H7)

Raziskave z organizacijskega in vedenjskega področja priporočajo vključitev kontrolne spremenljivke oz. vključitev dejavnikov, ki bi zaradi svojih značilnosti lahko imeli učinek na odvisno spremenljivko – ATB in BI. Fishbein in Ajzen (2011) pravita, da imajo dejavniki v ozadju, kot so spol, starost, socialno-ekonomski status, izobrazba itd., posreden vpliv na ATB in BI ter so povezani z razlikami v vedenju. Vendar, da bi spol imel vpliv na BI, mora ta imeti učinek na še eno ali več spremenljivk, predvsem pa na ATB (Fishbein & Ajzen, 2011).

Ne glede na vedenje, ki ga preiskujemo, večina raziskav med drugim zbira podatke o demografskih značilnostih raziskovalne populacije. Najpogosteje so to podatki o spolu, rasi, etnični pripadnosti, starosti, izobrazbi, dohodku, družbenem razredu ali drugih kazalnikih socialno-ekonomskega statusa. Segmentacija populacije po teh dimenzijah

omogoča raziskovalcem, da ugotovijo, ali se razširjenost proučevanega vedenja razlikuje med podskupinami (Fishbein & Ajzen, 2011, p. 225).

Kljub temu, da so nekatere raziskave (Herath & Rao, 2009b; Gratian, et al., 2018; Mamonov & Benbunan-Fich, 2018) preučevale neposredno povezanost spola na ATB in BI, vloga spola še vedno ni popolnoma jasna. Nekateri raziskovalni modeli spol uporabljajo kot predhodnik konstruktov, kot so npr. zaznano tveganje (Garbarino & Strahilevitz, 2004), zaskrbljenost glede zasebnosti informacij (Mohamed & Ahmad, 2012), zaznana ranljivost, učinkovitost odzivanja in varnostna samoučinkovitost (Chen & Zahedi, 2016). Spol je v raziskovalnih modelih uporabljen tudi kot moderator (Maçada & Luciano, 2010).

Z našo raziskavo povezanosti med spolom ter ATB in BI zaposlenih v zdravstveni negi nismo zaznali.

Rezultati novejše metaanalize kažejo na manjše razlike v ATB med ženskami in moškimi (Cai, et al., 2017). Obstoječa literatura kaže na obstoj razlik med spoloma v dojemanju informacijske varnosti, za katere je bilo prav tako dokazano, da so povezane z varnostnim vedenjem (Anderson & Agarwal, 2010; Liang & Xue, 2010; Boss, et al., 2015; Mwagwabi, et al., 2018).

McGill in Thompson (2018) sta v svoji raziskavi »*Gender Differences in Information Security Perceptions and Behaviour*« dokazala, da imajo ženske nižjo stopnjo varnostnega vedenja kot moški, kar je skladno tudi s prejšnjimi raziskavami (Sheng, et al., 2010; Gratian, et al., 2018). Ženske naj bi obenem imele večje pomisleke glede ustreznosti informacijske varnosti (Laric, et al., 2009; Hoy & Milne, 2010; Mohamed & Ahmad, 2012) in izrazitejšo skrb glede spletne zasebnosti (Laric, et al., 2009; Milne, et al., 2009; Hoy & Milne, 2010; Mohamed & Ahmad, 2012). Pri iskanju razlogov za večjo dovzetnost žensk za phising napade so Sheng, et al. (2010) ugotovili, da je bilo njihovo tehnično znanje in usposabljanje slabše kot pri moških.

Roer in Petric (2018) sta v poročilu »*Age, Experience, Risk and Security*« predstavila povezanost med starostjo, izkušnjami, tveganji in varnostjo. Avtorja sta ugotovila, da so starost in izkušnje močno povezane z osebno strategijo obvladovanja tveganj in varnostnim vedenjem.

Z našo raziskavo povezanosti med starostjo ter ATB in BI zaposlenih v zdravstveni negi nismo dokazali.

Roer in Petric (2018) poročata o izrazitem trendu izboljšanja informacijske varnostne kulture s starostjo, kar zamaje pretekla opredeljevanja, da naj bi mladi, ki so odraščali z računalniki in rabo spleta, znali bolje rokovati s tehnologijo in bolj razumeli spletno varnost. Poročilo kaže, da se stališča do varnostne kulture izboljšujejo s starostjo in ta niso posledica večje izpostavljenosti tehnologiji, temveč posledica usposabljanja in družbenega konteksta na vedenje. Obstaja namreč nekaj pomembnih razlik v vedenju zaposlenih v organizaciji glede na starost. Ena izmed razlik je v ravnanju z občutljivimi informacijami, od katerih je 43,8 % zaposlenih do 35 let in 40,3 % zaposlenih od 36 do 45 let poročalo o dvomljivem ravnanju z občutljivimi podatki. Mlajši zaposleni so izkazovali bolj tvegano uporabo računalnika kot starejši. Skladnost z varnostnimi politikami organizacije se močno razlikuje glede na starostne razrede. Selektivna privrženost je najbolj prisotna med mlajšimi zaposlenimi (18,3 % zaposlenih pod 35 let). Ozaveščenost o »procesih v sili« je boljša pri starejših (Roer & Petric, 2018).

Le 50,9 % zaposlenih, starih 35 let in manj, ima pozitivna stališča do organizacijskega nadzora. Pozitivna stališča so razširjena med zaposlenimi v starosti od 36 do 55 let (75,6 %) in starejšimi od 55 let (72,0 %). Med mlajšimi prevladujejo negativna stališča do preventivnih ukrepov, medtem ko se starejšim zaposlenim preventivni ukrepi zdijo koristni za varnost organizacije – zaradi tega imajo starejši zaposleni pozitivnejša stališča do organizacijske varnosti (Roer & Petric, 2018).

Med različnimi starostnimi skupinami so razlike v znanju in zavedanju o varnosti. Več kot polovica (54 %) zaposlenih, starih od 36 do 45 let, ne bi opazili nenavadnega delovanja računalnika, medtem ko je odstotek nižji v preostalih starostnih skupinah.

Ozaveščenost o preventivnih ukrepih je na splošno nizka v vseh starostnih skupinah, so pa o njih precej bolj ozaveščeni zaposleni do 35. leta starosti (25,4 %), pri starejših od 55 let pa odstotek pade na 11,9 % (Roer & Petric, 2018).

Obstajajo tudi razlike med starostnimi razredi in uporabo komunikacijskih kanalov za hiter odziv na napade in sodelovanje v informacijskih varnostnih politikah. Hiter odziv na napade narašča s starostjo. Podoben trend gre opaziti tudi v percepciji zaposlenih o možnostih sodelovanja v razpravah o varnostnih vprašanjih. Zaposleni, mlajši od 35 let, izražajo nižjo stopnjo vključenosti v informacijsko varnostno politiko (31,4 %), medtem ko starejši od 55 let poročajo o visoki stopnji vključenosti (44,9 %) (Roer & Petric, 2018).

Posredovanje občutljivih sporočil je pogosteje zaznano kot neproblematična praksa med mlajšimi zaposlenimi. Polovica zaposlenih, starih 35 let in manj, je mnenja, da je izmenjava takih sporočil nekaj običajnega (50,3 %), medtem ko so starejši zaposleni pri posredovanju takšnih sporočil previdnejši (Roer & Petric, 2018).

Zaposleni iz različnih starostnih skupin se razlikujejo tudi pri zavedanju odgovornosti pri varnosti organizacije. Najvišjo stopnjo zavedanja osebne odgovornosti imajo zaposleni nad 55 let (94,1 %), najnižjo pa zaposleni do 35 let (Roer & Petric, 2018).

Število let zaposlitve v določeni organizaciji je značilnost populacije povezana z vidiki varnostne kulture. Dlje kot je posameznik zaposlen v organizaciji, boljša je njegova uspešnost v poddimenzijah, ki gradijo varnostno kulturo (Roer & Petric, 2018).

Z našo raziskavo povezave med delovno dobo ter ATB in BI zaposlenih v zdravstveni negi nismo dokazali (tabela 40).

Tvegano ravnanje z občutljivimi informacijami se je izkazalo za precejšnjo težavo pri zaposlenih z manj izkušnjami, saj jih je kar 43 % z manj kot 5 let delovne dobe poročalo o tveganem rokovanju z občutljivimi podatki. Stopnja tveganega ravnanja z občutljivimi podatki je še vedno precej visoka pri zaposlenih s 30 ali več leti delovne dobe (27,2 %). Zaposleni z več delovnimi izkušnjami pogosteje tudi razpravljajo o varovanju informacij.

Zavedanje osebne odgovornosti je zelo visoko med zaposlenimi s 30 in več leti delovne dobe (96,1 %); sledijo zaposleni z delovno dobo od 15 do 30 let (92,1 %) in od 5 do 15 let (90,5 %). Izstopa skupina z najmanj delovnimi izkušnjami, saj je zavedanje individualne odgovornosti najnižje (83,3 %) (Roer & Petric, 2018).

Z našo raziskavo nismo dokazali povezanosti stopnje izobrazbe z ATB in BI zaposlenih v zdravstveni negi.

Nobena od demografskih spremenljivk ni povezana z BI. Zaradi tega smo omenjene spremenljivke izključili iz nadaljnjih analiz merilnega in strukturnega modela.

5.3 RAZPRAVA O REZULTATIH RAZISKOVALNEGA VPRAŠANJA

Zdravstvene in socialnovarstvene ustanove naj za zmanjševanje tveganja za kršitev zaupnosti zdravstvenih podatkov s strani zaposlenih v zdravstveni negi uporabijo vzvode, kot so dimenzije informacijske varnostne kulture PO in ISKS. Čeprav imata omenjeni dimenziji majhno velikost učinka, gre za statistično pomembni povezanosti z ATB. Z omenjenima vzvodoma lahko organizacije delujejo na posameznikova ATB. Poleg tega imata omenjeni dimenziji posredni učinek na BI (tabela 36).

ATB so prediktor BI. Le-ta pa vodi v samo izvedbo vedenja, zatorej je smiselno delovati na ATB zaposlenih z ozaveščanjem, ki se osredotoča na njihova osebna prepričanja in etiko. Zaposleni se pogosto srečujejo z etičnimi dilemami, zato jih je smiselno vključiti v razprave. Na zaposlene naj se deluje preko kontinuiranih izobraževanj. Ob tem je pomembno, da se tudi sami znajdejo v vlogi tistega, ki podaja znanje ali izkušnje. Rezultati so pokazali, da je najnižja vrednost mediane prav pri dimenziji ISKS (tabela 18).

Organizacije naj kot vzvod uporabijo tudi dimenzijo SO. Kljub majhnemu učinku ima dimenzija statistično pomembno povezanost z NB.

Čeprav obstajajo pomembne povezave z dimenzijami informacijske varnostne kulture, te razlagajo relativno nizek delež variabilnosti v ATB, SN in PBC ($R^2 < 0{,}10$). Ob tem velja poudariti, da imajo največji učinek na BI prav NB, sledijo pa jim ATB (tabela 34).

Vzvod, ki naj ga uporabijo organizacije, naj bo tudi dimenzija SETA. Kljub majhnemu učinku gre za dimenzijo, ki ima statistično značilno povezanost s PBC.

5.4 OMEJITVE RAZISKAVE

Naša raziskava ima nekaj omejitev, ki jih je potrebno izpostaviti in upoštevati pri posploševanju rezultatov in nadaljnjem delu na tem področju.

Prva izmed njih je ta, da je informacijska varnostna kultura večdimenzionalen in kompleksen koncept, zato odločitev za uporabo kateregakoli teoretičnega okvirja nalaga določene omejitve. Za preučevanje tega fenomena smo izbrali operacionalizacijo po Nasir, et al. (2019a, b) in modelu dodali dodatni dimenziji PO in SO, predstavljeni v Mikuletič, et al. (2024).

Druga omejitev je uporaba ankete za vrednotenje BI. Z raziskavo nismo merili vedenja zaposlenih v zdravstveni negi. Prav gotovo bi relevantnejše rezultate dobili z analizo opazovanja vedenja zaposlenih v delovnih okoljih. Vendar je k dejanski analizi vedenja smiselno pristopiti, ko imamo zbrane podatke o količini, obsegu in značilnostih pojava ter morebitni povezanosti opazovanih spremljanih spremenljivk, kar nam omogoča presečno raziskovanje. Ker je naša raziskava omenjenega tipa, so bili podatki zajeti v določenem časovnem okvirju na populaciji poklicne skupine zaposlenih v zdravstveni negi. Rezultati naše raziskave se torej nanašajo na določeno omejeno časovno obdobje. Iz rezultatov smo tako lahko kvečjemu analizirali odnos med omenjenimi konstrukti, ne pa tudi vzročne povezanosti. Ker take raziskave še ni bilo izvedene v Sloveniji, je uporaba omenjenega raziskovalnega dizajna upravičena. Izvedena raziskava nam je namreč dala osnove za uporabo dizajnov višje ravni hierarhije dokazov.

Slovenska različica vprašalnika je bila prilagojena za področje zdravstvene nege, zato je tretja omejitev raziskave ta, da je rezultate mogoče posplošiti zgolj na tarčno populacijo zaposlenih v zdravstveni negi v Sloveniji. Udeleženci raziskave predstavljajo heterogeno skupino naključnega vzorca ciljne populacije.

Problem dostopnosti do spletne ankete (napaka nepokritja) vsem zaposlenim v zdravstveni negi je četrta omejitev, saj vedno obstaja možnost, da vsi nimajo dostopa do interneta ali ne spremljajo elektronskih sporočil Zbornice – Zveze. Prav tako omenjena institucija trenutno še ne razpolaga z elektronskimi naslovi vseh zaposlenih v zdravstveni negi in vsi člani Zbornice – Zveze ne berejo informativnega biltena Utrip. Potrebno je še upoštevati, da so v Sloveniji tudi zaposleni v zdravstveni negi, ki niso člani Zbornice – Zveze in le-te smo poskušali zajeti s povabilom k raziskavi, ki smo ga objavili na družbenem omrežju Facebook.

Peta omejitev je samoocenjevanje, saj je le-to podvrženo pristranosti, v primeru informacijske varnosti pa smo pričakovali celo družbeno zaželene odgovore.

Pri izvedbi ankete vedno ostajajo odprta vprašanja, ki zadevajo problem pristranosti podatkov zaradi CMB. Zaradi tega smo v vprašalnik vnesli spremenljivko, ki se nanaša na družbeno zaželenost (Hays, et al., 1989). Slednjo smo uporabili za ugotavljanje CMB učinka v kasnejši fazi analize podatkov (Podsakoff, et al., 2003). Rezultati analiz za ugotavljanje te vrste težav so pokazali, da v zbranih podatkih ni prisotnega CMB (priloga 13).

5.5 PRILOŽNOSTI ZA NADALJNJE RAZISKOVANJE

Težko je spregledati vlogo, ki jo ima organizacijska kultura, zlasti glede na raziskave, ki širijo uporabo Scheinovega modela organizacijske kulture in tiste, ki kažejo, da je varnostna kultura subkultura organizacijske kulture. Kot pravijo Uchendu, et al. (2021), je gledanje na informacijsko varnostno kulturo kot na subkulturo upravičeno, vendar pa Whelan (2017) navaja, da je za resnično razumevanje subkultur znotraj in med organizacijami potrebno opraviti veliko več raziskav.

V literaturi gre zaslediti prevladujočo domeno teoretičnih okvirjev informacijske varnostne kulture. Uporabljeni pristopi se med seboj razlikujejo, vendar je nekatere težko uporabiti, predvsem zaradi značilnosti organizacij. Vse organizacije recimo nimajo enakih sredstev in predstavljajo različne panoge, ki se srečujejo z različnimi vrstami vprašanj. Vse vodijo do iskanja pristopov, ki jih je mogoče po potrebi dodatno prilagoditi določenemu sektorju ali organizaciji. Uporaba vprašalnikov, kot je npr. vprašalnik za ocenjevanje znanja o informacijski varnosti je pogosta. Edini način za razvoj učinkovitih orodij je tesna interakcija med praktiki in raziskovalci, kjer lahko praktiki zagotovijo resnična okolja za opravljanje raziskave, raziskovalci pa svoje strokovno znanje o načrtovanju in vrednotenju orodja. Takšne interakcije lahko omogočijo tudi srednjeročno in dolgoročno uporabo in izboljšanje meritev, ki lahko koristijo organizacijam.

Vsaka organizacija mora uporabiti pristop ali okvir na način, ki ustreza že vzpostavljenim sistemom in strukturam (Pătrașcu, 2019). Ključna gonilna sila za razumevanje, upravljanje, podporo in spreminjanje informacijske varnostne kulture temelji na razumevanju trenutnega stanja informacijske varnosti, vlaganju v posebne pobude, ki pomagajo zmanjšati stroške, hkrati pa zmanjšati tveganje za informacijsko varnost in ustvarjanje trajnostnega pristopa k upravljanju in izboljšanju fenomena (Govender, et al., 2020). Vendar pa lahko individualno vsako organizacijo in zaposlenega gledamo kot na vprašanje, ki ga je v raziskavah potrebno obravnavati skupaj oz. v celoti. Iz literature je razvidno, da je le malo pristopov ovrednotenih v znatnem časovnem obdobju, zato je tudi težko razumeti njihovo resnično vrednost za raziskovalce in zaposlene v organizacijskih okoljih. Vsekakor je delo v prihodnosti nujno potrebno, v kolikor se želimo resnično soočiti z varnostnimi izzivi v zdravstvenih ustanovah.

Vprašalnik, ki je bil preveden in prilagojen za področje zdravstvene nege bi v prihodnosti lahko uporabili kot merski instrument za pridobivanje podatkov pri zaposlenih v zdravstveni negi tudi v tujini. Ker je ena od obveznosti doktorskega študija objava rezultatov raziskave v reviji s faktorjem vpliva, smo z objavo vprašalnik naredili tudi mednarodno dostopen (Mikuletič, et al., 2024). Tako bo vprašalnik mogoče prevesti tudi v ostale jezike in omogočiti njegovo mednarodno rabo na področju zdravstvene nege. Smiselno bi bilo preveriti, kako se dojemanje dimenzij informacijske varnostne kulture

in njihova povezanost s konstrukti TPB razlikujejo od države do države. Prednost vprašalnika je, da omogoča razmeroma enostavno ugotavljanje realnega stanja znotraj posamezne zdravstvene organizacije. Z njegovo uporabo bodo lahko organizacije identificirale probleme in razumele vedenje zaposlenih glede informacijske varnosti. Prednost vprašalnika je tudi njegova prilagodljivost za ostala področja kršitev informacijske varnosti z zamenjavo scenarijev (npr. primer dajanje informacij po telefonu, posojanje gesel ipd.).

Specifičen dejavnik, ki se pojavlja v raziskavah je nacionalna kultura, kar nakazuje, da ima informacijska varnostna kultura na nacionalni ravni tudi ključno vlogo pri gradnji organizacijske informacijske varnostne kulture (Uchendu, et al., 2021). Ko se informacijska varnost obravnava na nacionalni ravni, ta pomaga vzpostaviti prizadevanja tudi v organizacijah. Prihodnje raziskave bi se lahko opredelile do preučevanja o kultivaciji nacionalne informacijske varnostne kulture, vendar bi bila taka kultivacija za prebivalstvo bistveno večji izziv v primerjavi z organizacijo (Uchendu, et al., 2021). Bada, et al. (2019) so npr. preučili nacionalno ozaveščenost o kibernetski varnosti v afriških državah in ugotovili, da bi morali po opredelitvi področij nacionalnih potreb po kampanjah ozaveščanja vključiti deležnike iz različnih sektorjev ter vključiti člane izvršnega odbora in zaposlene v malih in srednje velikih podjetjih.

5.6 PRISPEVEK K ZNANOSTI IN K RAZVOJU ZNANSTVENE DISCIPLINE

Z rezultati doktorske naloge pozivamo k pozornosti, kako so dimenzije informacijske varnostne kulture povezane s konstrukti prepričanj in dopolnjujemo obstoječo literaturo s širitvijo obzorja za naslednje raziskave in razvoj novih teorij.

Pričujoča raziskava je ena prvih, ki preučuje nepooblaščen dostop do zdravstvenih podatkov z vidika informacijske varnostne kulture pri zaposlenih v zdravstveni negi in daje pomemben teoretični prispevek k bodočim raziskavam informacijske varnostne kulture za področje zdravstvene nege, širše tudi zdravstva. Gre za raziskavo, ki ima več teoretičnih implikacij. Združuje teoretični okvir TPB in na dimenzijah temelječ model

informacijske varnostne kulture v eno celoto, katere namen je ugotavljanje povezanosti dimenzij na konstrukte TPB in BI zaposlenih v zdravstveni negi za izvedbo nepooblaščenega dostopa do zdravstvenih podatkov v organizacijskem okolju. Pri tem poudarja kritično vlogo, ki jo igrajo dimenzije informacijske varnostne kulture pri upravljanju informacijske varnosti, obenem pa izpopolnjuje razumevanje posebnih mehanizmov, preko katerih dimenzije oblikujejo ATB, SN, NB ter PBC zaposlenih v zdravstveni negi glede omenjene kršitve.

Raziskava definira in operacionalizira dve novi dimenziji informacijske varnostne kulture – PO in SO. Omenjeni sta bili podprti z EFA in CCA ter prestali teste veljavnosti in zanesljivosti. Enako velja tudi za ostalih sedem dimenzij. Poleg tega rezultati kažejo, da imata novi dimenziji različni vlogi pri oblikovanju ATB in dojemanju družbenih norm v zvezi z nepooblaščenim dostopom do podatkov.

Pomemben prispevek doktorske disertacije k znanosti je prevod in prilagoditev vprašalnika. Vprašalnik omogoča veljaven in zanesljiv način merjenja teoretičnih konstruktov. Gre za eno prvih raziskav, ki vključuje tako konstrukt SN kot tudi NB v isti raziskovalni model. Gledano iz teoretičnega zornega kota, so NB predhodnik SN (Bulgurcu, et al., 2010). Gre za konstrukte, ki so bili v literaturi pogosto uporabljeni kot alternativa, ki obravnava družbeni vpliv na posameznika (Lebek, et al., 2014). Zato je malo znanega o njihovem odnosu. Rezultati so pokazali, da gre za različna konstrukta, čeprav glede na njuno vlogo pri razlagi vedenja podobna. CCA je potrdila razlikovanje med konstruktoma. Oba sta tudi prestala vse teste veljavnosti in zanesljivosti. Povezavi med SN in BI ter NB in BI se razlikujeta glede na velikost učinka. Medtem ko je velikost učinka SN majhna, je velikost učinka NB na BI srednja velika. Ne glede na to, sta obe povezavi statistično značilni, ko sta hkrati vključeni v model, kar nakazuje, da predstavljata različni dimenziji družbenega vpliva in nista alternativi, ki naj bi ju bilo mogoče uporabiti izmenično.

Potrditev primernosti TPB pri preučevanju vedenj na področju informacijske varnosti v zdravstveni negi predstavlja enega od pomembnejših doprinosov k znanosti pričujoče doktorske disertacije.

5.6.1 Možen prenos spoznanj raziskave na aplikativno raven

Pričujoča raziskava ima nekaj praktičnih implikacij, ki lahko pomagajo zdravstvenim delavcem in oblikovalcem politik pri obvladovanju nepooblaščenega dostopa do zdravstvenih podatkov s strani zaposlenih v zdravstveni negi ali drugih zdravstvenih delavcev ter pomagajo razvijati in načrtovati programe usposabljanja.

Rezultati raziskave lahko pomagajo določiti intervencije takšnih ozaveščanj. V osnovi lahko ozaveščanja ciljajo na krepitev družbenega vpliva na zaposlene v zdravstveni negi, njihove odnose ali oboje. Odnos zaposlenih v zdravstveni negi je mogoče okrepiti z ozaveščanjem, ki se osredotoča na njihova osebna prepričanja in etiko. Poklicna etika igra pomembno vlogo pri omenjeni populaciji, zato je poudarjanje neetičnih vidikov nevarnega vedenja lahko za to populacijo relativno učinkovito. Ker so zaposleni v zdravstveni negi pogosto soočeni z etičnimi dilemami, bi bilo smiselno vključiti razprave o najpogostejših etičnih dilemah v ozaveščevalne programe. Slednje bi lahko pripomoglo k boljšemu razumevanju in ravnanju v situacijah, kjer se takšne dileme pojavljajo in k oblikovanju sprejemljivega vedenja, kar bi zaposlene v zdravstveni negi oplemenitilo z znanjem, kako ravnati v etično spornih okoliščinah. Organizacije bi lahko začele spremljati raven družbenega vpliva in/ali odnosa zaposlenih, da bi ugotovile, katere ozaveščevalne intervencije so potrebne v določenem trenutku. S tem pristopom bi organizacije lahko bolje usmerjale svoje napore v izboljšanje etičnega ravnanja zaposlenih.

5.7 IZVIRNI PRISPEVEK K RAZVOJU STROKE

Informacijska varnostna kultura je na področju zdravstva in zdravstvene nege kot discipline razmeroma slabo raziskana. Po nam znanih podatkih je malo raziskav, ki preučujejo obravnavano temo, predvsem takih, ki bi v zadostni meri pojasnjevale povezave s samo namero kršitve informacijske varnosti.

Z doktorsko disertacijo tako pomembno prispevamo k razvoju stroke z izsledki, ki predstavljajo kakovostno izhodišče za nadgradnjo formalnih in neformalnih

izobraževalnih programov, namenjenih zaposlenim v zdravstveni negi. Na ta način lahko stroko zdravstvene nege oplemenitimo z dodatnim praktičnimi znanji, ki so nepogrešljiva pri uporabi sodobne IKT. Uvedba programov, ki ciljajo na spreminjanje ATB, SN in PBC, niso le pomembna dopolnila, temveč nujne učinkovite komponente za upravljanje z varnostjo informacij.

Informacijsko varnostno kulturo na področju zdravstvene nege je mogoče krepiti tudi preko nacionalnih organov ali strokovnih združenj. Kar temelji na predpostavki, da obravnava ne poteka le na organizacijski ravni, temveč tudi na drugih ravneh, kot so skupina, stroka, država (Sharma & Aparicio, 2022). Zaradi tega je smiselno, da tudi nacionalna telesa ali strokovna združenja vključijo in nudijo usmerjanje in izobraževanje o pomembnih vidikih informacijske varnostne kulture na področju zdravstvene nege.

6 SKLEPI

- Pričujoča raziskava je ena prvih, ki preučuje nepooblaščen dostop do zdravstvenih podatkov z vidika informacijske varnostne kulture med zaposlenimi v zdravstveni negi.
- Raziskava prispeva k teoriji z identifikacijo in operacionalizacijo novih dimenzij informacijske varnostne kulture, poudarjajoč ločeno vlogo subjektivnih norm in normativnih prepričanj v kontekstu informacijske varnosti.
- Raziskava izpostavlja kompleksne odnose med dimenzijami informacijske varnostne kulture, stališči do vedenja, subjektivnimi normami, normativnimi prepričanji in zaznanim vedenjskim nadzorom.
- Izsledki raziskave doprinašajo k razumevanju informacijske varnostne kulture ter povezanosti njenih dimenzij na vedenjsko namero zaposlenih v zdravstveni negi do nepooblaščenega dostopa do zdravstvenih podatkov.
- Rezultati raziskave osvetljujejo pomembne povezave med dimenzijami informacijske varnostne kulture, t.s. usmerjenost k zagotavljanju zasebnosti, usmerjenost k varnosti podatkov, izmenjava znanja o informacijski varnosti; varnostno izobraževanje, usposabljanje in ozaveščanje. Na ta način vzpostavlja posredno povezavo med informacijsko varnostno kulturo in nepooblaščenim dostopom do zdravstvenih podatkov.
- Rezultati v celoti potrjujejo primernost Teorije načrtovanega vedenja pri razlaganju nepooblaščenega dostopa do zdravstvenih podatkov s strani zaposlenih v zdravstveni negi. Povezave med konstrukti Teorije načrtovanega vedenja so vse statistično pomembne in pojasnjujejo velik del variabilnosti v vedenjski nameri.
- Povezava med normativnimi prepričanji in vedenjsko namero ima največjo velikost učinka in tako presega prag za srednjo velikost učinka. Povezava med stališči do vedenja in vedenjsko namero je rahlo pod tem pragom. Omenjeni povezavi sta najpomembnejši pri oblikovanju vedenjske namere in posledično vedenja – izvedba kršitve varnosti zdravstvenih podatkov. Čeprav obstajajo statistično pomembne povezave med subjektivnimi normami in vedenjsko namero ter zaznanim vedenjskim nadzorom in vedenjsko namero, imajo omenjene majhno velikost učinka, kar kaže, da so manj pomembni napovedovalci.

- Raziskava ni dokazala povezanosti med spolom, starostjo, delovnimi izkušnjami, stopnjo izobrazbe s stališči do vedenja in vedenjsko namero.
- Izsledki raziskave imajo praktične implikacije, ki lahko pomagajo zdravstvenim strokovnjakom pri obvladovanju kršitev varnosti zdravstvenih podatkov s strani zaposlenih v zdravstveni negi ali drugih zdravstvenih profilov.
- Izsledki raziskave lahko pomagajo pri razvoju in načrtovanju programov usposabljanja, na način, da določijo smeri, v katerih naj se izvajajo intervencije ozaveščanja. V osnovi naj se intervencije osredotočajo na krepitev družbenega vpliva na zaposlene v zdravstvu in zdravstveni negi ter njihovih stališč do vedenja.
- Nadaljnje raziskovanje z obstoječim vprašalnikom, ki je prilagojen za področje zdravstva ter zdravstvene nege, znotraj posameznih organizacij kot del ocenjevanja stanja informacijske varnostne kulture ter potencialnih nevarnosti kršitev informacijske varnosti znotraj naše države in širše, saj vprašalnik predstavlja dober merski instrument.
- Omejitve raziskave so uporaba presečnega načrta, ankete za vrednotenje vedenjske namere, napaka nepokritja, posploševanje rezultatov na tarčno populacijo ter samoocenjevanje.

7 ZAKLJUČEK

Informacijska varnostna kultura je na področju zdravstva razmeroma slabo raziskana. S pričujočo raziskavo smo ugotovili obseg, količino in značilnosti pojava; prepoznali smo povezane dejavnike v zvezi s katerimi je smiselno uvajati ukrepe izboljšav pri delu z zaposlenimi in procesom dela, da bi lahko zmanjšali incidenco kršenja informacijske varnosti. Na ta način smo identificirali vzvode, ki jih lahko uporabijo zdravstvene in socialnovarstvene ustanove za zmanjšanje tveganja za kršitev zaupnosti zdravstvenih podatkov s strani zaposlenih v zdravstveni negi ter tako identificirali priporočila namenjena managementu zdravstvenih ustanov, kako izboljšati stanje na tem področju.

Višjo raven informacijske varnosti je moč doseči z razumevanjem delovanja organizacijskih, kulturnih in individualnih kognitivnih dejavnikov na vedenjsko namero in vedenje samo. Raziskava je potrdila, da so uveljavljene vedenjske determinante povezane z vedenjsko namero zaposlenih v zdravstveni negi glede izvedbe nepooblaščenega dostopa do zdravstvenih podatkov. Z raziskavo smo dokazali povezanost nekaterih dimenzij informacijske varnostne kulture na vedenjsko namero zaposlenih v zdravstveni negi.

Izvedena raziskava je tako dala eksplorativni vpogled v opisan raziskovalni problem. Tako izvedena raziskava in spoznanja le-te so primerni temelji za zasnovo eksplikativne raziskave v izbranih kliničnih okoljih, ki vključuje metodo sistematičnega opazovanja in nadzora neodvisnih in odvisnih spremenljivk v neposrednem okolju na randomiziranem vzorcu. Naša raziskava tako prispeva nabor neodvisnih in odvisnih spremenljivk, ki jih je smiselno opazovati s prospektivnimi raziskovalnimi metodami v naslednjih raziskavah.

Raziskovalni model je potrebno v prihodnosti uporabili tudi na drugih poklicnih skupinah v zdravstvu, da bi tako lahko pridobili širšo sliko povezanosti informacijske varnostne kulture s konstrukti TPB.

8 SUMMARY

Protecting sensitive health data represents a major challenge. Nursing employees, who make up a large part of the healthcare workforce and have direct access to health data, play a crucial role in this endeavour. Although information security culture is critical to the protection of health data, the relationship between these two concepts remains unclear.

The aim of this study was to investigate the phenomenon of unauthorised access to health data in the Slovenian nursing staff population and to explore the relationship between the dimensions of information security culture and the attitudes, subjective norms, normative beliefs, perceived behavioural control and behavioural intentions related to committing such breaches.

The literature review revealed an increase in health data security breaches, a lack of research in the field of nursing, and unclear conceptualisations of information security culture. In addition, there is a need to distinguish the factors that constitute or influence this phenomenon.

The research objectives were as follows:

- To examine the concept of the dimensions and current state of information security culture among nursing staff in the Republic of Slovenia.
- To examine the relationship between the dimensions of information security culture and the constructs of the Theory of Planned Behaviour.
- To identify the levers related to information security culture that healthcare and social welfare institutions can utilise to reduce the risk of breaches of health data confidentiality by nursing employees.

The main research question was: »To what extent do the dimensions of information security culture provide a good indicator of the behavioural intention for information security breaches in nursing employees?«

The term »dimensions of information security culture« encompasses the following meanings: procedural countermeasures; risk management; security education, training, and awareness; top management commitment; security monitoring; information security knowledge; information security knowledge sharing; security oriented; and privacy oriented.

Seven hypotheses were tested in the study:

- H1: The dimensions of information security culture are negatively correlated with nurses' attitudes towards nursing staff behaviour of unauthorised access to health data.
- H2: The dimensions of information security culture are negatively correlated with nurses' subjective norms or normative beliefs regarding unauthorised access to health data.
- H3: The dimensions of information security culture are negatively correlated with nurses' perceived behavioural control regarding unauthorised access to health data.
- H4: Attitudes towards nurses' behaviour related to unauthorised access to health data are positively correlated with the behavioural intention to commit such breaches.
- H5: Nurses' subjective norms and normative beliefs regarding unauthorised access to health data are positively correlated with the behavioural intention to commit such breaches.
- H6: Nurses' perceived behavioural control over unauthorised access to health data is positively correlated with the behavioural intention to commit such breaches.
- H7: Variables such as nurses' age, education, and work experience are negatively correlated with their attitude towards behaviours and behavioural intentions regarding unauthorised data access.
- H7a: Nurses' age is negatively correlated with their attitudes towards the behaviour of unauthorised access to health data.
- H7b: Nurses' age is negatively correlated with their behavioural intentions to commit unauthorised access to health data.

- H7c: Nurses' education is negatively correlated with their attitude towards the behaviour of unauthorised access to health data.
- H7d: Nurses' education is negatively correlated with their behavioural intentions to commit unauthorised access to health data.
- H7e: Nurses' work experience is negatively correlated with their attitude towards the behaviour of unauthorised access to health data.
- H7f: Nurses' work experience is negatively correlated with their behavioural intention to commit unauthorised access to health data.

A cross-sectional study with a one-off sample was conducted. The cross-sectional study had its foundations in the preliminary qualitative research, the aim of which was to explore the conceptualisation of the phenomenon in the field of nursing and health care. Seventeen interviews were conducted with experts from the fields of nursing and clinical informatics. The interviews revealed that, in addition to the dimensions defined in the literature, information security culture manifests a specific dimension that reflects the discipline of nursing.

The sample included 527 nurses, of whom there were 70 (13.3%) males and 457 (86.7%) females. The average age of the participants was 42.4 years (SD = 10.4), with the youngest being 22 years old and the oldest being 63 years old. Participants' average work experience in the organisation was 16.7 years (SD = 11.9), with a minimum of less than one year and a maximum of 42 years. The sample consisted of 23.5% (n = 124) registered nurses, 3.6% (n = 19) of higher-level nurses / higher medical technicians, 58.4% (n = 308) of graduate nurses / graduate health professionals, and 14.4% (n = 76) master's degree holders in nursing. The type of organisation where the participants were employed was distributed as follows: 24.3% (n = 128) in health centres, 19% (n = 100) in general hospitals, 4.6% (n = 24) in specialised hospitals, 20.7% (n = 109) in clinical centres (including clinics), 3% (n = 16) in independent clinics, 1.3% (n = 7) in institutes, 23.8% (n = 125) in social care institutions, and 3.2% (n = 17) in other institutions.

The online survey was conducted between April 2021 and March 2022. Respondents were recruited through various channels. Firstly, the Nurses and Midwives Association

of Slovenia sent the invitation to participate in the research project to over 12,000 e-mails of their members, all nursing employees. The Association also posted the invitation in its Facebook group. In addition, the nursing interest groups under the auspices of the Association were encouraged to disseminate the invitation among their members. Next, Slovenian health and social care institutions were asked to distribute the invitation among their contacts. Finally, the target population was also invited to participate via the magazine Utrip, which, in addition to its online edition, has a circulation of 15,300 printed copies.

To measure the dimensions of information security culture, a translated and adapted questionnaire by Nasir, Abdullah Arshah and Ab Hamid (2019) was used. The items of the questionnaire are the result of the work of several researchers. Two new constructs were added to the questionnaire, namely Security Oriented (emerging from the review of the relevant literature) and Privacy Oriented (based on the results of the preliminary qualitative research).

The research was approved by the Commission of the Republic of Slovenia for Medical Ethics on 2 February 2021 (No. 0120-583/2020/7). Before taking the survey, participants were informed that by filling out the questionnaire they consented to participate in the study.

The data collected was analysed using IBM SPSS 22.0 and SmartPLS 4.0.8.3. To determine the associations between the data, descriptive statistical analyses were used (i.e., representation of the sample size (N), percentages (%), frequencies (f), minimum (Min), maximum (Max) and mean values). Inferential statistical analyses were then performed to test and verify the hypotheses. We also performed an evaluation of the measurement and structural model with reflective constructs.

As the research model included two newly developed theoretical constructs, we first conducted an exploratory factor analysis (EFA), and then a confirmatory composite analysis (CCA). Convergent validity was determined through an analysis of the average variance extracted (AVE) and factor loadings of the items on the corresponding latent

variables. Discriminant validity was assessed by analysing the heterotrait-monotrait ratio of correlations (HTMT) and the Fornell-Larcker criterion. Reliability was determined using Cronbach's alpha (CA) and composite reliability (CR). The results confirmed the validity and reliability of the defined and operationalised dimensions of information security. The data collected was also tested for potential common method bias using Harman's single factor test, which showed that the largest factor accounted for 35.96% of the variance, indicating no serious risk for common method bias.

The results showed that the two dimensions with the lowest median value were Security Monitoring and Information Security Knowledge Sharing, while the highest median value was observed for Privacy Oriented. A weak but positive correlation was found between the age of the participants and the Risk Management dimension ($r_s = 0.211; n = 527; p < 0.001$), as well as between the number of years of service, Procedural Countermeasures ($r_s = 0.167; n = 527; p < 0.001$), Risk Management ($r_s = 0.123; n = 527; p = 0.005$), and Security Education, Training and Awareness ($r_s = 0.142$; $n = 527$; $p < 0.001$). Statistically significant differences in the mean ranks between men and women were identified for the Security Monitoring ($U\ (n_{man} = 70, n_{female} = 457) = 12069.5; Z = -3.330; p = 0.001$) and Information Security Knowledge Sharing ($U\ (n_{man} = 70\ , n_{female} = 457) = 12762.5; Z = -2.739; p = 0.006$) dimensions. The results of the Kruskal-Wallis H test showed no statistically significant differences in the mean values of the ranks of the dimensions of information security culture depending on the education level, organisations or levels of health care.

Hypotheses H1-H6 were tested using a structural model. For an easier interpretation of the results, effect sizes (f^2) and confidence intervals ($CI: 2.5; 97.5\%$) were calculated for all assumed relations.

The dimensions Privacy Oriented; Procedural Countermeasures; Security Education, Training and Awareness; Top Management Commitment; Security Monitoring and Information Security Knowledge were negatively correlated with Attitude Towards Behaviour. However, of these dimensions, only the Privacy Oriented dimension showed a statistically significant association with Attitude Towards Behaviour ($\beta = -0.269; f^2 =$

0.039; t = 2.118; p = 0.034; 97.5% CI [-0.525; -0.029]). Conversely, a positive and statistically significant correlation was found between Attitude Towards Behaviour (*β = 0.167; f^2=0.010; t = 2.385; p = 0.017; 97.5% CI [0.030; 0.304]*) and the Information Security Knowledge Sharing dimension. H1 was therefore partially confirmed.

The significant negative association between Privacy Oriented and Attitude Towards Behaviour suggests that the attitude may be shaped by internal "bottom-up" factors pertaining to organisational culture. Personal beliefs, values, and ethics shape individuals' attitudes toward unlawful acts, such as unauthorised access to health data.

The results of this research also partially confirm H2. The dimensions Security Oriented; Privacy Oriented; Procedural Countermeasures; Security Education, Training and Awareness; Top Management Commitment, and Security Monitoring showed a negative correlation with Subjective Norms, although none of these correlations were found to be statistically significant. Similarly, the dimensions Privacy Oriented; Security Education, Training and Awareness; Security Monitoring, and Security Oriented were found to have a negative association with Normative Beliefs, but only the Security Oriented dimension showed a statistically significant correlation (*β = -0.313; f^2 = 0.041; t = 3.320; p = 0.001; 97.5% CI [-0.490; -0.117]*).

The negative association between Security Oriented and Normative Beliefs may suggest that the social influence may stem from "top-down" organisational data protection practices, dictating how employees are to deal with information security. These results suggest that social influence is based on individual perception of important organisational values, norms, and accepted ways of working as defined by organisational policies and legal acts.

The Privacy Oriented; Security Education, Training and Awareness and Top Management Commitment dimensions were found to have a negative correlation with Perceived Behavioural Control. Among these, only Security Education, Training and Awareness showed a statistically significant correlation with Perceived Behavioural

Control (*β = -0.253; f^2=0.018; t = 2.235; p = 0.025; 97.5% CI [-0.471; -0.032]*). H3 was therefore partially confirmed.

H4-H6 were confirmed, as the results indicate that the relationship between Attitude Towards Behaviour and Behavioural Intention was found to be positive and statistically significant (*β = 0.306; f^2 = 0.131; t = 3.865; p < 0.001; 97.5% CI [0.168; 0.481]*). Similarly, the relationship between Subjective Norms and Behaviour Intention was found to be positive and statistically significant (*β = 0.161; f^2 = 0.029; t = 2.046; p = 0.041; 97.5% CI [0.000; 0.307]*), as was the relationship between Normative Beliefs and Behaviour Intention (*β = 0.369; f^2 = 0.160; t = 3.615; p < 0.001; 97.5% CI [0.163; 0.570]*), and the positive and statistically significant relationship between Perceived Behavioural Control and Behaviour Intention (*β = 0.124; f^2= 0.035; t =3.272; p = 0.001; 97.5% CI [0.049; 0.193]*).

Our analyses found no statistically significant relationship between the variable Age and Attitude Towards Behaviour or Behavioural Intention, while the variables Attitude Towards Behaviour and Behavioural Intention were found to be statistically significantly correlated. H7a and b were rejected.

Our analyses found a statistically significant relationship between the education level variable and Attitude Towards Behaviour and Behavioural Intention, but it was extremely weak with both Spearman's rho coefficients below 0.3 (Attitude Towards Behaviour -0.246 and Behavioural Intention -0.187). Therefore, H7c and d were rejected.

The results show no statistically significant relationship between the variable work experience and Attitude Towards Behaviour and Behavioural Intention. Consequently, H7e and H7f were also rejected.

Answer to the research question: The largest indirect effect on the Behavioural Intention of nursing staff with regard to unauthorised access to health data is exerted by the dimension Privacy Oriented (*β = -0.154; t = 2.346; p = 0.019; 97.5% CI [-0.288; -0.025]*). Another dimension with an indirect effect on Behavioural Intention is the

Information Security Knowledge Sharing dimension (*β = 0.133; t = 2.155; p = 0.031; 97.5% CI [0.245; 0.133]*). The relationship between Privacy Oriented and Attitude Towards Behaviour, Information Security Knowledge Sharing and Attitude Towards Behaviour, Security Oriented and Normative Beliefs, Security Education, Training and Awareness and Perceived Behavioural Control, Attitude Towards Behaviour and Behavioural Intention, Subjective Norms and Behavioural Intention, Perceived Behavioural Control and Behavioural Intention were found to have small effect sizes, while the link between Normative Beliefs and Behavioural Intention was found to have a medium effect size. Although there were significant correlations with information security dimensions, they only explain a relatively small percentage of the variability in Attitude Towards Behaviour, Subjective Norms and Perceived Behavioural Control (R^2 < 0.10). The R^2 values for Behavioural Intention were 0.623, which means that Attitude Towards Behaviour, Subjective Norms, Normative Beliefs, and Perceived Behavioural Control explain 62.3% of the variance in Behavioural Intention. The largest effect on Behavioural Intention can be attributed to Normative Beliefs ($f^2 = 0.160$), followed by Attitude Towards Behaviour ($f^2 = 0.131$), Perceived Behavioural Control ($f^2 = 0.035$) and Subjective Norms ($f^2 = 0.029$).

This study is one of the first investigations into unauthorised access to health data from the perspective of information security culture among nursing staff. As such, it has several important theoretical implications.

The research defines and operationalises two new dimensions of information security culture – Security Oriented and Privacy Oriented. Both are supported by EFA and CCA and have passed the validity and reliability tests, as have the other seven dimensions. Moreover, the results indicate that these dimensions play different roles in shaping Attitudes Towards Behaviour and perceptions of social norms related to unauthorised data access. The questionnaire provides a valid and reliable means of measuring theoretical constructs and this is one of the first studies to include both Subjective Norms and Normative Beliefs in the same research model. The results show that although similar in explaining behaviour, Subjective Norms and Normative Beliefs are distinct constructs,

which has also been confirmed by CCA, with both having passed the validity and reliability tests.

The lowest median values were observed for the Security Monitoring and Information Security Knowledge Sharing dimensions, while the highest value was observed for the Privacy Oriented dimension. This result argues in favour of introducing a new dimension of Privacy Oriented into the existing model developed by Nasir, et al. (2019). The results indicate a strong perception and agreement on the Privacy Oriented dimension for nursing. It is a dimension that refers to the commitment to professional confidentiality, commitment to and protection of patients' privacy, the defence of patients' rights to privacy and the rule: "Don't do unto others what you don't want done onto you" regarding patient privacy, which has an ethical component. As nursing is a practice underpinned by ethics and ethical decision-making, the ethical conduct of nurses in relation to data security is of paramount importance for respecting the ideals and ethical norms of the profession. This is a specific requirement in nursing. It is therefore not surprising that the profession-specific dimension of information security culture associated with the field of ethics in nursing was found to have the highest median score.

The lowest median score was observed for the dimension of information security culture Information Security Knowledge Sharing. These results indicate that the sharing of information security knowledge among healthcare professionals is either not viewed as important, or it has diminished or is non-existent. It can be assumed that nurses do not perceive the transfer of information security knowledge and skills as a priority to be included in ongoing training and education, or as a key element in the knowledge sharing process. These results are surprising, given that nursing staff represent a population that perceives continuous training, education as crucial to their professional and career development.

In addition to the Information Security Knowledge Sharing dimension, the lowest median was observed for the Security Monitoring dimension, indicating that employees are either unaware of tend to ignore the consequences of privacy breaches in patient health data. At the same time, statistically significant differences in mean values between men and

women were identified for the Security Monitoring dimension. The mean value was higher for women. These results indicate a positive but weak correlation between nurses' age, years of service and perceptions regarding the Risk Management dimension. They also suggest that the years of work experience of employees can reduce the risk of data breaches. Employees who have worked for an organisation for many years have a better understanding of information security policy. We found no statistically significant differences in the mean values of the ranks of the dimensions of information security culture depending on the level of education or the type of healthcare organisations. Due to the organisational structures between the levels of healthcare and social care institutions and the size of the organisations and educational programmes, we expected different perceptions of the dimensions of information security culture. This raises the following questions: a) are the existing educational programs sufficient to equip future nursing staff with the knowledge on how to handle health data, and b) can the results obtained be attributed to the difficulties in applying the acquired knowledge in nursing practice? The results of the survey therefore provide a starting point for upgrading training programmes that can enrich the nursing profession with additional practical skills essential for the use of modern information and communication technologies.

This study has several practical implications that can assist healthcare professionals and policymakers in managing unauthorised access to health data by nursing staff or other healthcare workers. It can also help in the development and design of training programmes. Awareness raising is an important tool to ensure the application of appropriate ethical norms, such as privacy in nursing practice.

The results of the study can help determine the direction in which awareness-raising interventions should be implemented. Essentially, awareness-raising interventions can aim to strengthen the social influence on nursing staff, their attitudes, or both. Nurses' attitudes can be strengthened through awareness-raising programmes focussing on their personal beliefs and professional ethics. Professional ethics play a critical role in this population, which is why emphasising the unethical aspects of dangerous behaviour can be relatively effective for this population. As nurses are often faced with ethical dilemmas, it would be useful to incorporate discussions about the most common ethical

dilemmas into awareness-raising programmes. This could contribute to a better understanding and handling of situations in which such dilemmas arise and shape acceptable behaviour. Imparting knowledge about how to behave in ethically difficult situations could enrich nursing employees. Organisations could begin to monitor levels of social influence and/or staff attitudes so as to determine which awareness-raising interventions are required at a given time. With this approach, organisations could better manage their efforts to improve the ethical behaviour of their staff.

Limitations of the study include the use of a cross-sectional design and a survey for assessing behavioural intentions, coverage error, generalisation of results to the target population and self-reporting. Despite these limitations, the study determined the extent, quantity and characteristics of occurrence and identified associated factors that suggest the implementation of improvement measures in nursing staff behaviour and work process. This can lead to a decrease in the incidence of information security breaches. We identified the main levers related to information security culture that healthcare and social welfare organisations can use to reduce the risk of confidentiality breaches by healthcare employees. In doing so, we have formulated recommendations for organisations on how they can improve in this area.

9 LITERATURA

Agaku, I.T., Adisa, A.O., Ayo-Yusuf, O.A. & Connolly, G.N., 2013. Concern about security and privacy, and perceived control over collection and use of health information are related to withholding of health information from healthcare providers. *Journal of the American Medical Informatics Association*, 21(2), pp. 374-378. 10.1136/amiajnl-2013-002079.

Aigbefo, Q.A., Blount, Y. & Marrone, M., 2022. The influence of hardiness and habit on security behaviour intention. *Behaviour & Information Technology*, 41(6), pp. 1151-1170. 10.1080/0144929X.2020.1856928.

Ajzen, I., 1991. The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, 50(2), pp. 179-211.

Ajzen, I., 2002. Perceived behavioral control, self-efficacy, locus of control, and the theory of planned behavior 1. *Journal of Applied Social Psychology*, 32(4), pp. 665-683. 10.1111/j.1559-1816.2002.tb00236.x.

Ajzen, I., 2005. *Attitudes, personality and behaviour*. 2nd ed. Maidenhead: Open University.

Alanazi, M., Freeman, M. & Tootell, H., 2022. Exploring the factors that influence the cybersecurity behaviors of young adults. *Computers in Human Behavior*, 136, p. 107376. 10.1016/j.chb.2022.107376.

AlHogail, A. & Mirza, A., 2014a. Information security culture: A definition and a literature review. In: *Proceedings of the 2014 World Congress on Computer Applications and Information Systems (WCCAIS). Hammamet, Tunisia, 17-19 January.* Piscataway: Institute of Electrical and Electronics Engineers, pp. 1-7. 10.1109/WCCAIS.2014.6916579.

Alhogail, A. & Mirza, A., 2014b. A Framework of information security culture change. *Journal of Theoretical & Applied Information Technology,* 64(2), pp. 540-549.

AlHogail, A., 2015a. Cultivating and assessing an organizational information security culture; an empirical study. *International Journal of Security and Its Applications,* 9(7), pp. 163-178. 10.14257/ijsia.2015.9.7.15.

AlHogail, A., 2015b. Design and validation of information security culture framework. *Computers in Human Behavior,* 49, pp. 567-575. 10.1016/j.chb.2015.03.054.

Alnatheer, M.A. & Nelson, K., 2009. Proposed framework for understanding information security culture and practices in the Saudi context. In: C. Bolan, ed. P*roceedings of the 7th Australian Information Security Management Conference, Perth, Western Australia, 1-3 December 2009.* Australia: Security Research Centre, School of Computer and Security Science, Edith Cowan University, pp. 6-17. 10.4225/75/579850d331b4d.

Alnatheer, M.A., Chan, T. & Nelson, K., 2012. Understanding and measuring information security culture. In: S.L. Pan & T.H. Cao, eds. *Proceedings of the 16th Pacific Asia Conference on Information Systems (PACIS). Vietnam, July.* Vietnam: University of Science, AIS Electronic Library (AISeL), pp. 144-159.

Alnatheer, M.A., 2014. A Conceptual Model to Understand Information Security Culture. *International Journal of Social Science and Humanity,* 4(2), pp. 104-107. 10.7763/IJSSH.2014.V4.327.

Alnatheer, M.A., 2015. Information Security Culture Critical Success Factors. In: S. Latifi, ed. *Proceedings of the 12th International Conference on Information Technology - New Generations*. *Las Vegas, Nevada, 13-15 April.* Piscataway: Institute of Electrical and Electronics Engineers, pp. 731-735. 10.1109/ITNG.2015.124.

Alshaikh, M., 2020. Developing cybersecurity culture to influence employee behavior: A practice perspective. *Computers & Security,* 98(2), pp. 102003-102013. 10.1016/j.cose.2020.102003.

Alsharida, R.A., Al-rimy, B.A.S., Al-Emran, M. & Zainal, A., 2023. A systematic review of multi perspectives on human cybersecurity behavior. *Technology in Society*, 73, p. 102258. 10.1016/j.techsoc.2023.102258.

Amankwa, E., Loock, M. & Kritzinger, E., 2018. Establishing information security policy compliance culture in organizations. *Information & Computer Security*, 26(4), pp. 420-436. 10.1108/ICS-09-2017-0063.

Anderson, C.L. & Agarwal, R., 2010. Practicing safe computing: A multimethod empirical examination of home computer user security behavioral intentions. *MIS Quarterly*, 34(3), pp. 613-643. 10.2307/25750694.

Angst, C.M. & Agarwal, R., 2009. Adoption of electronic health records in the presence of privacy concerns: The elaboration likelihood model and individual persuasion. *MIS Quarterly*, 33(2), pp. 339-370. 10.2307/20650295.

Appari, A. & Johnson, M.E., 2010. Information security and privacy in healthcare: Current state of research. *International Journal of Internet and Enterprise Management*, 6(4), pp. 279-314. 10.1504/IJIEM.2010.035624.

Asgari, S., Shafipour, V., Taraghi, Z. & Yazdani-Charati, J., 2019. Relationship between moral distress and ethical climate with job satisfaction in nurses. *Nursing Ethics*, 26(2), pp. 346-356. 10.1177/0969733017712083.

Astakhova, L., 2014. The concept of the information-security culture. *Scientific and Technical Information Processing*, 41(1), pp. 22-28. 10.3103/S0147688214010067.

Bada, M., Von Solms, B. & Agrafiotis, I., 2019. Reviewing national cybersecurity awareness in Africa: An empirical study. In: S. Chan, T. Klemans, X. Liu, K. Joiner & M. Massoth, eds. *The Third International Conference on Cyber-Technologies and Cyber-Systems, CYBER, Athens, Greece, 18-22 November, 2018.* s.l.: University of Cambridge

Repository. International Academy, Research, and Industry Association (IARIA), pp. 78-83.

Bagozzi, R.P. & Yi, Y., 1988. On the evaluation of structural equation models. *Journal of the Academy of Marketing Science*, 16(1), pp. 74-94. 10.1007/BF02723327.

Baillie, L., 2009. Patient dignity in an acute hospital setting: A case study. *International Journal of Nursing Studies*, 46(1), pp. 23-37. 10.1016/j.ijnurstu.2008.08.003.

Bakry, S.H., 2004. Development of e-government: A STOPE view. *International Journal of Network Management*, 14(5), pp. 339-350. 10.1002/nem.529.

Becker, J.M., Ringle, C.M., Sarstedt, M. & Völckner, F., 2015. How collinearity affects mixture regression results. *Marketing Letters*, 26(4), pp. 643-659. 10.1007/s11002-014-9299-9.

Ben-Asher, N. & Gonzalez, C., 2015. Effects of cyber security knowledge on attack detection. *Computers in Human Behavior*, 48(1), pp. 51-61. 10.1016/j.chb.2015.01.039.

Bidabadi, F.S., Yazdannik, A. & Zargham-Boroujeni, A., 2019. Patient's dignity in intensive care unit: A critical ethnography. *Nursing Ethics*, 26(3), pp. 738-752. 10.1177/0969733017720826.

Blanken-Webb, J., 2020. Cybersecurity and the Ethics of Care. *Information Security Education Journal*, 7(2), pp. 31-39. 10.6025/isej/2020/7/2/31-39.

Blythe, J.M., Gray, A. & Collins, E., 2020. Human Cyber Risk Management by Security Awareness Professionals: Carrots or Sticks to Drive Behaviour Change? In: A. Moallem, ed. *HCI for Cybersecurity, Privacy and Trust. HCII 2020. Lecture Notes in Computer Science, Copenhagen, Denmark, 19-24 July*. Switzerland: Springer, pp. 76-91. 10.1007/978-3-030-50309-3_6.

Boss, S.R., Galletta, D.F., Lowry, P.B., Moody, G.D. & Polak, P., 2015. What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. *MIS Quarterly*, 39(4), pp. 837-864.

Box, D. & Pottas, D., 2013. Improving Information Security Behaviour in the Healthcare Context. *Procedia Technology*, 9, pp. 1093-1103. 10.1016/j.protcy.2013.12.122.

Božić, F., 2016. *Človeški dejavnik pri zagotavljanju informacijske varnosti*: *magistrsko delo.* Univerza v Ljubljani, Fakulteta za računalništvo in informatiko.

Brady, J.W., 2010. *An Investigation of Factors that Affect HIPAA Security Compliance in Academic Medical Centers*: *doktorska disertacija.* United States: Nova Southeastern University, Graduate School of Computer and Information Sciences.

Brown, T.A., 2015. *Confirmatory factor analysis for applied research*. 2nd ed. New York: Guilford press.

Bruursema, K., 2007. *How individual values and trait boredom interface with job characteristics and job boredom in their effects on counterproductive work behavior: doktorska disertacija*. United States: University of South Florida, College of Arts and Sciences.

Bryan Foltz, C., Schwager, P.H. & Anderson, J.E., 2008. Why users (fail to) read computer usage policies. *Industrial Management & Data Systems*, 108(6), pp. 701-712. 10.1108/02635570810883969.

Bulgurcu, B., Cavusoglu, H. & Benbasat, I., 2010. Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, 34(3), pp. 523-548. 10.2307/25750690.

Butavicius, M., Parsons, K., Lillie, M., Mc Cormac, A., Pattinson, M. & Calic, D., 2020. When believing in technology leads to poor cyber security: Development of a trust in

technical controls scale. *Computers & Security*, 98, pp. 102020-102031. 10.1016/j.cose.2020.102020.

Cagliano, A.C., Grimaldi, S. & Rafele, C., 2011. A systemic methodology for risk management in healthcare sector. *Safety Science*, 49(5), pp. 695-708. 10.1016/j.ssci.2011.01.006.

Cai, Z., Fan, X. & Du, J., 2017. Gender and attitudes toward technology use: A meta-analysis. *Computers & Education*, 105, pp. 1-13. 10.1016/j.compedu.2016.11.003.

Cameron, K.S. & Quinn, R.E, 2011. *Diagnosing and changing organizational culture: Based on the competing values framework.* 3rd. ed. San FranciscoJohn: Jossey-Bass, pp. 30-31.

Cannoy, S.D. & Salam, A.F. 2010. A framework for health care information assurance policy and compliance. *Communications of the ACM*, 53(3), pp. 126-131. 10.1145/1666420.1666453.

Chan, M., Woon, I. & Kankanhalli, A., 2005. Perceptions of Information Security in the Workplace: Linking Information Security Climate to Compliant Behavior. *Journal of Information Privacy and Security*, 1(3), pp. 18-41. 10.1080/15536548.2005.10855772.

Chang, E.S. & Lin, C., 2007. Exploring organizational culture for information security management. *Industrial Management & Data Systems*, 107(3), pp. 438-458. 10.1108/02635570710734316.

Chao, S.Y., Chang, Y.C., Yang, S.C. & Clark, M.J., 2017. Development, implementation, and effects of an integrated web-based teaching model in a nursing ethics course. *Nurse Education Today*, 55, pp. 31-37. 10.1016/j.nedt.2017.04.011.

Chau, P.Y. & Hu, P.J.H., 2001. Information technology acceptance by individual professionals: A model comparison approach. *Decision Sciences*, 32(4), pp. 699-719. 10.1111/j.1540-5915.2001.tb00978.x.

Chau, P.Y. & Hu, P.J.H., 2002. Investigating healthcare professionals' decisions to accept telemedicine technology: An empirical test of competing theories. *Information & Management*, 39(4), pp. 297-311. 10.1016/S0378-7206(01)00098-2.

Chen, H., Chau, P.Y. & Li, W., 2018. The effects of moral disengagement and organizational ethical climate on insiders' information security policy violation behavior. *Information Technology & People*, 32(4), pp. 973-992. 10.1108/ITP-12-2017-0421.

Chen, Y., Ramamurthy, K.R. & Wen, K.W., 2015. Impacts of Comprehensive Information Security Programs on Information Security Culture. *Journal of Computer Information Systems*, 55(3), pp. 11-19. 10.1080/08874417.2015.11645767.

Chen, Y., Ramamurthy, K.R. & Wen, K.W., 2012. Organizations' information security policy compliance: Stick or carrot approach? *Journal of Management Information Systems*, 29(3), pp. 157-188. 10.2753/MIS0742-1222290305.

Chen, Y. & Zahedi, F.M., 2016. Individuals' Internet Security Perceptions and Behaviors. *Mis Quarterly*, 40(1), pp. 205-222.

Chernyshev, M., Zeadally, S. & Baig, Z., 2018. Healthcare Data Breaches: Implications for Digital Forensic Readiness. *Journal of Medical Systems*, 43(1), p. 7. 10.1007/s10916-018-1123-2.

Chi, M.T., 2006. Two approaches to the study of experts' characteristics. In: K.A. Ericsson, N. Charness, P.J. Feltovich & R.R. Hoffman, eds. *The Cambridge Handbook of Expertise and Expert Performance*. Cambridge: Cambridge University Press, pp. 21-30.

Chin, W.W., 1998. The partial least squares approach to structural equation modeling. In: G.A. Marcoulides, ed. *Modern Methods for Business Research*. New York: Psychology Press, Taylor & Francis group, pp. 295-336.

Chin, W.W., Marcolin, B.L. & Newsted, P.R., 2003. A partial least squares latent variable modeling approach for measuring interaction effects: Results from a Monte Carlo simulation study and an electronic-mail emotion/adoption study. *Information Systems Research*, 14(2), pp. 189-217. 10.1287/isre.14.2.189.16018.

Chin, W.W., 2010. How to write up and report PLS analyses. In: V.V. Esposito, W.W. Chin, J. Henseler & H. Wang, eds. *Handbook of partial least squares: Concepts, Methods and Applications.* Heidelberg, Berlin: Springer, pp. 655-690.

Chin, W.W., Thatcher, J.B., Wright, R.T. & Steel, D., 2013. Controlling for common method variance in PLS analysis: The measured latent marker variable approach. In: H. Abdi, W. Chin, V. Esposito Vinzi, G. Russolillo & L. Trinchera, eds. *New perspectives in partial least squares and related methods. Springer Proceedings in Mathematics & Statistics.* New York: Springer, pp. 231-239. 10.1007/978-1-4614-8283-3_16.

Cohen, J., 1988. *Statistical power analysis for the behavioral sciences*. 2nd ed. New York: Routledge.

Cram, W.A., D'arcy, J. & Proudfoot, J.G., 2019. Seeing the forest and the trees: A meta-analysis of the antecedents to information security policy compliance. *MIS Quarterly*, 43(2), pp. 525-554. 10.25300/MISQ/2019/15117.

Da Veiga, A., Martins, N. & Eloff, J.H., 2007. Information security culture-validation of an assessment instrument. *Southern African Business Review*, 11(1), pp. 147-166.

Da Veiga, A., 2008. *Cultivating and assessing information security culture: doktorska disertacija.* South Africa: University of Pretoria, Faculty of Engineering, Built Environment and Information Technology.

Da Veiga, A. & Eloff, J.H., 2010. A framework and assessment instrument for information security culture. *Computers & Security*, 29(2), pp. 196-207. 10.1016/j.cose.2009.09.002.

Da Veiga, A. & Martins, N., 2015. Information security culture and information protection culture: A validated assessment instrument. *Computer Law & Security Review*, 31(2), pp. 243-256. 10.1016/j.clsr.2015.01.005.

Da Veiga, A., 2016. A cybersecurity culture research philosophy and approach to develop a valid and reliable measuring instrument. In: *Proceedings of 2016 Science and Information Conference (SAI). London, UK, 13-15 July*. Piscataway: Institute of Electrical and Electronics Engineers, pp. 1006-1015. 10.1109/SAI.2016.7556102.

Da Veiga, A. & Martins, N., 2017. Defining and identifying dominant information security cultures and subcultures. *Computers & Security*, 70, pp. 72-94. 10.1016/j.cose.2017.05.002.

Da Veiga, A., 2018. An approach to information security culture change combining ADKAR and the ISCA questionnaire to aid transition to the desired culture. *Information & Computer Security*, 26(5), pp. 584-612. 10.1108/ICS-08-2017-0056.

Da Veiga, A., Astakhova, L.V., Botha, A. & Herselman, M., 2020. Defining organisational information security culture—Perspectives from academia and industry. *Computers & Security*, 92, pp. 101713-101736. 10.1016/j.cose.2020.101713.

Danks, N.P. & Ray, S., 2018. Predictions from partial least squares models. In: F. Ali, S.M. Rasoolimanesh & C. Cobanoglu, eds. *Applying partial least squares in tourism and hospitality research*. Bingley, UK: Emerald Publishing Limited, pp. 35-52. 10.1108/978-1-78756-699-620181003.

D'Arcy, J., Hovav, A. & Galletta, D., 2009. User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach. *Information Systems Research,* 20(1), pp. 79-98. 10.1287/isre.1070.0160.

D'arcy, J. & Herath, T., 2011. A review and analysis of deterrence theory in the IS security literature: Making sense of the disparate findings. *European Journal of Information Systems,* 20(6), pp. 643-658. 10.1057/ejis.2011.23.

D'Arcy, J. & Greene, G., 2014. Security culture and the employment relationship as drivers of employees' security compliance. *Information Management & Computer Security*, 22(5), pp. 474-489. 10.1108/IMCS-08-2013-0057.

Dash, G. & Paul, J., 2021. CB-SEM vs PLS-SEM methods for research in social sciences and technology forecasting. *Technological Forecasting and Social Change*, 173, pp. 121092-121103. 10.1016/j.techfore.2021.121092.

de Araújo Lima, P.F., Crema, M. & Verbano, C., 2020. Risk management in SMEs: A systematic literature review and future directions. *European Management Journal*, 38(1), pp. 78-94. 10.1016/j.emj.2019.06.005.

de Lusignan, S., Chan, T., Theadom, A. & Dhoul, N., 2007. The roles of policy and professionalism in the protection of processed clinical data: A literature review. *International Journal of Medical Informatics*, 76(4), pp. 261-268. 10.1016/j.ijmedinf.2005.11.00310.1016/j.ijmedinf.2005.11.003.

Degirmenci, K., Guhr, N. & Breitner, M., 2013. Mobile applications and access to personal information: A discussion of users' privacy concerns. In: M. Chau & R. Baskerville, eds. *Proceedings of the 34th International Conference on Information Systems (ICIS 2013). Milano, Italy: 15-18. December*. s.l.: Association for Information Systems (AIS), pp. 1-21.

Department for Business, Energy and Industrial Strategy (BEIS), 2020. *Business population estimates for the UK and regions: 2019 statistical release*. [pdf] BEIS. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/852919/Business_Population_Estimates_for_the_UK_and_regions_-_2019_Statistical_Release.pdf [Accessed 15 January 2023].

Diamantopoulos, A., Sarstedt, M., Fuchs, C., Wilczynski, P. & Kaiser, S., 2012. Guidelines for choosing between multi-item and single-item scales for construct measurement: A predictive validity perspective. *Journal of the Academy of Marketing Science*, 40(3), pp. 434-449. 10.1007/s11747-011-0300-3.

Dijkstra, T.K., 2010. Latent variables and indices: Herman Wold's basic design and partial least squares. In: V. Esposito Vinzi, W. Chin, J. Henseler & H. Wang, eds. *Handbook of partial least squares: Concepts, Methods and Applications.* Heidelberg, Berlin: Springer, pp. 23-46.

Dijkstra, T.K., 2014. PLS'Janus face-response to professor Rigdon's 'rethinking partial least squares modeling: In praise of simple methods'. *Long Range Planning*, 47(3), pp. 146-153. 10.1016/j.lrp.2014.02.004.

Dijkstra, T.K. & Schermelleh-Engel, K., 2014. Consistent partial least squares for nonlinear structural equation models. *Psychometrika*, 79(4), pp. 585-604. 10.1007/s11336-013-9370-0.

Dijkstra, T.K. & Henseler, J., 2015. Consistent partial least squares path modeling. *MIS Quarterly*, 39(2), pp. 297-316.

Dinev, T. & Hu, Q., 2007. The centrality of awareness in the formation of user behavioral intention toward protective information technologies. *Journal of the Association for Information Systems*, 8(7), pp. 386-408.

Dziak, J.J., Dierker, L.C. & Abar, B., 2020. The interpretation of statistical power after the data have been gathered. *Current Psychology*, 39(3), pp. 870-877. 10.1007/s12144-018-0018-1.

Dolce, P., Esposito Vinzi, V. & Lauro, C., 2017. Predictive path modeling through PLS and other component-based approaches: Methodological issues and performance evaluation. In: H. Latan & R. Noonan, eds. *Handbook of Partial Least Squares Path Modeling: Concepts, Methods and Applications*. Cham: Springer, pp. 153-172. 10.1007/978-3-319-64069-3_7.

Dolezel, D. & McLeod, A., 2019. Cyber-Analytics: Identifying Discriminants of Data Breaches. *Perspectives in Health Information Management*, 16, pp. 1-16.

Dollah, W. & Ali, J., 2012. Determining factors influencing information security culture among ICT librarians. *Journal of Theoretical and Applied Information Technology*, 37(1), pp. 132-140.

Dolnicar, S., Coltman, T. & Sharma, R., 2015. Do satisfied tourists really intend to come back? Three concerns with empirical studies of the link between satisfaction and behavioral intention. *Journal of Travel Research*, 54(2), pp. 152-178. 10.1177/00472875135131.

Dolnicar, S., 2020. Why quantitative papers based on primary data get desk-rejected by Annals of Tourism Research. *Annals of Tourism Research*, 83, 102981. 10.1016/j.annals.2020.102981.

Donaldson, M.S., Corrigan, J.M. & Kohn, L. T., 2000. *To err is human: Building a safer health system*. Washington: National Academies Press.

Dong, K., Ali, R.F., Dominic, P. & Ali, S.E.A., 2021. The effect of organizational information security climate on information security policy compliance: The mediating

effect of social bonding towards healthcare nurses. *Sustainability*, 13(5), pp. 2800-2825. 10.3390/su13052800.

Dunning, D., Heath, C. & Suls, J.M., 2004. Flawed self-assessment: Implications for health, education, and the workplace. *Psychological Science in the Public Interest*, 5(3), 69-106. 10.1111/j.1529-1006.2004.00018.x.

Eckert, T., Dunn, E., Codding, R. & Guiney, K., 2000. Self-report: Rating scale measures. In: E.S. Shapiro & T.R. Kratochwill, eds. *Conducting School-Based Assessments of Child and Adolescent Behavior*. New York, London: Guilford Press, pp. 150-169.

Egea, J.M.O. & González, M.V.R., 2011. Explaining physicians' acceptance of EHCR systems: An extension of TAM with trust and risk factors. *Computers in Human Behavior*, 27(1), pp. 319-332. 10.1016/j.chb.2010.08.010.

Farzandipour, M., Sadoughi, F., Ahmadi, M. & Karimi, I., 2010. Security requirements and solutions in electronic health records: Lessons learned from a comparative study. *Journal of Medical Systems*, 34(4), pp. 629-642. 10.1007/s10916-009-9276-7.

Ferguson, G.W., 2016. *Ambulatory surgery centers: A case study of breach deterrence of healthcare information*: *doktorska disertacija.* United States: Capella University.

Fertig, T., Schütz, A.E. & Weber, K., 2020. *Current Issues Of Metrics For Information Security Awareness.* In: F. Rowe, R. El Amrani, M. Limayem, S. Newell, N. Pouloudi, E. van Heck & A. El Quammah, eds. *Proceedings of 28th European Conference on Information Systems - Liberty, Equality, and Fraternity in a Digitizing World, ECIS 2020, Marrakech, Morocco, June 15-17, 2020.* s.l.: AIS Electronic Library.

Fishbein, M. & Ajzen, I., 1975. *Belief, attitude, intention, and behavior: An introduction to theory and research*. Philippines: Addison-Wesley, p. 16.

Fishbein, M. & Ajzen, I., 2011. *Predicting and changing behavior: The reasoned action approach*. New York: Psychology press, pp. 22, 130, 225, 233-237, 241.

Flores, W.R., Antonsen, E. & Ekstedt, M., 2014. Information security knowledge sharing in organizations: Investigating the effect of behavioral information security governance and national culture. *Computers & Security*, 43, pp. 90-110. 10.1016/j.cose.2014.03.004.

Fornell, C. & Larcker, D.F., 1981. Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research*, 18(1), pp. 39-50. 10.1177/002224378101800104.

Francis, J., Eccles, M.P., Johnston, M., Walker, A., Grimshaw, J.M., Foy, R., Kaner, E.F., Smith, L. & Bonetti, D., 2004. *Constructing questionnaires based on the theory of planned behaviour: A manual for health services researchers*. UK: Centre for Health Service Research, University of Newcastle upon Tyne.

Friese, S., 2013. *ATLAS. ti 7: User guide and reference.* Berlin: ATLAS. Ti Scientific Software Development GmbH.

Fuller, C.M., Simmering, M.J., Atinc, G., Atinc, Y. & Babin, B.J., 2016. Common methods variance detection in business research. *Journal of business research*, 69(8), pp. 3192-3198. 10.1016/j.jbusres.2015.12.008.

G Maçada, A.C. & Luciano, E.M., 2010. The influence of human factors on vulnerability to information security breaches. In: *Proceedings of 16th Americas Conference on Information Systems (AMCIS), Lima, Peru, 12-15 Avgust.* s.l.: Association for Information Systems (AIS) AIS Electronic Library (AISeL), p. 531.

Garbarino, E. & Strahilevitz, M., 2004. Gender differences in the perceived risk of buying online and the effects of receiving a site recommendation. *Journal of Business Research*, 57(7), pp. 768-775. 10.1016/S0148-2963(02)00363-6.

Gartrell, K., 2014. *Factors Associated with Electronic Personal Health Record Use among Registered Nurses for Their Own Health Management*: *doktorska disertacija.* United States: University of Maryland.

Gatersleben, B., Murtagh, N. & Abrahamse, W., 2014. Values, identity and pro-environmental behaviour. *Contemporary Social Science,* 9(4), pp. 374-392. 10.1080/21582041.2012.682086.

Gaunt, N., 2000. Practical approaches to creating a security culture. *International Journal of Medical Informatics,* 60(2), pp. 151-157. 10.1016/S1386-5056(00)00115-5.

Gebrasilase, T. & Lessa, L.F., 2011. Information Security Culture in Public Hospitals: The Case of Hawassa Referral Hospital. *The African Journal of Information Systems,* 3(3), pp. 72-86.

Gefen, D., Straub, D. & Boudreau, M.C., 2000. Structural equation modeling and regression: Guidelines for research practice. *Communications of the Association for Information Systems*, 4(1), pp. 1-7. 10.17705/1CAIS.00407.

Geisser, S., 1974. A predictive approach to the random effect model. *Biometrika,* 61(1), pp. 101-107. 10.1093/biomet/61.1.101.

Ghafir, I., Saleem, J., Hammoudeh, M., Faour, H., Prenosil, V., Jaf, S., Jabbar, S. & Baker, T., 2018. Security threats to critical infrastructure: The human factor. *The Journal of Supercomputing*, 74(10), pp. 4986-5002. 10.1007/s11227-018-2337-2.

Glegg, S.M., Holsti, L., Velikonja, D., Ansley, B., Brum, C. & Sartor, D., 2013. Factors influencing therapists' adoption of virtual reality for brain injury rehabilitation. *Cyberpsychology, Behavior, and Social Networking*, 16(5), pp. 385-401. 10.1089/cyber.2013.1506.

Gong, M., Wang, S., Wang, L., Liu, C., Wang, J., Guo, Q., Zheng, H., Xie, K., Wang, C. & Hui, Z., 2020. Evaluation of Privacy Risks of Patients' Data in China: Case Study. *JMIR Medical Informatics*, 8(2), p. e13046.10.2196/13046.

Goodall, J.R., Lutters, W.G. & Komlodi, A., 2009. Developing expertise for network intrusion detection. *Information Technology & People*, 22(2), pp. 92-108. 10.1108/09593840910962186.

Goodhue, D.L., Lewis, W. & Thompson, R., 2012. Does PLS have advantages for small sample size or non-normal data? *MIS Quarterly*, 36(3), pp. 981-1001. 10.2307/41703490.

Govender, S.G., Kritzinger, E. & Loock, M., 2020. A Framework for the Assessment of Information Security Risk, the Reduction of Information Security Cost and the Sustainability of Information Security Culture. In: R. Silhavy, ed. *Applied Informatics and Cybernetics in Intelligent Systems*. Cham: Springer, pp. 69-84. 10.1007/978-3-030-51974-2_7.

Gratian, M., Bandi, S., Cukier, M., Dykstra, J. & Ginther, A., 2018. Correlating human traits and cyber security behavior intentions. *Computers & Security*, 73, pp. 345-358. 10.1016/j.cose.2017.11.015.

Greene, G. & D'Arcy, J., 2010. Assessing the impact of security culture and the employee-organization relationship on IS security compliance. In: S. Goel, ed. *Proceedings of the 5th Annual Symposium on Information Assurance Academic track of the 13th Annual 2009 NYS Cyber Security Conference, New York, USA, 16-17 June.* s.l., s.n., pp. 42-50.

Greig, A., Renaud, K. & Flowerday, S., 2015. An ethnographic study to assess the enactment of information security culture in a retail store. *In Proceedings of 2015 World Congress on Internet Security (WorldCIS). Dublin, Ireland, 19-21 Octobre.* Hoes Lane, Piscataway: Institute of Electrical and Electronics Engineers, pp. 61-66. 10.1109/WorldCIS.2015.7359415.

Griffin-Heslin, V.L., 2005. An analysis of the concept dignity. *Accident and Emergency Nursing*, 13(4), pp. 251-257. 10.1016/j.aaen.2005.09.003.

Gwebu, K.L., Wang, J. & Hu, M.Y. 2020. Information security policy noncompliance: An integrative social influence model. *Information Systems Journal*, 30(2), pp. 220-269. 10.1111/isj.12257.

Hahn, J., Galuska, L., Polifroni, E.C. & Dunnack, H., 2021. Joy and Meaning in Nurse Manager Practice. *The Journal of Nursing Administration*, 51(1), pp. 38-42. 10.1097/NNA.0000000000000964.

Hai, N.K., Lawpoolsri, S., Jittamala, P., Huong, P.T.T. & Kaewkungwal, J., 2017. Practices in security and confidentiality of HIV/AIDS patients' information: A national survey among staff at HIV outpatient clinics in Vietnam. *PloS One*, 12(11), p. e0188160. 10.1371/journal.pone.0188160.

Hair, J.F., Ringle, C.M. & Sarstedt, M., 2011. PLS-SEM: Indeed a silver bullet. *Journal of Marketing Theory and Practice*, 19(2), pp. 139-152. 10.2753/MTP1069-6679190202.

Hair, J.F., Sarstedt, M., Ringle, C.M. & Mena, J.A., 2012. An assessment of the use of partial least squares structural equation modeling in marketing research. *Journal of the Academy of Marketing Science*, 40(3), pp. 414-433. 10.1007/s11747-011-0261-6.

Hair, J.F., Ringle, C.M. & Sarstedt, M., 2013. Partial least squares structural equation modeling: Rigorous applications, better results and higher acceptance. *Long Range Planning*, 46(1-2), pp. 1-12.

Hair, J.F., Hult, G.T.M., Ringle, C.M., Sarstedt, M. & Thiele, K.O., 2017. Mirror, mirror on the wall: A comparative evaluation of composite-based structural equation modeling methods. *Journal of the Academy of Marketing Science*, 45(5), pp. 616-632. 10.1007/s11747-017-0517-x.

Hair, J.F., Risher, J.J., Sarstedt, M. & Ringle, C.M., 2019a. When to use and how to report the results of PLS-SEM. *European Business Review*, 31(1), pp. 2-24. 10.1108/EBR-11-2018-0203.

Hair, J.F., Sarstedt, M. & Ringle, C.M., 2019b. Rethinking some of the rethinking of partial least squares. *European Journal of Marketing*, 53(4), pp. 566-584. 10.1108/EJM-10-2018-0665.

Hair, J.F., Howard, M.C. & Nitzl, C., 2020. Assessing measurement model quality in PLS-SEM using confirmatory composite analysis. *Journal of Business Research*, 109, pp. 101-110. 10.1016/j.jbusres.2019.11.069.

Hair, J.F., Hult, G.T.M., Ringle, C.M., Sarstedt, M., Danks, N.P. & Ray, S., 2021. *Partial Least Squares Structural Equation Modeling (PLS-SEM) Using R: A Workbook*. Switzerland: Springer Nature. 10.1007/978-3-030-80519-7.

Hansson, S.O. & Fröding, B., 2021. Ethical conflicts in patient-centred care. *Clinical Ethics*, 16(2), pp. 55-66. 10.1177/1477750920962356.

Harris, S.G., 1994. Organizational culture and individual sensemaking: A schema-based perspective. *Organization Science*, 5(3), pp. 309-321. 10.1287/orsc.5.3.309.

Hassan, N.H. & Ismail, Z., 2012. A conceptual model for investigating factors influencing information security culture in healthcare environment. *Procedia-Social and Behavioral Sciences*, 65, pp. 1007-1012. 10.1016/j.sbspro.2012.11.234.

Hassan, N.H., Maarop, N., Ismail, Z. & Abidin, W.Z., 2017. Information security culture in health informatics environment: A qualitative approach. *2017 International Conference on Research and Innovation in Information Systems (ICRIIS)*. *Langkawi, Malaysia, 16-17 July*. Hoes Lane, Piscataway: Institute of Electrical and Electronics Engineers, pp. 1-6. 10.1109/ICRIIS.2017.8002450.

Hayden, L., 2016. *People-Centric Security: Transforming Your Enterprise Security Culture*. New York: McGraw-Hill Education.

Hays, R.D., Hayashi, T. & Stewart, A.L., 1989. A five-item measure of socially desirable response set. *Educational and Psychological Measurement*, 49(3), pp. 629-636. 10.1177/001316448904900315.

He, Y. & Johnson, C., 2017. Challenges of information security incident learning: An industrial case study in a Chinese healthcare organization. *Informatics for Health and Social Care*, 42(4), pp. 393-408. 10.1080/17538157.2016.1255629.

Hedström, K., Dhillon, G. & Karlsson, F., 2010. Using Actor Network Theory to Understand Information Security Management. In K. Rannenberg, V. Varadharajan, & C. Weber, eds. *Security and Privacy - Silver Linings in the Cloud*: *Proceedings of 25th IFIP TC 11 International Information Security Conference, SEC 2010, Held as Part of WCC 2010, Brisbane, Australia, 20-23 September, 2010.* Berlin Heidelberg: Springer, pp, 43-54. 10.1007/978-3-642-15257-3_5.

Hedström, K., Karlsson, F. & Kolkowska, E., 2013. Social action theory for understanding information security non-compliance in hospitals: The importance of user rationale. *Information Management & Computer Security*, 24(4), pp. 266-287. 10.1108/IMCS-08-2012-0043.

Henseler, J., Ringle, C.M. & Sinkovics, R.R., 2009. The use of partial least squares path modeling in international marketing. In: R.R. Sinkovics & P.N. Ghauri, eds. *New challenges to international marketing*. Bingley: Emerald Group Publishing Limited, pp. 277-319. 10.1108/S1474-7979(2009)0000020014.

Henseler, J. & Sarstedt, M., 2013. Goodness-of-fit indices for partial least squares path modeling. *Computational Statistics*, 28(2), pp. 565-580. 10.1007/s00180-012-0317-1.

Henseler, J., Dijkstra, T.K., Sarstedt, M., Ringle, C.M., Diamantopoulos, A., Straub, D.W., Ketchen J., D.J., Hair, J.F., Hult, G.T.M. & Calantone, R.J., 2014. Common beliefs and reality about PLS: Comments on Rönkkö and Evermann (2013). *Organizational Research Methods*, 17(2), pp. 182-209. 10.1177/10944281145269.

Henseler, J., Ringle, C.M. & Sarstedt, M., 2015. A new criterion for assessing discriminant validity in variance-based structural equation modeling. *Journal of the Academy of Marketing Science*, 43(1), pp. 115-135. 10.1007/s11747-014-0403-8.

Henseler, J., Hubona, G. & Ray, P.A., 2016. Using PLS path modeling in new technology research: Updated guidelines. *Industrial Management & Data Systems*, 116(1), pp. 2-20. 10.1108/IMDS-09-2015-0382.

Herath, T. & Rao, H.R., 2009a. Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems*, 47(2), pp. 154-165. 10.1016/j.dss.2009.02.005.

Herath, T. & Rao, H.R., 2009b. Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems*, 18(2), pp. 106-125. 10.1057/ejis.2009.6.

Heyden, M.L.M., Fourné, S.P.L., Koene, B.A.S., Werkman, R. & Ansari, S., 2017. Rethinking 'Top-Down' and 'Bottom-Up' Roles of Top and Middle Managers in Organizational Change: Implications for Employee Support. *Journal of Management Studies*, 54(7), pp. 961-985. 10.1111/joms.12258.

Hofstede, G., Neuijen, B., Ohayv, D.D. & Sanders, G., 1990. Measuring organizational cultures: A qualitative and quantitative study across twenty cases. *Administrative Science Quarterly*, 35(2), pp. 286-316. 10.2307/2393392.

Hojati, H. & Azma, F., 2014. Relationship between ethical climate and the intention to remain in clinical nurses. *Quarterly Journal of Nursing Management*, 3(1), pp. 19-26.

Hong, Y. & Furnell, S., 2022. Motivating information security policy compliance: Insights from perceived organizational formalization. *Journal of Computer Information Systems*, 62(1), pp. 19-28. 10.1080/08874417.2019.1683781.

Hovav, A. & D'Arcy, J., 2012. Applying an extended model of deterrence across cultures: An investigation of information systems misuse in the US and South Korea. *Information & Management*, 49(2), pp. 99-110. 10.1016/j.im.2011.12.005.

Hoy, M.G. & Milne, G., 2010. Gender differences in privacy-related measures for young adult Facebook users. *Journal of Interactive Advertising*, 10(2), pp. 28-45. 10.1080/15252019.2010.10722168.

Hsieh, P.J., 2015. Physicians' acceptance of electronic medical records exchange: An extension of the decomposed TPB model with institutional trust and perceived risk. *International Journal of Medical Informatics*, 84(1), pp. 1-14. 10.1016/j.ijmedinf.2014.08.008.

Hsu, C.L., Lee, M.R. & Su, C.H., 2013. The Role of Privacy Protection in Healthcare Information Systems Adoption. *Journal of Medical Systems*, 37(5), pp. 9966. 10.1007/s10916-013-9966-z.

Hu, Q., Dinev, T., Hart, P. & Cooke, D., 2012. Managing employee compliance with information security policies: The critical role of top management and organizational culture. *Decision Sciences*, 43(4), pp. 615-660. 10.1111/j.1540-5915.2012.00361.x.

Huang, C.D., Behara, R.S. & Goo, J., 2014. Optimal information security investment in a Healthcare Information Exchange: An economic analysis. *Decision Support Systems*, 61, pp. 1-11. 10.1016/j.dss.2013.10.011.

Huang, D.L., Rau, P.L.P. & Salvendy, G., 2010. Perception of information security. *Behaviour & Information Technology*, 29(3), pp. 221-232. 10.1080/01449290701679361.

Hughes, V., 2017. Standout nurse leaders... What's in the research? *Nursing Management*, 48(9), pp. 16-24. 10.1097/01.NUMA.0000522171.08016.29.

Hulland, J., 1999. Use of partial least squares (PLS) in strategic management research: A review of four recent studies. *Strategic Management Journal*, 20(2), pp. 195-204. 10.1002/(SICI)1097-0266(199902)20:2<195::AID-SMJ13>3.0.CO;2-7.

Hung, S.Y., Ku, Y.C. & Chien, J.C., 2012. Understanding physicians' acceptance of the Medline system for practicing evidence-based medicine: A decomposed TPB model. *International Journal of Medical Informatics*, 81(2), pp. 130-142. 10.1016/j.ijmedinf.2011.09.009.

Hwang, H., Sarstedt, M., Cheah, J.H. & Ringle, C.M., 2020. A concept analysis of methodological research on composite-based structural equation modeling: Bridging PLSPM and GSCA. *Behaviormetrika*, 47(1), pp. 219-241. 10.1007/s41237-019-00085-5.

Hwang, J.I. & Park, H.A., 2014. Nurses' perception of ethical climate, medical error experience and intent-to-leave. *Nursing Ethics*, 21(1), pp. 28-42. 10.1177/0969733013486797.

IBM Software Group, 2013. *IBM SPSS Statistics 22 Brief Guide*. USA: s.n., s.l.

Informacijski pooblaščenec, n.d. *Prijava kršitev varnosti.* [online]. Available at: https://www.ip-rs.si/zakonodaja/reforma-evropskega-zakonodajnega-okvira-za-varstvo-osebnih-podatkov/kljucna-podrocja-uredbe/prijava-krsitev-varnosti/ [Accessed 21 March 2022].

International Council of Nurses, 2021. *The ICN code of ethics for nurses*. [pdf] International Council of Nurses. Available at: https://www.icn.ch/system/files/2021-10/ICN_Code-of-Ethics_EN_Web_0.pdf [Accessed 26 January 2023].

Ioannou, M., Stavrou, E. & Bada, M., 2019. Cybersecurity Culture in Computer Security Incident Response Teams: Investigating difficulties in communication and coordination. Proceedings of 2019 *International Conference on Cyber Security and Protection of Digital Services (Cyber Security), Oxford, UK, 3-4 Jun.* s.l.: Institute of Electrical and Electronics Engineers, pp. 1-4. 10.1109/CyberSecPODS.2019.8885240.

Ismail, Z., Masrom, M., Sidek, Z. & Hamzah, D., 2010. Framework to manage information security for Malaysian Academic Environment. *Information Assurance & Cybersecurity*, 2010, pp. 1-16. 10.5171/2010.305412.

Jakobsen, M. & Jensen, R., 2015. Common method bias in public management studies. *International public management journal*, 18(1), pp. 3-30. 10.1080/10967494.2014.997906.

Jalali, M.S., Bruckes, M., Westmattelmann, D. & Schewe, G., 2020. Why employees (still) click on phishing links: Investigation in hospitals. *Journal of Medical Internet Research*, 22(1), p. e16775. doi.org/10.2196/16775.

Jamalimoghadam, N., Yektatalab, S., Momennasab, M., Ebadi, A. & Zare, N., 2019. Hospitalized adolescents' perception of dignity: A qualitative study. *Nursing Ethics*, 26(3), pp. 728-737. 10.1177/0969733017720828.

James, H.S., 2000. Reinforcing ethical decision making through organizational structure. *Journal of Business Ethics*, 28(1), pp. 43-58. 10.1023/A:1006261412704.

Johnson, M.E., 2009. Data Hemorrhages in the Health-Care Sector. In: R. Dingledine & P. Golle, eds. *Financial Cryptography and Data Security: Lecture Notes in Computer Science.* Berlin Heidelberg: Springer, pp. 71-89.

Jones, A., 2007. A framework for the management of information security risks. *BT Technology Journal*, 25(1), pp. 30-36. 10.1007/s10550-007-0005-9.

Jöreskog, K.G., 1971. Simultaneous factor analysis in several populations. *Psychometrika*, 36(4), pp. 409-426. 10.1007/BF02291366.

Kamoun, F. & Nicho, M., 2014. Human and Organizational Factors of Healthcare Data Breaches: The Swiss Cheese Model of Data Breach Causation And Prevention. *International Journal of Healthcare Information Systems and Informatics*, 9(1), pp. 42-60. 10.4018/ijhisi.2014010103.

Karlsson, F., Hedström, K. & Goldkuhl, G., 2017. Practice-based discourse analysis of information security policies. *Computers & Security*, 67, pp. 267-279. 10.1016/j.cose.2016.12.012.

Kearns, A.J., 2017. A Duty-Based Approach for Nursing Ethics & Practice. In: P.A. Scott, ed. *Key Concepts and Issues in Nursing Ethics.* Cham: Springer International Publishing, pp. 15-27. 10.1007/978-3-319-49250-6_2.

Kessler, S.R., Pindek, S., Kleinman, G., Andel, S.A. & Spector, P.E., 2020. Information security climate and the assessment of information security risk among healthcare employees. *Health Informatics Journal*, 26(1), pp. 461-473. 10.1177/1460458219832048.

Khan, G.F., Sarstedt, M., Shiau, W.L., Hair, J.F., Ringle, C.M. & Fritze, M.P., 2019. Methodological research on partial least squares structural equation modeling (PLS-SEM): An analysis based on social network approaches. *Internet Research*, 29(3), pp. 407-429. 10.1108/IntR-12-2017-0509.

Kline, R.B., 2015. *Principles and practice of structural equation modeling*. 4th ed. New York: Guilford publications.

Knapp, K.J., Marshall, T.E., Kelly Rainer, R. & Nelson Ford, F., 2006. Information security: Management's effect on culture and policy. *Information Management & Computer Security*, 14(1), pp. 24-36. 10.1108/09685220610648355.

Kock, N. & Lynn, G., 2012. Lateral collinearity and misleading results in variance-based SEM: An illustration and recommendations. *Journal of the Association for Information Systems*, 13(7), pp. 546-580.

Kock, F., Berbekova, A. & Assaf, A.G., 2021. Understanding and managing the threat of common method bias: Detection, prevention and control. *Tourism Management*, 86, p. 104330. 10.1016/j.tourman.2021.104330.

Kranz, J. & Haeussinger, F., 2014. Why deterrence is not enough: The role of endogenous motivations on employees' information security behavior. *Proceedings of the International Conference on Information Systems - Building a Better World through Information Systems, ICIS. Auckland, New Zeland, 14-17 December*. s.l.: Association for Information Systems, pp. 23-44.

Kreitner, R. & Kinicki, A., 1995. *Organisational behaviour*. 3rd ed. Chicargo: Irwin.

Kumar, R., 2011. *Research methodology: A step-by-step guide for beginners*. 3rd ed. London: Sage Publications Ltd.

Kwon, J. & Johnson, M.E., 2012. Security practices and regulatory compliance in the healthcare industry. *Journal of the American Medical Informatics Association*, 20(1), pp. 44-51. 10.1136/amiajnl-2012-000906.

Kwon, J. & Johnson, M.E., 2018. Meaningful healthcare security: Does meaningful-use attestation improve information security performance? *MIS Quarterly*, 42(4), pp. 1043-1068. 10.25300/MISQ/2018/13580.

Lacey, D., 2010. Understanding and transforming organizational security culture. *Information Management & Computer Security*, 18(1), pp. 4-13. 10.1108/09685221011035223.

Lambe, G., Linnane, N., Callanan, I. & Butler, M.W., 2018. Cleaning up the paper trail-our clinical notes in open view. *International Journal of Health Care Quality Assurance*, 31(3), pp. 228-236. 10.1108/IJHCQA-09-2016-0126.

Landoll, D.J., 2011. *The security risk assessment handbook: A complete guide for performing security risk assessments.* 2nd ed. Boca Raton: CRC Press.

Laric, M.V., Pitta, D.A. & Katsanis, L.P., 2009. Consumer concerns for healthcare information privacy: A comparison of US and Canadian perspectives. *Research in Healthcare Financial Management*, 12(1), pp. 93-111.

Lee, E. & Seomun, G., 2021. Structural Model of the Healthcare Information Security Behavior of Nurses Applying Protection Motivation Theory. *International Journal of Environmental Research and Public Health*, 18(4), p. 2084. 10.3390/ijerph18042084.

Lee, M.C., 2009. Factors influencing the adoption of internet banking: An integration of TAM and TPB with perceived risk and perceived benefit. *Electronic Commerce Research and Applications*, 8(3), p. 130-141. 10.1016/j.elerap.2008.11.006.

Lee, Y., Kozar, K.A. & Larsen, K.R., 2003. The technology acceptance model: Past, present, and future. *Communications of the Association for Information Systems*, 12(1), pp. 752-780. 10.17705/1CAIS.01250.

Liang, H. & Xue, Y.L., 2010. Understanding security behaviors in personal computer usage: A threat avoidance perspective. *Journal of the Association for Information Systems*, 11(7), pp. 394-413. 10.17705/1jais.00232.

Lin, H.F., 2007. Predicting consumer intentions to shop online: An empirical test of competing theories. *Electronic Commerce Research and Applications*, 6(4), pp. 433-442. 10.1016/j.elerap.2007.02.002.

Ling, L.S., 2017. Impacts of information technology capabilities on small and medium enterprises (SMEs) and Large Enterprises. *Journal of Innovation Management in Small and Medium Enterprise*, 2017, pp. 1-9. 10.5171/2017.133143.

Liu, C.H., Chung, Y.F., Chen,T.S. & Wang, S.D., 2012. The Enhancement of Security in Healthcare Information Systems. *Journal of Medical Systems*, 36(3), pp. 1673-1688. 10.1007/s10916-010-9628-3.

Liu, L., Feng, Y., Hu, Q. & Huang, X., 2011. From transactional user to VIP: how organizational and cognitive factors affect ERP assimilation at individual level. *European Journal of Information Systems*, 20(2), pp. 186-200. 10.1057/ejis.2010.66.

Lloyd, G., 2020. The business benefits of cyber security for SMEs. *Computer Fraud & Security*, 2020(2), pp. 14-17. 10.1016/S1361-3723(20)30019-1.

Lopes, I. & Oliveira, P., 2014. Understanding Information Security Culture: A Survey in Small and Medium Sized Enterprises. In: Á. Rocha, A.M. Correia, F.B. Tan & K.A. Stroetmann, eds. *New Perspectives in Information Systems and Technologies: Advances in Intelligent Systems and Computing.* Cham: Springer International Publishing, pp. 277-286. 10.1007/978-3-319-05951-8_27.

Lundy, O. & Cowling, A., 1996. *Strategic human resource management*. London: International Thomson Business Pres.

Ma, X., 2022. IS professionals' information security behaviors in Chinese IT organizations for information security protection. *Information Processing & Management*, 59(1), p. 102744. 10.1016/j.ipm.2021.102744.

Ma, C.C., Kuo, K.M. & Alexander, J.W., 2015. A survey-based study of factors that motivate nurses to protect the privacy of electronic medical records. *BMC Medical Informatics and Decision Making*, 16(1), pp. 1-11. 10.1186/s12911-016-0254-y.

MacKinnon, D.P., Johnson, C.A., Pentz, M.A., Dwyer, J.H., Hansen, W.B., Flay, B.R. & Wang, E.Y.I., 1991. Mediating mechanisms in a school-based drug prevention program: First-year effects of the Midwestern Prevention Project. *Health Psychology*, 10(3), pp. 164-172. 10.1037/0278-6133.10.3.164.

Mamonov, S. & Benbunan-Fich, R., 2018. The impact of information security threat awareness on privacy-protective behaviors. *Computers in Human Behavior*, 83, pp. 32-44. 10.1016/j.chb.2018.01.028.

Marcoulides, G.A., Chin, W.W. & Saunders, C., 2009. A critical look at partial least squares modeling. *MIS Quarterly*, 33(1), pp. 171-175. 10.2307/20650283.

Marcoulides, G.A., Chin, W.W. & Saunders, C., 2012. When imprecise statistical statements become problematic: A response to Goodhue, Lewis, and Thompson. *Mis Quarterly*, 36(3), pp. 717-728. 10.2307/41703477.

Martins, A. & Eloff, J., 2002. Information Security Culture. In: M. A. Ghonaimy, M.T. El-Hadidi & H.K. Aslan, eds. *Security in the Information Society: IFIP Advances in Information and Communication Technology*. Boston: Springer, pp. 203-214. 10.1007/978-0-387-35586-3_16.

Martins, N. & Da Veiga, A., 2015. An Information Security Culture Model Validated with Structural Equation Modelling. In: S.M. Furnell & N.L. Clarke, eds. *Proceedings of the Ninth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2015. Mytilene, Greece, 1-3 July*. Plymouth: University of Plymouth, pp. 11-21.

Masrek, M.N., Harun, Q. & Sahid, N., 2018. Assessing the information security culture in a government context: The case of a developing country. *International Journal of Civil Engineering and Technology*, 9(8), pp. 96-112.

Mateos-Aparicio, G., 2011. Partial least squares (PLS) methods: Origins, evolution, and application to social sciences. *Communications in Statistics-Theory and Methods*, 40(13), pp. 2305-2317. 10.1080/03610921003778225.

Mayer, P., Kunz, A. & Volkamer, M., 2017. Reliable behavioural factors in the information security context. In: ARES 17: *International Conference on Availability, Reliability and Security Proceedings of the 12th International Conference on Availability, Reliability and Security 29 August - 1 September 2017, Reggio Calabria, Italy*. United States: Association for Computing Machinery New York. 10.1145/3098954.3098986.

McCoy, T.H. & Perlis, R.H., 2018. Temporal trends and characteristics of reportable health data breaches, 2010-2017. *Jama*, 320(12), pp. 1282-1284. 10.1001/jama.2018.9222.

McGill, T. & Thompson, N., 2018. Gender differences in information security perceptions and behaviour. In: M. Noble, ed. A*ustralasian Conference on Information Systems 2018. Sydney, 3-5 December*. Broadway: University of Technology Sydney. 10.5130/acis2018.co.

Metalidou, E., Marinagi, C., Trivellas, P., Eberhagen, N., Skourlas, C. & Giannakopoulos, G., 2014. The human factor of information security: Unintentional damage perspective. *Procedia-Social and Behavioral Sciences*, 147, pp. 424-428. 10.1016/j.sbspro.2014.07.133.

Mikuletič, S., 2021. Poziv k sodelovanju v raziskavi: Ali se zavedamo odgovornosti pri delu z zdravstvenimi podatki? In: M. Ažman. *Utrip: Glasilo Zbornice zdravstvene in babiške nege Slovenije - Zveze strokovnih društev medicinskih sester, babic in zdravstvenih tehnikov Slovenije*, 30(3), pp. 29-32.

Mikuletič, S., Vrhovec, S., Skela-Savič, B. & Žvanut, B., 2024. Security and privacy oriented information security culture (ISC): Explaining unauthorized access to healthcare data by nursing employees. *Computers & Security*, 134. 10.1016/j.cose.2023.103489.

Milfelner, B., Mumel, D. & Snoj, B., 2006. Metaanaliza dveh pristopov k raziskovanju kompleksnih marketinških problemov. *Our Economy*, 52(5/6), pp. 37-15.

Milliken, A. & Grace, P., 2017. Nurse ethical awareness: Understanding the nature of everyday practice. *Nursing Ethics*, 24(5), pp. 517-524. 10.1177/0969733015615172.

Milliken, A., Ludlow, L. & Grace, P., 2019. Ethical Awareness Scale: Replication Testing, Invariance Analysis, and Implications. *AJOB Empirical Bioethics*, 10(4), pp. 231-240. 10.1080/23294515.2019.1666176.

Milne, G.R., Labrecque, L.I. & Cromer, C., 2009. Toward an Understanding of the Online Consumer's Risky Behavior and Protection Practices. *Journal of Consumer Affairs*, 43(3), pp. 449-473. 10.1111/j.1745-6606.2009.01148.x.

Mohamed, N. & Ahmad, I.H., 2012. Information privacy concerns, antecedents and privacy measure use in social networking sites: Evidence from Malaysia. *Computers in Human Behavior*, 28(6), pp. 2366-2375. 10.1016/j.chb.2012.07.008.

Mohammadi, F., Tabatabaei, H. sadate, Mozafari, F. & Gillespie, M., 2020. Caregivers' perception of women's dignity in the delivery room: A qualitative study. *Nursing Ethics*, 27(1), pp. 116-126. 10.1177/0969733019834975.

Mohd, H. & Syed Mohamad, S.M., 2005. Acceptance model of electronic medical record. *Journal of Advancing Information and Management Studies*, 2(1), pp. 75-92.

Mokwetli, M. & Zuva, T., 2018. *A*doption of the ICT Security Culture in SMME's in the Gauteng Province, South Africa. *2018 International Conference on Advances in Big Data, Computing and Data Communication Systems (icABCD). Durban, South Africa, 6-7 Avgust.* s.l.: Institute of Electrical and Electronics Engineers, pp. 1-7. 10.1109/ICABCD.2018.8465139.

Moody, G.D., Siponen, M. & Pahnila, S., 2018. Toward a unified model of information security policy compliance. *MIS Quarterly*, 42(1), pp. 285-335. 10.25300/MISQ/2018/13853.

Munthe, C., Sandman, L. & Cutas, D., 2012. Person centred care and shared decision making: Implications for ethics, public health and research. *Health Care Analysis*, 20(3), pp. 231-249. 10.1007/s10728-011-0183-y.

Murko, A. & Vrhovec, S., 2019. Bitcoin adoption: Scams and anonymity may not matter but trust into Bitcoin security does. *Central European Cybersecurity Conference (CECC) 2019: Proceedings of the Third Central European Cybersecurity Conference. Germanj, Munich, 14-15 November*. New York: Association for Computing Machinery, pp. 1-6. 10.1145/3360664.3360679.

Mwagwabi, F., McGill, T. & Dixon, M., 2018. Short-term and long-term effects of fear appeals in improving compliance with password guidelines. *Communications of the Association for Information Systems*, 42(1), pp. 147-182. 10.17705/1CAIS.04207.

Nacionalni inštitut za javno zdravje, 2018. *Viri v zdravstvu, izvajalci zdravstvene dejavnosti*. [online] Available at: https://podatki.nijz.si/pxweb/sl/NIJZ%20podatkovni%20portal/ [Accessed 23 March 2022].

Nævestad, T.O., Meyer, S.F. & Honerud, J.H., 2018. Organizational information security culture in critical infrastructure: Developing and testing a scale and its relationships to other measures of information security. In: S. Haugen, A. Barros, C. Gulijk, T. Kongsvik & J.E. Vinnem, eds. *Proceedings of ESREL 2018: Safety and Reliability - Safe Societies in a Changing World. Trondheim, Norway, 17-21 June*.s.l.: CRC Press, pp. 3021-3029.

Narain Singh, A., Gupta, M.P. & Ojha, A., 2014. Identifying factors of "organizational information security management". *Journal of Enterprise Information Management*, 27(5), pp. 644-667. 10.1108/JEIM-07-2013-0052.

Nasir, A., Abdullah Arshah, R. & Ab Hamid, M.R., 2019a. A dimension-based information security culture model and its relationship with employees' security behavior: A case study in Malaysian higher educational institutions. *Information Security Journal: A Global Perspective*, 28(3), pp. 55-80. 10.1080/19393555.2019.1643956.

Nasir, A., Arshah, R.A., Ab Hamid, M.R. & Fahmy, S., 2019b. An analysis on the dimensions of information security culture concept: A review. *Journal of Information Security and Applications*, 44, pp. 12-22. 10.1016/j.jisa.2018.11.003.

Nasir, A., Arshah, R.A. & Ab Hamid, M.R., 2020. Information Security Culture for Guiding Employee's Security Behaviour: A Pilot Study. *2020 6th IEEE International Conference on Information Management (ICIM). United Kindom, London, 27-29 March.* United Kingdom, London: Institute of Electrical and Electronics Engineers, pp. 205-209. 10.1109/ICIM49319.2020.244699.

Nasir, A., Arshah, R.A., Ab Hamid, M.R. & Fahmy, S., 2022. Information Security Culture Concept towards Information Security Compliance: A Comparison between IT and Non-IT Professionals. *International Journal of Integrated Engineering*, 14(3), pp. 57-165. 10.30880/ijie.2022.14.03.017.

Natsiavas, P., Kakalou, C., Votis, K., Tzovaras, D. & Koutkias, V., 2019. Citizen Perspectives on Cross-Border eHealth Data Exchange: A European Survey. *Studies in Health Technology and Informatics*, 264, pp. 719-723. 10.3233/SHTI190317.

Neame, R.L., 2014. Privacy protection in personal health information and shared care records. *Journal of Innovation in Health Informatics*, 21(2), pp. 84-91. 10.14236/jhi.v21i2.55.

Nel, F. & Drevin, L., 2019. Key elements of an information security culture in organisations. *Information & Computer Security*, 27(2), pp. 146-164. 10.1108/ICS-12-2016-0095.

Nijsingh, N., Jansky, B., Marckmann, G. & Kuehlmeyer, K., 2020. Mind the Gap: How Should We Translate Specific Ethical Norms Into Interventions? *The American Journal of Bioethics*, 20(4), pp. 89-91. 10.1080/15265161.2020.1730500.

Nitzl, C., 2016. The use of partial least squares structural equation modelling (PLS-SEM) in management accounting research: Directions for future theory development. *Journal of Accounting Literature*, 37(1), pp. 19-35. 10.1016/j.acclit.2016.09.003.

Noureddine, S., 2001. Development of the ethical dimension in nursing theory. *International Journal of Nursing Practice*, 7(1), pp. 2-7. 10.1046/j.1440-172x.2001.00253.x.

Nunnally, J.C. & Bernstein, I., 1994. *Psychometric Theory*. 3rd ed. New York: The Clarindu Compuny.

Oh, S. & Han, H., 2020. Facilitating organisational learning activities: Types of organisational culture and their influence on organisational learning and performance. *Knowledge Management Research & Practice*, 18(1), pp. 1-15. 10.1080/14778238.2018.1538668.

Olivos, O., 2012. Creating a Security Culture Development Plan and a case study. In: N. Clarke & S. Furnell, eds. *Proceedings of the Sixth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2012)*. Crete, Greece, 6-8 Jun. United Kongdom: Plymouth University, pp. 13-32.

Oluka, O.C., Nie, S. & Sun, Y., 2014. Quality assessment of TPB-based questionnaires: A systematic review. *PloS One*, 9(4), p. e94419. 10.1371/journal.pone.0094419.

Omidosu, J. & Ophoff, J., 2016. A theory-based review of information security behavior in the organization and home context. In: V. Kumar, U.G. Singh & S.D. Sudarsan, eds. *2016 International Conference on Advances in Computing and Communication*

Engineering (ICACCE). Durban, South Africa, 28-29 Nov. s.l.: Institute of Computing and Communication Engineering, pp. 225-231. 10.1109/ICACCE.2016.8073752.

Orehek, Š., 2017. *Merjenje informacijske varnostne kulture: Metaanaliza anketnih merskih inštrumentov: magistrsko delo.* Ljubljana: Univerza v Ljubljani, Fakulteta za družbene vede.

Ovijač, D., Velepic, M., Adamic, M., Eder, J., Buček Hajdarević, I., Kardoš, Z., Klemenc, D., Marin, E., Marinič, M., Naka, S., Peterka-Novak, J., Štebe, V. & Vojnovič, A., 2017. *Kodeks etike v zdravstveni negi in oskrbi Slovenije*. Zbornica zdravstvene in babiške nege Slovenije – Zveza strokovnih društev medicinskih sester, babic in zdravstvenih tehnikov Slovenije.

Pai, J., 2006. An empirical study of the relationship between knowledge sharing and IS/IT strategic planning (ISSP). *Management Decision*, 44(1), pp. 105-122. 10.1108/00251740610641490.

Park, H.S. & Smith, S.W., 2007. Distinctiveness and influence of subjective norms, personal descriptive and injunctive norms, and societal descriptive and injunctive norms on behavioral intent: A case of two behaviors critical to organ donation. *Human Communication Research*, 33(2), pp. 194-218. 10.1111/j.1468-2958.2007.00296.x.

Parsons, K.M., Young, E., Butavicius, M.A., McCormac, A., Pattinson, M.R. & Jerram, C., 2015. The Influence of Organizational Information Security Culture on Information Security Decision Making. *Journal of Cognitive Engineering and Decision Making*, 9(2), pp. 117-129. 10.1177/1555343415575152.

Pătrașcu, P., 2019. Promoting cybersecurity culture through education. *Conference proceedings of »15th eLearning and Software for Education« (eLSE), Bucharest, Romania, 11-12 Apr.* s.l.: Carol I National Defence University Publishing House, pp. 273-279.

Pauly, B., Varcoe, C., Storch, J. & Newton, L., 2009. Registered nurses' perceptions of moral distress and ethical climate. *Nursing Ethics*, 16(5), pp. 561-573. 10.1177/0969733009106649.

Pavlou, P.A. & Fygenson, M., 2006. Understanding and predicting electronic commerce adoption: An extension of the theory of planned behavior. *MIS Quarterly*, 30(1), pp. 115-143. 10.2307/25148720.

Peikari, H.R., Shah, M.H. & Lo, M.C., 2018. Patients' perception of the information security management in health centers: The role of organizational and human factors. *BMC Medical Informatics and Decision Making*, 18(1), pp. 1-13. 10.1186/s12911-018-0681-z.

Philip, S.J., Luu, T.J. & Carte, T., 2023. There's No place like home: Understanding users' intentions toward securing internet-of-things (IoT) smart home networks. *Computers in Human Behavior*, 139, p. 107551. 10.1016/j.chb.2022.107551.

Pishgooie, A.H., Barkhordari-Sharifabad, M., Atashzadeh-Shoorideh, F. & Falcó-Pegueroles, A., 2019. Ethical conflict among nurses working in the intensive care units. *Nursing Ethics*, 26(7-8), pp. 2225-2238. 10.1177/0969733018796686.

Podsakoff, P.M., MacKenzie, S.B., Lee, J.Y. & Podsakoff, N.P., 2003. Common method biases in behavioral research: A critical review of the literature and recommended remedies. *Journal of Applied Psychology*, 88(5), pp. 879-903. 10.1037/0021-9010.88.5.879.

Podsakoff, P.M., MacKenzie, S.B. & Podsakoff, N.P., 2012. Sources of method bias in social science research and recommendations on how to control it. *Annual Review of Psychology*, 63, pp. 539-569. 10.1146/annurev-psych-120710-100452.

Polit, D.F. & Beck, C.T., 2008. *Essentials of nursing research: Appraising evidence for nursing practice*. 7th ed. Philadelphia: Lippincott Williams & Wilkins.

Polites, G.L., Roberts, N. & Thatcher, J., 2012. Conceptualizing models using multidimensional constructs: A review and guidelines for their use. *European Journal of Information Systems*, 21(1), pp. 22-48. 10.1057/ejis.2011.10.

Ponemon Institute, 2015. C*ost of Data Breach Study: Global Analysis*. [pdf] Ponemon Institute. Available at: https://nhlearningsolutions.com/Portals/0/Documents/2015-Cost-of-Data-Breach-Study.PDF [Accessed 2 December 2017].

Ponemon Institute LLC, 2020. *Cost of a Data Breach Report 2020.* [pdf] IBM Corporation. Available at: https://www.ibm.com/security/digital-assets/cost-data-breach-report/ [Accessed 15 March 2021].

Posey, C. & Folger, R., 2020. An exploratory examination of organizational insiders' descriptive and normative perceptions of cyber-relevant rights and responsibilities. *Computers & Security*, 99(1), pp. 102038. 10.1016/j.cose.2020.102038.

Price-Waterhouse-Coopers, 2016. *The Global State of Information Security Survey 2016*. [pdf] The Global State of Information Security. Available at: https://www.pwc.com/sg/en/publications/assets/pwc-global-state-of-information-security-survey-2016.pdf [Accessed 2 December 2017].

Price, S. & Reichert, C., 2017. The Importance of Continuing Professional Development to Career Satisfaction and Patient Care: Meeting the Needs of Novice to Mid- to Late-Career Nurses throughout Their Career Span. *Administrative Sciences*, 7(2), pp. 17. 10.3390/admsci7020017.

Price, W.N. & Cohen, I.G., 2019. Privacy in the age of medical big data. *Nature Medicine*, 25(1), pp. 37-43. 10.1038/s41591-018-0272-7.

Pridmore, J. & Oomen, T.A.P., 2021. A Practice-Based Approach to Security Management: Materials, Meaning and Competence for Trainers of Healthcare Cybersecurity. In: G. Jacobs, I. Suojanen, K. Horton & P. Bayerl, eds. *Advanced Sciences*

and Technologies for Security Applications: Information Security Management - New Solutions to Complexity. Cham: Springer, pp. 357-369. 10.1007/978-3-030-42523-4_24.

Puhakainen, P. & Siponen, M., 2010. Improving Employees' Compliance Through Information Systems Security Training: An Action Research Study. *MIS Quarterly*, 34(4), pp. 757-778. 10.2307/25750704.

Quinn, R.E., 1988. *Beyond rational management: Mastering the paradoxes and competing demands of high performance.* San Francisco: Jossey-Bass.

Raithel, S., Sarstedt, M., Scharf, S. & Schwaiger, M., 2012. On the value relevance of customer satisfaction. Multiple drivers and multiple markets. *Journal of the Academy of Marketing Science*, 40(4), pp. 509-525. 10.1007/s11747-011-0247-4.

Rajab, M. & Eydgahi, A., 2019. Evaluating the explanatory power of theoretical frameworks on intention to comply with information security policies in higher education. *Computers & Security*, 80, pp. 211-223. 10.1016/j.cose.2018.09.016.

Rantos, K., Fysarakis, K. & Manifavas, C., 2012. How effective is your security awareness program? An evaluation methodology. *Information Security Journal: A Global Perspective*, 21(6), pp. 328-345. 10.1080/19393555.2012.747234.

Raykov, T., 1998. Coefficient alpha and composite reliability with interrelated nonhomogeneous items. *Applied Psychological Measurement*, 22(4), pp. 375-385. 10.1177/014662169802200407.

Reid, R. & Van Niekerk, J., 2014. From information security to cyber security cultures. In: H.S. Venter, M. Loock, M. Coetzee & M.M. Eloff, eds. 2*014 Information Security for South Africa (ISSA): Proceedings of the ISSA 2014 Conference. Johannesburg, South Africa, 13-14 Aug.* s.l.: The Institute of Electrical and Electronics Engineers computer society, pp. 1-7. 10.1109/ISSA.2014.6950492.

Reid, R., Van Niekerk, J. & Renaud, K., 2014. Information security culture: A general living systems theory perspective. In: H.S. Venter, M. Loock, M. Coetzee & M.M. Eloff, eds. *2014 Information Security for South Africa (ISSA): Proceedings of the ISSA 2014 Conference. Johannesburg, South Africa, 13-14 Aug.* s.l.: The Institute of Electrical and Electronics Engineers computer society, pp. 1-8. 10.1109/ISSA.2014.6950493.

Reinartz, W., Haenlein, M. & Henseler, J., 2009. An empirical comparison of the efficacy of covariance-based and variance-based SEM. *International Journal of Research in Marketing*, 26(4), pp. 332-344. 10.1016/j.ijresmar.2009.08.001.

Rigdon, E.E., 2012. Rethinking partial least squares path modeling: In praise of simple methods. *Long Range Planning*, 45(5-6), pp. 341-358. 10.1016/j.lrp.2012.09.010.

Rigdon, E.E., 2014a. Comment on "Improper use of endogenous formative variables". *Journal of Business Research*, 67(1), pp. 2800-2802. 10.1016/j.jbusres.2012.08.005.

Rigdon, E.E., 2014b. Rethinking partial least squares path modeling: Breaking chains and forging ahead. *Long Range Planning*, 47(3), pp. 161-167. 10.1016/j.lrp.2014.02.003.

Rigdon, E.E., 2016. Choosing PLS path modeling as analytical method in European management research: A realist perspective. *European Management Journal*, 34(6), pp. 598-605. 10.1016/j.emj.2016.05.006.

Ringle, C.M., Wende, S. & Becker, J.M., 2022. *SmartPLS4.* [programska oprema] Available at: https://www.smartpls.com/ [Accessed 8 July 2022].

Robbins, 2001. *Organisational behaviour: Leading and managing in Australia and New Zeland*. 3rd ed. New South Wales, Australia: Pearson Education Australia.

Rocha Flores, W. & Ekstedt, M., 2016. Shaping intention to resist social engineering through transformational leadership, information security culture and awareness. *Computers & Security*, 59(1), pp. 26-44. 10.1016/j.cose.2016.01.004.

Roer, K. & Petric, G., 2018. *Age, Experience, Risk and Security: A Security Culture Report*. [pdf] CLTRe North America. Available at: https://www. get.clt.re/blog/new-report-on-how-age-and-experience-influence-risk-and-security-free-download [Accessed 5 January 2023].

Ruhwanya, Z. & Ophoff, J., 2019. Information security culture assessment of small and medium-sized enterprises in Tanzania. In: P. Nielsen & H.C. Kimaro, eds. *15th IFIP WG 9.4 International Conference on Social Implications of Computers in Developing Countries - Information and Communication Technologies for Development: Strengthening Southern-Driven Cooperation as a Catalyst for CT4D, Tanzania, 1-3 May*. Cham: Springer, pp. 776-788. 10.1007/978-3-030-18400-1_63.

Ruighaver, A.B., Maynard, S.B. & Warren, M., 2010. Ethical decision making: Improving the quality of acceptable use policies. *Computers & Security*, 29(7), pp. 731-736. 10.1016/j.cose.2010.05.004.

Ryu, S., Ho, S.H. & Han, I., 2003. Knowledge sharing behavior of physicians in hospitals. *Expert Systems with Applications*, 25(1), pp. 113-122. 10.1016/S0957-4174(03)00011-3.

Saberi, Z., Shahriari, M. & Yazdannik, A.R., 2019. The relationship between ethical conflict and nurses' personal and organisational characteristics. *Nursing Ethics*, 26(7-8), pp. 2427-2437. 10.1177/0969733018791350.

Safa, N.S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N.A. & Herawan, T., 2015. Information security conscious care behaviour formation in organizations. *Computers & Security*, 53(1), pp. 65-78. 10.1016/j.cose.2015.05.012.

Safa, N.S., Von Solms, R. & Furnell, S., 2016. Information security policy compliance model in organizations. *Computers & Security*, 56(1), pp. 70-82. 10.1016/j.cose.2015.10.006.

Safa, N.S., 2017. The information security landscape in the supply chain. *Computer Fraud & Security*, 2017(6), pp. 16-20. 10.1016/S1361-3723(17)30053-2.

Sale, D.N., 2005. *Understanding clinical governance and quality assurance: Making it happen*. New York: Palgrave Macmillan.

Saleh, Z.I., Refai, H. & Mashhour, A., 2011. Proposed Framework for Security Risk Assessment. *Journal Information Security*, 2(2), pp. 85-90. 10.4236/jis.2011.22008.

Santos-Olmo, A., Sánchez, L.E., Caballero, I., Camacho, S. & Fernandez-Medina, E., 2016. The importance of the security culture in SMEs as regards the correct management of the security of their assets. *Future Internet*, 8(3), p. 30. 10.3390/fi8030030.

Saranto, K., Kivekäs, E., Kinnunen, U.M. & Palojoki, S., 2018. Lack of Patient Data Privacy Challenges Patient Safety. *Studies in Health Technology and Informatics*, 251(1), pp. 163-166. 10.3233/978-1-61499-880-8-163.

Sarbaz, M., Manouchehri Monazah, F., Banaye Yazdipour, A. & Kimiafar, K., 2019. Views of Health Information Management Staff on Non-Technical Security Management Factors. In: A. Shabo, I. Madsen, H.U. Prokosch, K. Hayrinen, K.H. Wolf, F. Martin-Sanchez, M. Lobe & T.M. Deserno, eds. *ICT for health science research: proceedings of the EFMI 2019 Special Topic Conference, Hanover, Germany, 7-10 Apr.* Amsterdam: IOS Press, pp. 65-69. 10.3233/978-1-61499-959-1-65.

Sari, P.K., Prasetio, A., Candiwan, Handayani, P.W., Hidayanto, A.N., Syauqina, S., Astuti, E.F. & Tallei, F.P., 2021. Information security cultural differences among health care facilities in Indonesia. *Heliyon*, 7(6), p. e07248. 10.1016/j.heliyon.2021.e07248.

Sarstedt, M., Ringle, C.M., Henseler, J. & Hair, J.F., 2014. On the emancipation of PLS-SEM: A commentary on Rigdon (2012). *Long Range Planning*, 47(3), pp. 154-160. 10.1016/j.lrp.2014.02.007.

Sarstedt, M., Hair, J.F., Ringle, C.M., Thiele, K.O. & Gudergan, S.P., 2016. Estimation issues with PLS and CBSEM: Where the bias lies! *Journal of Business Research,* 69(10), pp. 3998-4010. 10.1016/j.jbusres.2016.06.007.

Sarstedt, M., 2019. Der knacks and a silver bullet. In: B.J. Babin & M. Sarstedt, eds. *The Great Facilitator*. Cham: Springer, pp. 155-164. 10.1007/978-3-030-06031-2_19.

Sarstedt, M. & Cheah, J.H., 2019. Partial least squares structural equation modeling using SmartPLS: a software review. *Journal of Marketing Analytics*, 7(1), pp. 196-202. 10.1057/s41270-019-00058-3.

Sarstedt, M., Ringle, C.M. & Hair, J.F., 2021. Partial least squares structural equation modeling. In: C. Homburg, M. Klarmann & A. Vomberg, eds. *Handbook of market research*. Cham: Springer, pp. 587-632. 10.1007/978-3-319-57413-4_15.

Schein, E.H. & Schein, P.A., 2019. *The corporate culture survival guide*. 3rd ed. New Jersey: John Wiley & Sons, p. 21.

Schlienger, T. & Teufel, S., 2003. Analyzing information security culture: Increased trust by an appropriate information security culture. *DEXA '03:14th International Workshop on Database and Expert Systems Applications, Prague, Czech Republic, 1-5 Sept.* Washington: The Institute of Electrical and Electronics Engineers computer society, pp. 405-409. 10.1109/DEXA.2003.1232055.

Selič, P., 1999. *Psihologija bolezni našega časa*. Ljubljana: Znanstveno in publicistično središče, p. 42.

Seyal, A.H. & Turner, R., 2013. A study of executives' use of biometrics: An application of theory of planned behaviour. *Behaviour & Information Technology,* 32(12), pp. 1242-1256. 10.1016/j.heliyon.2021.e07248.

Shameli-Sendi, A., Aghababaei-Barzegar, R. & Cheriet, M., 2016. Taxonomy of information security risk assessment (ISRA). *Computers & Security*, 57(1), pp. 14-30. 10.1016/j.cose.2015.11.001.

Sharma, P.N., Shmueli, G., Sarstedt, M., Danks, N. & Ray, S., 2019a. Prediction-oriented model selection in partial least squares path modeling. *Decision Sciences*, 52(3), pp. 567-607. 10.1111/deci.12329.

Sharma, P., Sarstedt, M., Shmueli, G., Kim, K.H. & Thiele, K.O., 2019b. PLS-based model selection: The role of alternative explanations in information systems research. *Journal of the Association for Information Systems*, 20(4), pp. 346-397. 10.17005/1.jais.00538.

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L.F. & Downs, J., 2010. Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions. *The 28th Annual CHI Conference The 28th Annual CHI Conference on Human Factors in Computing Systems. Atlanta, Georgia, USA, 10-15 Apr.* New York: Association for Computing MachineryNew York, pp. 373-382. 10.1145/1753326.1753383.

Sherif, E., Furnell, S. & Clarke, N., 2015. An identification of variables influencing the establishment of information security culture. In: T. Tryfonas & I. Askoxylakis, eds. *Human Aspects of Information Security, Privacy, and Trust: Third International Conference, Held as Part of HCI International 2015. Los Angeles, CA, USA, 2-7 Aug.* Cham: Springer, pp. 436-448. 10.1007/978-3-319-20376-8_39.

Shmueli, G., 2010. To explain or to predict? *Statistical Science*, 25(3), pp. 289-310. 10.1214/10-STS330.

Shmueli, G. & Koppius, O.R., 2011. Predictive analytics in information systems research. *MIS Quarterly*, 35(3), pp. 553-572. 10.2307/23042796.

Shmueli, G., Ray, S., Estrada, J.M.V. & Chatla, S.B., 2016. The elephant in the room: Predictive performance of PLS models. *Journal of Business Research*, 69(10), pp. 4552-4564. 10.1016/j.jbusres.2016.03.049.

Shmueli, G., Sarstedt, M., Hair, J.F., Cheah, J.H., Ting, H., Vaithilingam, S. & Ringle, C.M., 2019. Predictive model assessment in PLS-SEM: guidelines for using PLSpredict. *European Journal of Marketing,* 53(11), pp. 2322-2347. 10.1108/EJM-02-2019-0189.

Slovenian Computer Emergency Response Team (SI-CERT), 2021. *Poročilo o kibernetski varnosti za leto 2020.* [pdf] Javni zavod Arnes. Available at: https://www.cert.si/wp-content/uploads/2021/07/Si-CERT-e_porocilo-o-kibern-varnosti-2020.pdf [Accessed 27 January 2023].

Slovensko društvo informatika, 2016. *Islovar* [online] Available at: http://www.islovar.org/islovar/islovar [Accessed 3 December 2021].

Siponen, M. & Vance, A., 2010. Neutralization: New insights into the problem of employee information systems security policy violations. *MIS Quarterly*, 34(3), pp. 487-502. 10.2307/25750688.

SmartPLS GmbH, 2023. *Goodness of Fit (GoF)* [online] Available at: https://www.smartpls.com/documentation/algorithms-and-techniques/goodness-of-fit/[Accessed 3 December 2023].

Smircich, L., 1983. Concepts of culture and organizational analysis. *Administrative Science Quarterly*, 83(28), pp. 339-358. 10.2307/2392246.

Smith, S., Winchester, D., Bunker, D. & Jamieson, R., 2010. Circuits of Power: A Study of Mandated Compliance to an Information Systems Security" De Jure" Standard in a Government Organization. *MIS Quarterly*, 34(3), pp. 463-486. 10.2307/25750687.

Soper, D.S., 2020. *A-priori Sample Size Calculator for Structural Equation Models.* [programska oprema] Available at: http://www.danielsoper.com/statcalc [Accessed 27 January 2023].

Splošna uredba EU o varstvu podatkov (GDPR), 2016. Uradni list Evropske unije št. 679, p. 34.

Srite, M. & Karahanna, E., 2006. The role of espoused national cultural values in technology acceptance. *MIS Quarterly*, 30(3), pp. 679-704. 10.2307/25148745.

Stango, A., Prasad, N.R. & Kyriazanos, D.M., 2009. A threat analysis methodology for security evaluation and enhancement planning. In: R. Falk, W. Goudalo, E.Y. Chen, R. Savola & M. Popescu, eds. *Third International Conference on Emerging Security Information, Systems and Technologies 2009. Athens, Greece, 18-23 June.* Piscataway: The Institute of Electrical and Electronics Engineers computer society, pp. 262-267. 10.1109/SECURWARE.2009.47.

Stavros, D., Nikolaos, B., George, A. & Apostolos, V., 2016. Organizational change management: Delineating employee reaction to change in SMEs located in Magnesia. *Academic Journal of Interdisciplinary Studies*, 5(1), pp. 309-309. 10.5901/ajis.2016.v5n1p309.

Stone, M., 1974. Cross-validatory choice and assessment of statistical predictions. *Journal of the Royal Statistical Society: Series B (Methodological)*, 36(2), pp. 111-133. 10.1111/j.2517-6161.1974.tb00994.x.

Straub, D., Boudreau, M.C. & Gefen, D., 2004. Validation guidelines for IS positivist research. *Communications of the Association for Information Systems*, 13(1), pp. 380-427. 10.17705/1CAIS.01324.

Straub, D.W. & Welke, R.J., 1998. Coping with systems risk: Security planning models for management decision making. *MIS Quarterly*, 22(4), pp. 441-469. 10.2307/249551.

Svantesson, M., Griffiths, F., White, C., Bassford, C. & Slowther, A., 2021. Ethical conflicts during the process of deciding about ICU admission: An empirically driven ethical analysis. *Journal of Medical Ethics*, 47(12), p. e87-e87. 10.1136/medethics-2020-106672.

Tabachnick, B. & Fidell, L., 2018. *Using multivariate statistics.* 7th ed. New York: Pearson Education.

Tan, H.V.D. & Conde, A.R., 2021. Nurse empowerment—Linking demographics, qualities and performances of empowered Filipino nurses. *Journal of Nursing Management*, 29(5), pp. 1302-1310. 10.1111/jonm.13270.

Tang, M., Li, M. & Zhang, T., 2016. The impacts of organizational culture on information security culture: A case study. *Information Technology and Management*, 17(2), pp. 179-186. 10.1007/s10799-015-0252-2.

Tarimo, C., Bakari, J., Yngström, L. & Kowalski, S., 2006. A Social-Technical View of ICT Security Issues, Trends, and Challenges: Towards a Culture of ICT Security: The Case of Tanzania. In: J.H.P. Eloff, L. Labuschagne, M.M. Eloff & H.S. Ventre, eds. *Proceedings of the ISSA 2006 from Insight to Foresight Conference. Sandton, South Africa, 5-7 Jul.* Pretoria, South Africa: ISSA, pp.1-12.

Taylor, S. & Todd, P.A., 1995. Understanding information technology usage: A test of competing models. *Information Systems Research*, 6(2), pp. 144-176. 10.1287/isre.6.2.144.

Tehseen, S., Ramayah, T. & Sajilan, S., 2017. Testing and controlling for common method variance: A review of available methods. *Journal of Management Sciences*, 4(2), pp. 142-168. 10.20547/jms.2014.

Tejero, A. & de la Torre, I., 2012. Advances and Current State of the Security and Privacy in Electronic Health Records: Survey from a Social Perspective. *Journal of Medical Systems*, 36(5), pp. 3019-3027. 10.1007/s10916-011-9779-x.

Terry, N., 2017. Existential challenges for healthcare data protection in the United States. *Ethics, Medicine and Public Health*, 3(1), pp. 19-27. 10.1016/j.jemep.2017.02.007.

Thomson, K.L., Von Solms, R. & Louw, L., 2006. Cultivating an organizational information security culture. *Computer Fraud & Security*, 2006(10), pp. 7-11. 10.1016/S1361-3723(06)70430-4.

Tolah, A., Furnell, S.M. & Papadaki, M., 2019. *A comprehensive framework for understanding security culture in organizations*, 557(1), pp. 143-156. 10.1007/978-3-030-23451-5_11.

Tolah, A., Furnell, S. & Papadaki, M., 2017. A Comprehensive Framework for Cultivating and Assessing Information Security Culture. In: S. Furnell & N.L. Clarke, eds. *Eleventh International Symposium on Human Aspects of Information Security & Assurance, HAISA 2017. Adelaide, Australia, 28-30 Nov.* s.l.: University of Plymouth, pp. 52-64.

Tonneau, D., 1997. Management tools and organization as key factors towards quality care: Reflections from experience. *International Journal for Quality in Health Care*, 9(3), pp. 201-205. 10.1093/intqhc/9.3.201.

Tsui, A.S., Zhang, Z.X., Wang, H., Xin, K.R. & Wu, J.B., 2006. Unpacking the relationship between CEO leadership behavior and organizational culture. *The Leadership Quarterly*, 17(2), pp. 113-137. 10.1016/j.leaqua.2005.12.001.

Tyler, T.R., Callahan, P.E. & Frost, J., 2007. Armed, and dangerous (?): Motivating rule adherence among agents of social control. *Law & Society Review*, 41(2), pp. 457-492. 10.1111/j.1540-5893.2007.00304.x.

Uchendu, B., Nurse, J.R., Bada, M. & Furnell, S., 2021. Developing a cyber security culture: Current practices and future needs. *Computers & Security,* 109(1), p. 102387. 10.1016/j.cose.2021.102387.

Uffen, J., Guhr, N. & Breitner, M.H., 2012. Personality traits and information security management: An empirical study of information security executives. *Proceedings of the International Conference on Information Systems - Thirty Third International Conference on Information Systems (ICIS) 2012.* Orlando, Florida, USA, 16-19 Dec. s.l.: Association for Information Systems, pp. 2-22.

U.S. Department of Health & Human Services - Office for Civil Rights, n.d. *Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information*. [online] Available at: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf [Accessed 15 March 2021].

U.S. Department of Labor, Employee Benefits Security Administration, 2004. *Health Coverage Portability: Health Insurance Portability and Accountability Act of 1996 (HIPAA).* Washington, D.C.: U.S. Department of Labor, Employee Benefits Security Administration.

Ustava Republike Slovenije (URS), 1991. Uradni list Republike Slovenije št. 33/91-I.

Van Niekerk, J. & Von Solms, R., 2006. Understanding Information Security Culture: A Conceptual Framework. In: J.H.P. Eloff, L. Labuschagne, M.M. Eloff & H.S. Ventre, eds. *Proceedings of the ISSA 2006 from Insight to Foresight Conference. Sandton, South Africa, 5-7 Jul.* Pretoria, South Africa: ISSA, pp. 1-9.

Van Niekerk, J. & Von Solms, R., 2010. Information security culture: A management perspective. *Computers & Security,* 29(4), pp. 476-486. 10.1016/j.cose.2009.10.005.

Van‘t Wout, C., 2019. Develop and maintain a cybersecurity organisational culture. In: N. van der Waag & L. Leen, eds. P*roceedings of the 14th International Conference on*

Cyber Warfare and Security (ICCWS) 2019. South Africa, Stellenbosch University and CSIR, 28 Feb - 1 Mar. Unitend Kindgdom: Academic Conferences and Publishing International Limited, pp. 457-466.

Viswanathan, M. & Kayande, U., 2012. Commentary on "common method bias in marketing: Causes, mechanisms, and procedural remedies".*Journal of Retailing*, 88(4), pp. 556-562. 10.1016/j.jretai.2012.10.002.

Von Solms, B. & Von Solms, R., 2004. The 10 deadly sins of information security management. *Computers & Security*, 23(5), pp. 371-376. 10.1016/j.cose.2004.05.002.

Voorhees, C.M., Brady, M.K., Calantone, R. & Ramirez, E., 2016. Discriminant validity testing in marketing: An analysis, causes for concern, and proposed remedies. *Journal of the Academy of Marketing Science*, 44(1), pp. 119-134. 10.1007/s11747-015-0455-4.

Vrhovec, S., Bernik, I. & Markelj, B., 2023. Explaining information seeking intentions: Insights from a Slovenian social engineering awareness campaign. *Computers & Security*, 125, p. 103038. 10.1016/j.cose.2022.103038.

Weijters, B. & Baumgartner, H., 2012. Misresponse to reversed and negated items in surveys: A review. *Journal of Marketing Research*, *49*(5), pp. 737-747. 10.1509/jmr.11.0.

Westland, J.C., 2015. Partial least squares path analysis. In: *Structural Equation Models: From Paths to Network (Studies in Systems, Decision and Control).* Cham: Springer, pp. 23-46. 10.1007/978-3-319-16507-3_3.

Whelan, C., 2017. Security networks and occupational culture: Understanding culture within and between organisations. *Policing and Society*, 27(2), pp. 113-135. 10.1080/10439463.2015.1020804.

Whitman, M.E., 2003. Enemy at the gate: Threats to information security. *Communications of the ACM*, 46(8), pp. 91-95. 10.1145/859670.859675.

Wiley, A., McCormac, A. & Calic, D., 2020. More than the individual: Examining the relationship between culture and Information Security Awareness. *Computers & Security*, 88(1), pp. 101640. 10.1016/j.cose.2019.101640.

Willaby, H.W., Costa, D.S., Burns, B.D., MacCann, C. & Roberts, R.D., 2015. Testing complex models with small sample sizes: A historical overview and empirical demonstration of what partial least squares (PLS) can offer differential psychology. *Personality and Individual Differences*, 84(1), pp. 73-78. 10.1016/j.paid.2014.09.008.

Wilson, M. & Hash, J., 2003. *Building an information technology security awareness and training program: National Institute of Standards and Technology (NIST) Special Publication*. Washington: U. S. Government Printing Office.

Wold, H., 1975. Path models with latent variables: The NIPALS approach. In: H.M. Blalock, A. Aganbegian, R. Boudon & V. Capecchi, eds. *Quantitative sociology*: *International Perspectives on Mathematical and Statistical Modeling.* United Kingdom: Academic Press Inc London, pp. 307-357. 10.1016/B978-0-12-103950-9.50017-4.

Wold, H., 1982. Soft modelling: The basic design and some extensions. In: K.G. Jöreskog & H. Wold, eds. *Systems under indirect observations: Part II.* Amsterdam: North-Holland, pp. 36-37.

Wolf, E.J., Harrington, K.M., Clark, S.L. & Miller, M.W., 2013. Sample size requirements for structural equation models: An evaluation of power, bias, and solution propriety. *Educational and Psychological Measurement*, 73(6), pp. 913-934. 10.1177/0013164413495237.

Wong, K.K., 2019. *Mastering partial least squares structural equation modeling (PLS-SEM) with Smartpls in 38 Hours*. USA: IUniverse.

Wong, W.P., Tan, H.C., Tan, K.H. & Tseng, M.L., 2019. Human factors in information leakage: Mitigation strategies for information sharing integrity. *Industrial Management & Data Systems*, 119(6), pp. 1242-1267. 10.1108/IMDS-12-2018-0546.

Wylder, J.O., 2003. Improving security from the ground up. *Information Security Journal: A Global Perspective*, 11(6), pp. 29-38. 10.1201/1086/43324.11.6.20030101/40429.6.

Yoo, K.H., Zhang, Y.A. & Yun, E.K., 2019. Registered Nurses (RNs)' knowledge sharing and decision-making: The mediating role of organizational trust. *International Nursing Review*, 66(2), pp. 234-241. 10.1111/inr.12488.

Zafar, H., 2013. Human resource information systems: Information security concerns for organizations. *Human Resource Management Review*, 23(1), pp. 105-113. 10.1016/j.hrmr.2012.06.010.

Zakaria, O., 2006. Internalisation of information security culture amongst employees through basic security knowledge. In: S. Fischer-Hübner, K. Rannenberg, L. Yngström & S. Lindskog, eds. *Security and Privacy in Dynamic Environments. Proceedings of the IFIP TC-11 21st International Information Security Conference (SEC 2006). Karlstad, Sweden, 22-24 May.* New York: Springer, pp. 437-441. 10.1007/0-387-33406-8_38.

Zakariya, N.I. & Kahn, M., 2015. Safety, security and safeguard. *Annals of Nuclear Energy*, 75(1), pp. 292-302. 10.1016/j.anucene.2014.08.051.

Zakon o pacientovih pravicah (ZPacP), 2008. Uradni list Republike Slovenije št. 15.

Zakon o varstvu osebnih podatkov (ZVOP-1), 2007. Uradni list Republike Slovenije št. 94, p. 12711.

Zbornica zdravstvene in babiške nege Slovenije - Zveza strokovnih društev medicinskih sester, babic in zdravstvenih tehnikov Slovenije, 2019. *Register izvajalcev zdravstvene*

ali babiške nege in licenca. [online] Available at: https://www.zbornica-zveza.si/register-licence-javna-pooblastila/register/ [Accessed 23 March 2022].

Zhang, J., Reithel, B.J. & Li, H., 2009. Impact of perceived technical protection on security behaviors. *Information Management & Computer Security*, 17(4), pp. 330-340. 10.1108/09685220910993980

Zohar, D. & Luria, G., 2005. A multilevel model of safety climate: Cross-level relationships between organization and group-level climates. *Journal of Applied Psychology*, 90(4), pp. 616-628. 10.1037/0021-9010.90.4.616.

Zohar, D. & Hofmann D.A., 2012. Oganizational culture and climate. In: S.W.J. Kozlowski, ed. *The Oxford Handbook of Organizational Psychology*. New York: Oxford University Press, pp. 643-666.

10 PRILOGE

Priloga 1 – Pregled literature

Priloga 2 – Kvalitativna preliminarna raziskava

Priloga 3 – Profil udeležencev raziskave

Priloga 4 – Vprašalnik

Priloga 5 – Faktorska analiza za TPB konstrukte

Priloga 6 – Faktorska analiza za dimenzije

Priloga 7– Factor loadings (cross loadings)

Priloga 8 – Crombah alpha

Priloga 9 – Protokol za zaščito podatkov pridobljenih med raziskavo

Priloga 10 – Sklep Zbornice – Zveze

Priloga 11 – Ocena etičnosti raziskave

Priloga 12 – Dovoljenje za uporabo vprašalnika

Priloga 13 – Preverjanje pristranosti zaradi uporabe ene metode

Priloga 14 – Izračun povezanosti dimenzij in spremenljivke starost

Priloga 15 – Izračun povezanosti dimenzij in spremenljivke delovna doba v organizaciji

Priloga 16 – Man Whitneyev U-test

10.1 PREGLED LITERATURE

Tabela: Analiza prejšnjih raziskav

Study	Domain	Country	ISC factors	ISC operationalization
Martins & Eloff (2002)	IT	*N/A*	*Organisation level* (policy & procedures, benchmarking, risk analysis, budget) *Group level* (management, trust) *Individual level* (awareness, ethical conduct)	Formed by ISC factors
Chan, et al. (2005)	Logistics, petrochemical	*N/A*	Co-worker socialization, direct supervisory practices, upper management practices	Perception of information security climate (i.e., manifestation of ISC culture)
Knapp, et al. (2006)	Various, including healthcare (5.1%)	23 countries	Top management support	Security culture
Da Veiga, et al. (2007)	Finance	*N/A*	Management of information security, performance management, performance accountability, communication, governance, capability development	Formed by ISC factors
Brady (2010)	Healthcare	US	*None*	Security culture
Da Veiga & Eloff (2010)	IT	South Africa	Leadership and governance, security management and operations, security policies, security programme management, user security management, technology protection and operations, change	Formed by ISC factors
Gebrasilase & Lessa (2011)	Healthcare	Ethiopia	Knowledge to information security, management of information security, communication, governance, performance accountability	Formed by ISC factors
Alnatheer, et al. (2012)	Various, including healthcare (8.3%)	Saudi Arabia	Top management involvement in information security, information security policy enforcements, information security training	*Security culture* (second order): information security awareness, information security ownership

Study	Domain	Country	ISC factors	ISC operationalization
D'Arcy & Greene (2014)	Various, including healthcare (7.9%)	US	Top management commitment, security communication, computer monitoring	Formed by ISC factors
Narain Singh, et al. (2014)	Various	India	*None*	ISC
Chen, et al. (2015)	*N/A*	US	Security policies, SETA programs, security monitoring	Security culture
Parsons, et al. (2015)	*N/A*	Australia	*None*	Organisational information security culture
Safa, et al. (2015)	Various, including healthcare (11.8%)	Malaysia	*None*	*ISC* (dimensions): information security awareness, organization policy
Hayden (2016)	Various	*N/A*	*None*	Security culture diagnostic survey
Rocha Flores & Ekstedt (2016)	Various, including healthcare (1.0%)	Sweden	Transformational leadership	ISC
Amankwa, et al. (2018)	Various, including healthcare	Ghana	Supportive organizational culture, information security policy compliance leadership, end-user involvement	*Information security policy compliance culture* (dimensions): attitude towards compliance with information security policy, information security policy compliance behavioural intention, information security policy compliance culture
Da Veiga (2018)	Finance	12 countries	*None*	*ISC* (dimensions): information security necessity and importance, information security accountability, management buy-in, information security policy effectiveness, information security commitment, information usage perception

Study	Domain	Country	ISC factors	ISC operationalization
Nasir, et al. (2019a)	Higher education	Malaysia	*None*	*ISC* (second order): procedure countermeasures, risk management, SETA, top management commitment, monitoring, information security knowledge, information security knowledge sharing
Sarbaz, et al. (2019)	Healthcare	Iran	*None*	*Organizational culture* (dimensions): managers' support, normative beliefs
Wong, et al. (2019)	Various	Malaysia	Education, training and awareness programs	ISC (several examples)
Kessler, et al. (2020)	Healthcare	*N/A*	*None*	*Information security climate* (dimensions): practices, importance, laxness
Dong, et al. (2021)	Healthcare	Malaysia	*None*	*Organizational climate* (dimensions): top management beliefs about IS security issues, organization's control of IS security issues
Pridmore & Oomen (2021)	Healthcare	*N/A*	*None*	Security culture / Security-oriented culture
Sari, et al. (2021)	Healthcare	Indonesia	*None*	Organizational culture

10.2 KVALITATIVNA PRELIMINARNA RAZISKAVA

Priloga 2 sestoji iz več poglavij, ki si sledijo po spodaj navedenem vrstnem redu:

- opis namena in poteka raziskave,
- prošnja za izvedbo raziskave,
- soglasje za izvedbo raziskave,
- soglasje subjektov za sodelovanje v raziskavi,
- vprašanja za intervju (instrument),
- nabor dejavnikov vpliva na vedenje – intervju (instrument),
- opis vzorca in evidenca opravljenih intervjujev,
- transkripti intervjujev.

OPIS NAMENA IN POTEK IZVEDBE PRELIMINARNE KVALITATIVNE RAZISKAVE

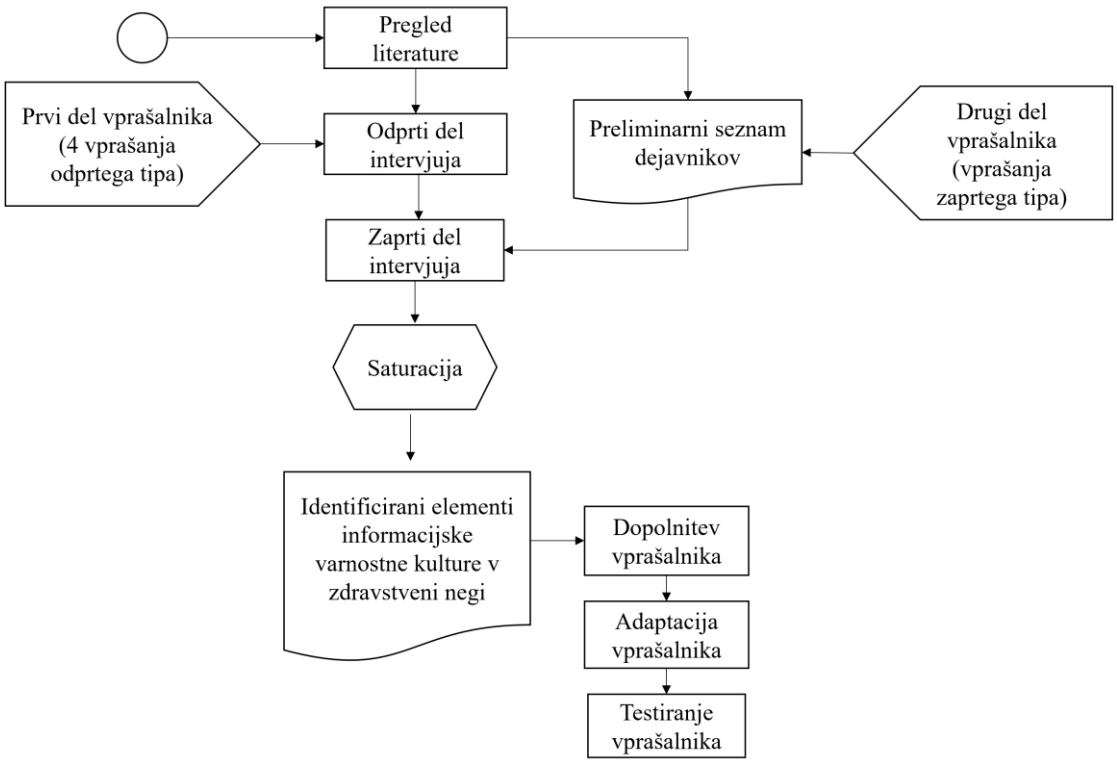
Da bi oblikovali vprašalnik za raziskovalni model, smo izvedli preliminarno kvalitativno (preiskovalno/eksplorativno) raziskavo (glej sliko). Njen namen je bil identifikacija morebitnih specifičnih dejavnikov informacijske varnostne kulture, značilnih za področje zdravstva/zdravstvene nege.

Raziskovalno vprašanje, na katerega smo pri tem poskušali odgovoriti, se glasi: »*Ali poleg splošnih, v literaturi identificiranih dejavnikov informacijske varnostne kulture obstajajo še specifični dejavniki značilni za področje zdravstva/zdravstvene nege in kateri so?*«.

Enote v vzorcu so bile izbrane subjektivno na osnovi presoje raziskovalca, z namenom, da bi izbrani posamezniki o proučevani zadevi lahko dali kar največ podatkov, kar bi omogočilo poglobljeno kvalitativno analizo. Opravljenih in posnetih (kot zvočni zapis) je bilo 17 intervjujev z zaposlenimi v zdravstveni negi ter informatiki iz kliničnega okolja. Uporabili smo namensko vzorčenje.

Instrument preliminarne kvalitativne raziskave je vprašalnik za podporo intervjuvanju, ki sestoji iz dveh delov: prvi del zajema štiri vprašanja odprtega tipa, drugi del vprašanja zaprtega tipa. Z drugim delom vprašalnika, ki vključuje trditve smo preverili učinek splošnih, v literaturi identificiranih dejavnikov informacijske varnostne kulture. S pridobljenim naborom dejavnikov smo dopolnili in prilagodili že obstoječi vprašalnik avtorjev Nasir, et al. (2019a).

Intervjuje smo posneli z diktafonom. Posamezen intervju je trajal okvirno 10–15 minut. Sledila je izdelava transkriptov. Omenjene smo prenesli v orodje ATLAS.ti 6 (Friese, 2013), s pomočjo katerega smo oblikovali kode in kategorije. Identificirana je bila dodatna dimenzija informacijske varnostne kulture – PO.



Slika: Potek preliminarne kvalitativne raziskave

PROŠNJA ZA IZVEDBO PRELIMINARNE KVALITATIVNE RAZISKAVE

assoc. prof. dr. Boštjan Žvanut
University of Primorska
Polje 42
6310 Izola
Slovenia

assoc. prof. dr. Zala Jenko Pražnikar
Commission for Scientific Research Work
University of Primorska
Faculty of Health Sciences
Polje 42
6310 Izola
Slovenia

Izola, 4 November 2019

Subject: Approval for research proposal entitled »The dimensions of information security culture in nursing: a qualitative study«

On behalf of our former student Mrs. Samanta Mikuletič, RN, MSc, we are kindly asking you for the approval to perform the study entitled »The dimensions of information security culture: a qualitative study«. In the appendix 1 the details of the study are presented. The current study represents a preliminary study to her final PhD thesis in order to identify, which information security culture determinants are relevant for this field.

Look forward for your positive response.

Sincerely,

assoc. prof. dr. Boštjan Žvanut

Appendices:

- Appendix 1 – The details of the study
- Appendix 2 – Open ended questionnaire
- Appendix 3 – Closed ended questionnaire

Appendix 1 – Study details

Adequate information security culture is a fulcrum for reducing information security threats and preventing information security breaches. Several studies define information security culture by considering different legal, organisational and technical factors. As the nursing profession is also ethically-driven, such a narrow definition does not reflect the actual state in this field.

Healthcare data represents one of the most sensitive and confidential personal data, which illicit exposure leads to unprecedented legal and financial consequences (Johnson, 2009). Furthemore, besides financial and legal responsibility also their ethical and moral responsibility becomes of paramount importance (Price & Cohen 2019). The improper disclosure or misuse of health information can cause serious reputational harm to the patient(s) e.g. discrimination, stigmatization, loss of insurance and/or employment.

Despite the fact there are several studies addressing the information security culture determinants in different fields, the results of literature review indicate there are no similar in the field of nursing. Hence we posed the following **two research questions**:

- Which determinants of information security culture are perceived as relevant for nurses?
- Are in the field of nursing present any other particular/specific information security culture determinants?

Design: The interviews will be performed with nurses working in clinical environment and other relevant employees (e.g. IT experts working with nurses). Two questionnaires, one with open and the other with closed-ended questions will be used as a reference for conducting the interviews.

Instruments:

- Appendix 2 – Open ended questionnaire
- Appendix 3 – Closed ended questionnaire

Settings: The interviewees will be invited to the face-to-face or online meeting, where open- and closed-ended questionnaire will serve as a reference for the interviews. We expect that the data will be collected from November 2019 to May 2020 (expected).

Ethical consideration: Before beginning the interview the participants will be informed about the purpose of the study, receive the study details and sign the informed consent (if they agree with it). The questionnaires do not address the participants' organisation as they refer to fictive characters: Marina & Matjaž.

Participants: We expect a maximum of cca. 20 interviewees in order to obtain the data saturation from their responses. No patients or any other fragile groups will participate in the study.

Expected results: We expect to identify the nursing-specific determinants of information security culture - ethical elements of information security culture that are not adequately addressed in previous studies in this field. These should not be neglected when nursing practice is under consideration.

Other relevant information: This study represents a preliminary study for preparing the PhD thesis proposal under the supervision of Boštjan Žvanut, co-supervisor Brigita Skela Savič at the Fakulteta za zdravstvo Angele Boškin.

SOGLASJE ZA IZVEDBO PRELIMINARNE KVALITATIVNE RAZISKAVE

Zala Jenko Pražnikar, PhD, Assoc. Prof.
Commission for Scientific Research Work
University of Primorska
Faculty of Health Sciences
Polje 42
6310 Izola
Slovenia

Boštjan Žvanut, PhD, Assoc. Prof.
University of Primorska
Polje 42
6310 Izola
Slovenia

Izola, 11 November 2019

Subject: Decision of the Commission for Scientific Research Work at University of Primorska Faculty of Health Sciences

Dear dr. Žvanut,

The Commission for Scientific Research Work at University of Primorska Faculty of Health Sciences has reviewed and evaluated your research proposal entitled "The dimensions of information security culture in nursing: a qualitative study"

The present proposal meets all guidelines set for such research by the National Commission. Therefore, the research proposal is approved, and the research can begin. The research must be conducted following the principles of Helsinki-Tokyo Declaration (World Medical Association, 2013) and Code of Ethics for Nurses and Nurse Assistants of Slovenia (2014).

Best regards,

Zala Jenko Pražnikar, PhD, Assoc. Prof.
President of the Commission for Scientific Research Work

SOGLASJE SUBJEKTOV ZA SODELOVANJE V RAZISKAVI

Naslov (okvirni): Informacijska varnostna kultura medicinskih sester v RS

Raziskovalec: Samanta Mikuletič, doktorandka Fakultete za zdravstvo Angele Boškin

Mentor: izr. prof. dr. Boštjan Žvanut, Fakulteta za vede o zdravju

Naslov za kontakt: samanta.mikuletic@gmail.com

Prosimo, da si natančno preberete navedene informacije. Sodelovanje v raziskavi je prostovoljno. V kolikor se odločite sodelovati, slednje potrdite s podpisom.

- **Namen raziskave:** Namen raziskave je preučiti koncept informacijske varnostne kulture in skozi teoretični okvir Teorije načrtovanega vedenja razložiti pojav dejanj (posojanje gesel in nepooblaščen dostop do zdravstvenih podatkov) pri medicinskih sestrah. Omenjena vedenja pri medicinskih sestrah, v tujini in pri nas, še niso bila v celoti pojasnjena.
- **Potek raziskave:** Raziskava bo potekala v več fazah. Z Vami bo opravljen intervju. Raziskovalec Vam bo zastavil 4 vprašanja, ki so povezana z naravo vašega dela. Pogovor se bo za namen ustreznega zapisa in interpretacije informacij snemal (nastal bo avdio posnetek). Po končanem intervjuju Vam bomo ponudili krajši vprašalnik, ki vsebuje sklop trditev, ki se nanašajo na omenjeno temo.
- **Tveganja:** S sodelovanjem niste izpostavljeni tveganjem.
- **Koristi:** S sodelovanjem boste spoznali temeljne vzroke zaradi katerih prihaja do izvedbe kršenja varnosti zdravstvenih podatkov na področju zdravstvene nege.
- **Trajanje:** Intervju je ocenjen na trajanje 20 minut.
- **Zaupnost podatkov**: Vaše sodelovanje v raziskavi je, kljub temu, da se morate na koncu te izjave podpisati z imenom in priimkom, anonimno. Osebni podatki bodo kodirani. Avdio zapis bo shranjen pri avtorju (raziskovalcu) 7 let od

zaključka raziskave. Po tem času bodo zapisi uničeni. Zaupnost bo zagotovljena z geslom.

- **Prostovoljnost sodelovanja:** Sodelovanje v raziskavi je prostovoljno in ga lahko prekinete na katerikoli točki, brez kakršnih koli posledic.
- **Rezultati:** V kolikor boste ob koncu raziskave želeli biti seznanjeni z rezultati, Vam bomo to omogočili. Željo sporočite na zgoraj navedeni elektronski naslov.

Zahteva za sodelovanje v raziskavi je polnoletnost ter delovanje v kliničnem okolju zdravstvene nege oz. na področju informatike v zdravstvu. Za sodelovanje ne prejmete nobenih denarnih ali kakršnih koli drugih materialnih nadomestil.

V primeru, da se strinjate z zgoraj navedenimi informacijami in s sodelovanjem, to izrazite tako, da navedete vaše ime in priimek, datum in se podpišete.

Podpisani, _____ (ime in priimek), izjavljam, da:

- soglašam za sodelovanje pri raziskavi,
- sem predhodno seznanjen(a), da Samanta Mikuletič, doktorandka Fakultete za zdravstvo Angele Boškin, za namen doktorske disertacije, snema, uporablja in hrani posnetek intervjuja na temo informacijske varnostne kulture pri medicinskih sestrah v RS (okvirni naslov),
- se navedeni posnetki obdelujejo le za namen izvedbe raziskave, možnosti ponovnega kasnejšega poslušanja ter ustreznega zapisa in interpretacije informacij.

Skladno z zgornjim obvestilom dovoljujem in soglašam z obdelavo in uporabo posnetkov.

Podpis sodelujočega: Kraj in datum:

Oseba, ki je pridobila soglasje: Podpis:
Samanta Mikuletič

VPRAŠANJA ZA INTERVJU

Zamislite si Marino oz. Matjaža, oba DMS. Oba imata opravka s podatki pacientov. Če želita, imata možnost vpogleda v podatke vseh pacientov.

1. Kaj po vašem mnenju najbolj vpliva na to, da Marina oz. Matjaž **ne dostopata do podatkov** pacientov, za katere nista pooblaščena?
   [Kaj še?]

2. Kaj pa po vašem mnenju vpliva na to, da Marina oz. Matjaž **dostopata do podatkov** pacientov, za katere nista pooblaščena?
   [Kaj še?]

3. Kaj po vašem mnenju vpliva na to, da se vsak od njiju posebej odloči, **da bo posodil geslo**?
   [Kaj še?]

4. Kaj po vašem mnenju vpliva na to, da se vsak od njiju posebej odloči, **da ne bo posodil gesla**?
   [Kaj še?]

NABOR DEJAVNIKOV VPLIVA NA VEDENJE – INTERVJU

Koliko po vašem mnenju vplivajo spodaj navedeni dejavniki na to, da Marina oz. Matjaž **dostopata do podatkov pacientov, za katere nista pooblaščena**? Prosimo, da s pomočjo lestvice od 0 (sploh ne vpliva) do 10 (v veliki meri vpliva) ocenite, koliko po vašem mnenju navedeni dejavniki vplivajo na. na zgoraj navedeno trditev.

	0 Sploh ne vpliva	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10 V veliki meri vpliva**
Finančna ali osebna korist, ki jo lahko pridobita s podatki.	0	1	2	3	4	5	6	7	8	9	10
Slabo zavarovani podatki v informacijskem sistemu.	0	1	2	3	4	5	6	7	8	9	10
Nesankcioniranje.	0	1	2	3	4	5	6	7	8	9	10
Prošnja/nagovarjanje prijateljev (prijatelja zanimajo podatki o dotičnemu pacientu).	0	1	2	3	4	5	6	7	8	9	10
Prošnja/nagovarjanje svojcev (družinskega člana zanimajo podatki o dotičnemu pacientu).	0	1	2	3	4	5	6	7	8	9	10
Prošnja/nagovarjanje sodelavcev (sodelavca zanimajo podatki o dotičnemu pacientu).	0	1	2	3	4	5	6	7	8	9	10
Nelegitimna zahteva nadrejenega.	0	1	2	3	4	5	6	7	8	9	10
Nelegitimna zahteva/-e ostalih pacientov.	0	1	2	3	4	5	6	7	8	9	10

Koliko po vašem mnenju vplivajo spodaj navedeni dejavniki na to, da Marina oz. Matjaž **ne dostopata do podatkov pacientov, za katere nista pooblaščena**? Prosimo, da s pomočjo lestvice od 0 (sploh ne vpliva) do 10 (v veliki meri vpliva) ocenite, koliko po vašem mnenju navedeni dejavniki vplivajo na na zgoraj navedeno trditev.

	0 Sploh ne vpliva	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10 V veliki meri vpliva**
Posledice (npr. sankcije, ki sta jih lahko deležna, če ju ujamejo pri delu).	0	1	2	3	4	5	6	7	8	9	10
Pravilniki organizacije.	0	1	2	3	4	5	6	7	8	9	10
Zakonodaja.	0	1	2	3	4	5	6	7	8	9	10
Etika/morala oz. etični kodeks.	0	1	2	3	4	5	6	7	8	9	10
Pomanjkanje časa na delovnem mestu.	0	1	2	3	4	5	6	7	8	9	10
Računalniško omejevanje pravic dostopa do podatkov.	0	1	2	3	4	5	6	7	8	9	10
Revizijska sled oz. strah, da bi ugotovili, da sta nepooblaščeno dostopala do podatkov.	0	1	2	3	4	5	6	7	8	9	10
Mnenje prijateljev (prijatelji menijo, da tega ne smeta početi).	0	1	2	3	4	5	6	7	8	9	10
Mnenje svojcev (družinskega člana zanimajo podatki o dotičnemu pacientu).	0	1	2	3	4	5	6	7	8	9	10
Sodelavci (sodelavca zanimajo podatki o dotičnemu pacientu).	0	1	2	3	4	5	6	7	8	9	10
Strah pred nadrejenim.	0	1	2	3	4	5	6	7	8	9	10
Strah pred izgubo zaupanja s strani pacienta/-ov.	0	1	2	3	4	5	6	7	8	9	10
Izkušnje/pretekli dogodki (zaradi nepooblaščenega gledanja v podatke so kaznovali njo/njega oz. sodelavce).	0	1	2	3	4	5	6	7	8	9	10
Znanje (ker so ju učili, da ne smeta nepooblaščeno dostopati do podatkov).	0	1	2	3	4	5	6	7	8	9	10
Strokovni in znanstveni viri.	0	1	2	3	4	5	6	7	8	9	10
Množični mediji (časniki, spletni portali).	0	1	2	3	4	5	6	7	8	9	10
Varnostna politika.	0	1	2	3	4	5	6	7	8	9	10

Koliko po vašem mnenju vplivajo spodaj navedeni dejavniki na to, da Marina oz. Matjaž **ne posojata svojega uporabniškega imena in gesla za dostop v službeni informacijski sistem**? Prosimo, da s pomočjo lestvice od 0 (sploh ne vpliva) do 10 (v veliki meri vpliva) ocenite, koliko po vašem mnenju navedeni dejavniki vplivajo na na zgoraj navedeno trditev.

	0 Sploh ne vpliva	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10 V veliki meri vpliva**
Posledice (npr. sankcije, ki sta ju lahko deležna, če vodilni ugotovijo, da sta posojala geslo).	0	1	2	3	4	5	6	7	8	9	10
Pravilniki organizacije.	0	1	2	3	4	5	6	7	8	9	10
Zakonodaja.	0	1	2	3	4	5	6	7	8	9	10
Etika/morala oz. etični kodeks.	0	1	2	3	4	5	6	7	8	9	10
Računalniško omejevanje pravic dostopa do podatkov.	0	1	2	3	4	5	6	7	8	9	10
Revizijska sled oz. strah, da bi ugotovili, da sta nepooblaščeno dostopala do podatkov.	0	1	2	3	4	5	6	7	8	9	10
Mnenje prijateljev (prijatelji menijo, da tega ne smeta početi).	0	1	2	3	4	5	6	7	8	9	10
Mnenje svojcev (svojci menijo, da tega ne smeta početi).	0	1	2	3	4	5	6	7	8	9	10
Sodelavci (sodelavci menijo, da tega ne smeta početi).	0	1	2	3	4	5	6	7	8	9	10
Nadrejeni (nadrejeni meni, da tega ne smeta početi).	0	1	2	3	4	5	6	7	8	9	10
Pacienti (pacienti menijo, da tega ne smeta početi).	0	1	2	3	4	5	6	7	8	9	10
Izkušnje/pretekli dogodki (zaradi nepooblaščenega gledanja v podatke so kaznovali njo/njega oz. sodelavce).	0	1	2	3	4	5	6	7	8	9	10
Znanje (ker so ju učili, da ne smeta nepooblaščeno dostopati do podatkov).	0	1	2	3	4	5	6	7	8	9	10
Strokovni in znanstveni viri (narekujejo, da tega ne smeta početi).	0	1	2	3	4	5	6	7	8	9	10
Množični mediji (časniki, spletni portali). narekujejo, da tega ne smeta početi.	0	1	2	3	4	5	6	7	8	9	10
Varnostna politika.	0	1	2	3	4	5	6	7	8	9	10

Koliko po vašem mnenju vplivajo spodaj navedeni dejavniki na to, da Marina oz. Matjaž **posojata svoje uporabniško ime in geslo za dostop v službeni informacijski sistem**? Prosimo, da s pomočjo lestvice od 0 (sploh ne vpliva) do 10 (v veliki meri vpliva) ocenite, koliko po vašem mnenju navedeni dejavniki vplivajo na zgoraj navedeno trditev.

	0 Sploh ne vpliva	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10 V veliki meri vpliva**
Prošnja sodelavca (sodelavec je pozabil svoje geslo).	0	1	2	3	4	5	6	7	8	9	10
Grožnja sodelavca (sodelavec je pozabil svoje geslo).	0	1	2	3	4	5	6	7	8	9	10
Prošnja zdravnika (zdravnik specializant je pozabil svoje geslo).	0	1	2	3	4	5	6	7	8	9	10
Grožnja zdravnika (zdravnik, specializant je pozabil svoje geslo).	0	1	2	3	4	5	6	7	8	9	10
Narava dela (ostaneta prijavljena, saj je odjavljanje in prijavljanje v sistem zamudno, npr. urgenca).	0	1	2	3	4	5	6	7	8	9	10
Nesankcioniranje.	0	1	2	3	4	5	6	7	8	9	10

Zahvaljujemo se Vam za sodelovanje.

OPIS VZORCA IN EVIDENCA OPRAVLJENIH INTERVJUJEV

Tabela: Značilnosti vzorca kvalitativne raziskave

Datum	Šifra	Spol	Starost	Izobrazba	Zaposlitev
23. 11. 2019	TN	ženski	1993	dipl. m. s.	dipl. m. s. v urgentni dejavnosti na sekundarnem zdravstvenem nivoju
25. 11. 2019	UV	ženski	1993	dipl. m. s.	dipl. m. s. v centralni intenzivni terapiji III – terciarni zdravstveni nivo
4. 12. 2019	DT	ženski	1991	TZN	tehnik zdravstvene nege na sekundarnem zdravstvenem nivoju
5. 12. 2019	KML	ženski	1974	dr. znanosti	glavna medicinska sestra na terciarnem zdravstvenem nivoju
5. 12. 2019	MT	moški	1974	informatik	sekundarni in terciarni zdravstveni nivo
5. 12. 2019	BV	moški	1976	informatik	sekundarni in terciarni zdravstveni nivo
9. 12. 2019	DS	moški	1976	mag. zdr. nege	dipl. zn. na primarnem zdravstvenem nivoju
10. 12. 2019	KK	ženski	1989	TZN	tehnik zdravstvene nege na sekundarnem zdravstvenem nivoju
15. 12. 2019	TMS	ženski	1972	mag. zdr. nege	glavna medicinska sestra specialistične bolnišnice
15.12. 2019	KT	ženski	1990	mag. zdr. nege	dipl. m. s. na primarnem zdravstvenem nivoju
30. 12. 2019	LF	moški	1976	informatik	sekundarni zdravstveni nivo
23. 1. 2020	PP	moški	1980	informatik	visokošolski učitelj visoke zdravstvene šole
3. 2. 2020	HS	ženski	1960	višja med. sestra	visokošolski učitelj, več let izkušenj na sekundarnem zdravstvenem nivoju
4. 2. 2020	SM	ženski	1984	mag. zdr. nege	visokošolski učitelj, več let izkušenj na sekundarnem zdravstvenem nivoju
22. 4. 2020	DZ	moški	1987	mag. zdr. nege	dipl. zn. na primarnem zdravstvenem nivoju
17. 5. 2020	RC	moški	1990	dipl. zn.	dipl. zn. na primarnem zdravstvenem nivoju
22. 6. 2020	PD	ženski	1993	mag. zdr. nege	dipl. m. s. na sekundarnem in terciarnem zdravstvenem nivoju

TRANSKRIPTI INTERVJUJEV

Šifra: TN **Datum:** 23. 11. 2019 **Spol:** ženski **Leto rojstva:** 1993 **Izobrazba:** dipl. m. s. **Zaposlitev:** dipl. m. s. na sekundarnem zdravstvenem nivoju	Na to, da Matjaž in Marina ne dostopata do podatkov pacientov, za katere ne skrbita, po mojem mnenju vpliva mnenje drugih … Če bodo ostali izvedeli, da sta dostopala do podatkov za katere nista pooblaščena – kaj bodo drugi mislili o njih … ? Morata biti fer. Npr. če gre dotična oseba, je to dejanje ok, če gre neka druga, potem izpadeš najslabši človek. Npr. Matjaž ne bo nepooblaščeno dostopal do podatkov, zato ker tudi sam ne želi, da bi kdo drug gledal njegove zdravstvene podatke. Nepooblaščeno ne bi dostopala tudi zaradi kazni. Nisem pa še slišala, da bi kdo odgovarjal za kako tako dejanje. Verjetno najbolj vpliva denar oz. izguba službe. Nepooblaščeno bi dostopala zaradi firbca – zanimanja, da bi dobila informacije sebi ali pa drugim, prijateljem ali pa sorodnikom, sosedom (ker vedno sprašujejo … ej ej ... kaj veš kje uni je?) … Zakaj se na primer pri nas posoja geslo … Ko se enkrat prijaviš, imaš potem še več prijav in je to enostavnejše – da je samo eden prijavljen. Ne vem, mogoče če bi Matjaž pozabil geslo in je zaupanja vreden in prijazen, mu ga posodimo. Včasih zdravnik s svojim geslom ne more dostopati do določenih podatkov in nam reče, da se prijavimo. Matjaž in Marina bi se lahko zavedala posledic posojanja gesla … Če bi nekdo drug dostopal do nekih podatkov … bo vse napisano na njihovo ime … V smislu, da sta ona dva gledala …
Šifra: UV **Datum:** 25. 11. 2019 **Spol:** ženski **Leto rojstva:** 1993 **Izobrazba:** dipl. m. s **Zaposlitev:** dipl. m. s. na terciarnem zdravstvenem nivoju	Marina in Matjaž ne bosta nepooblaščeno dostopala do podatkov pacientov za katere ne skrbita, ker onadva ne skrbita za te paciente in ti pacienti niso na njihovem oddelku – v informacijskem sistemu nimata dostopa. V Birpis sistemu imata zaprta nekatera področja. Jaz npr. ne morem dostopat do vseh, nimam dostopnih pravic. Če bi imela dostopne pravice, bi šla oba zaradi firbca gledat podatke – zgolj firbec! Na svojem oddelku lahko oba dostopata do podatkov pacientov na njihovem oddelku in lahko vse pogledata, vesta kaj se z njimi dogaja. Npr. če je Marina dežurna, mora vedeti, kaj se z vsemi pacienti dogaja, ne rabi pa vedeti o pacientih, ki ležijo na abdomnu. Če bi nekoga poznala, bi lahko dostopala s svojim geslom do podatkov, ampak če nima dostopa, v tem primeru to ne bi mogla. Lahko jo prosi za podatke tudi nekdo drug. Ampak spet je to zgolj firbec. Geslo bi Marina in Matjaž posodila, če bi ju kdo prosil, ali pa da je nekdo na novo zaposlen, ki gesla še nima, ga je izgubil. Načeloma so vsi striktno pod svojim geslom in se tudi odjavimo potem oz. če se ne odjaviš, te odjavi računalnik sam po 120 sekundah. Gesla ne bosta posodila, ker je geslo njuno, na njuno ime in zato v informacijskem sistemu vejo, da sta ona dva dostopala, pa čeprav ona dva nista bila …
Šifra: DT **Datum:** 4. 12. 2019 **Spol:** ženski **Leto rojstva:** 1991 **Izobrazba:** TZN **Zaposlitev:** TZN na sekundarnem zdravstvenem nivoju	Marina in Matjaž ne bosta šla gledat podatkov pacientov za katere nista skrbela samo, če ne bosta imela dostopa. Ni prav, da se gleda podatke drugih ljudi. Pogledala bosta v podatke …, ker grejo itak vsi pogledat. Razlog je firbec ... mogoče je tudi, da kaj prodajo, npr. novinarjem. Če bosta gledala nekega pacienta oz. njegove podatke, npr. Marina preko Matjaževega gesla, gre lahko Matjaž v zapor … Moral bi paziti svoje geslo. Morda je posodil geslo, ker nekdo drug nima gesla, lahko tudi zaradi tega, ker mu ga šef ni dodelil. Mi smo včasih imeli za en oddelek samo eno geslo. In to geslo smo uporabljali vsi in vsepovsod … Četudi je človek šel na drugo delovno mesto oz. drug oddelek. Isto geslo je imel še naprej. In to isto geslo te osebe smo mi še vedno uporabljali na oddelku, tudi npr. če je bila ta oseba na bolniški ali porodniški. Primer: naš bivši sodelavec dela sedaj v ustanovi X, mi pa smo še vedno uporabljali njegovo geslo npr. za naročanje sterilizacije. Na xxx oddelku in xxx oddelku smo vsi imeli geslo od ene sodelavke in smo 4 leta preko njenega gesla delali vsi. Dostop smo imeli do vseh kirurških oddelkov. Njeno geslo smo uporabljali, ker nismo imeli svojega. Jaz sem dobila svoje geslo za dostop po treh letih od kar sem se zaposlila. Geslo za sterilizacijo pa sem dobila 6 let po začetku službe. Vodilne smo silili v to, da nam dodelijo geslo, vendar nam ga niso dali. Rekli so nam, da ga ne potrebujemo …

Šifra: KML
Datum: 5. 12. 2019
Spol: ženska
Leto rojstva: 1974
Najvišja dosežena izobrazba: doktorica znanosti
Zaposlitev: glavna medicinska sestra na terciarnem zdravstvenem nivoju

Marina in Matjaž ne dostopata do podatkov pacientov za katere ne skrbita zaradi pomanjkanja časa na delovnem mestu. Če sam sebe nekdo vpraša, kaj bi se zgodilo, če bi ta zadeva prišla v javnost ali pa da bi ta zadeva prišla do pacienta oziroma do njegovih svojcev? Kakšne bodo posledice za Marino oziroma za Matjaža oziroma posledice za ustanovo, kjer sta zaposlena? V vsaki ustanovi so pravilniki in tudi seveda po mojem mnenju etično-moralnih vrednot, ki jih ima posameznik. S tem da jaz pričakujem, da ljudje, ki so diplomirali, da so se srečali pri svojem študiju z osnovnimi načeli kakovosti v zdravstvu in eno od teh šestih načel kakovosti v zdravstvu je tudi varnost – varnost pacienta, varnost v zdravstvu. In to tudi pomeni odsotnost kakršnih koli posledic za paciente, za zaposlene ali drugih, zaradi varnostnih odklonov. Pomembna se mi zdi tudi strokovna avtonomija in kaj pomeni sprejemanje odgovornih odločitev, na podlagi osebnih značilnosti in pa znanja, pa tudi odvisno od položaja … Če še malo razmišljam ... Na primer klinične poti, če se srečaš s kliničnimi potmi, ti ponudijo odgovor kdo, kdaj in kaj je recimo naredil pri določenem pacientu. Pri tem bi se osredotočila tudi na to, da ima vsaka organizacija, predvidevam kulturo varnosti. Vsaka oseba, ki je v zavodu priznava svojo odgovornost glede varnosti pacientov. Značilnost zdravstvene obravnave je tudi, da imamo veliko količino podatkov in s tem tudi osebnih podatkov o pacientih in je posledično tudi veliko dokumentiranja in zato mislim, da je pri tem procesu potrebno poskrbeti za kakovostno in varno obravnavo pacientov. Tukaj bi opomnila tudi na načelo, ki naj bi veljalo – varstvo osebnih podatkov. Opozorila bi tudi na to, da izvajalci zdravstvene dejavnosti za zagotavljanje zakonitosti, strokovnosti in kakovosti in tudi varnosti dela lahko opravljajo razne vrste nadzora. In takrat lahko te nepravilnosti pokukajo na plano. Če to pride do pacientov ali svojcev, lahko uveljavljajo tudi pravico do obravnave kršitev pacientovih pravic. To je vedno, kadar menijo, da je do kršitve prišlo. Tu imajo tudi pravico do sodnega varstva. Na prvem mestu, da Marina in Matjaž dostopata do podatkov za katere nista pooblaščena, je to, da se ne zavedata posledic, ne poznata pravilnika, ne poznata kakovostne obravnave varnosti pacientov, mogoče sta radovedna, imata premalo znanja ali pa imata neko osebno korist. Mogoče je, da ju nekdo prosi za neki podatek. Lahko je to nek sorodnik, ki ga skrbi za prijatelja in potem vpraša ali mu lahko nekdo nekaj pove. Glede posojanje gesel … Nekdo je lahko v stiski, ker mu mogoče nadrejeni ne pokaže ali pa mu ne da nekega navodila: »Glej moraš dat geslo meni ali pa sodelavcu, ker ga je pozabil …«. Lahko je geslo pozabil tudi zdravnik. Tukaj je lahko medicinska sestra v manj vrednem položaju – ali bo posodila ali ne bo posodila geslo zdravniku? Menim, da posameznik v nobenem primeru ne bi izkoristil oziroma zlorabil svojih pooblastil za neka dejanja, ki pomenijo kršitev varstva osebnih podatkov. Zakaj ne posodiš gesla? – to je lahko omejeno glede kompetenc zaposlenih. Računalniško orodje prepreči ali pa omeji dostop do vseh podatkov. Gesla ne posodiš zaradi nadzorov ali revizij. Kon'c koncev, tudi če te nekdo vpraša, jaz pričakujem potem od njega nek odgovor, ki utemelji, zakaj tisti, ki od mene ta podatek zahteva, zakaj ga potrebuje, kako ga bo hranil in kaj bo s tem podatkom počel. V današnjem času naj bi bili vsi, ki smo formalno izobraženi na prvi stopnji, seznanjeni z GDPR-jem, ki je začel veljati, mislim da 25. 5. 2016, uporablja pa se ga od 2018. leta. In v njem je podatek opredeljen kot katera koli informacija v zvezi z določenim ali določljivimi posamezniki. Če se zavedamo GDPR-ja, potem jaz mislim, da ne vem, če se lahko kaj dosti igramo s temi zadevami, ker lahko pride tudi do postopkov v primeru kršitve varstva zdravstvenih podatkov – torej postopek pred izvajalcem zdravstvene dejavnosti, postopek s tožbo pred sodiščem, kar je civilni postopek in nato še kazenski postopek. Torej, če se nekdo tega zaveda in kam te ta zadeva lahko pripelje …

Šifra: MT
Datum: 5. 12. 2019
Spol: moški
Leto rojstva: 1974
Najvišja dosežena izobrazba: univerzitetna
Zaposlitev: informatik v bolnišnici

Marina in Matjaž ne dostopata do podatkov za katere nista pooblaščena, četudi so jima na voljo (podatki niso zaščiteni, niti z gesli, niti v zaklenjeni omarici, v primeru papirnate kartoteke pacienta). Če razdelamo najprej situacijo, ko oba nimata preprečenega dostopa in tudi nista bila osveščena o tem, da ne smeta dostopati. V tem primeru se v veliki meri izrazi človeška drža oziroma človeški nagon – vedoželjnost, ki se pomoje spotencira s tem, da subjekt bolj ali manj pozna. Če podam dva primera … Če na oddelku leži sosed Francelj ali pa leži nekdo, ki ga ta Marina in Matjaž poznata, je za soseda Francelja veliko večja verjetnost, da bosta vpogledala ali pa ciljno poiskala njegove podatke, kot pa če bi šlo za popolnoma nepoznano osebo. Bolj kot je oseba poznana, bolj kot je domača, večja verjetnost je, da se ta vedoželjnost izrazi. Obstaja še en vidik, ki bi ga omenil … – naročilo. Leži sosed Francelj, soseda Francka pa bi rada kaj vedela o njem. Pa je v bistvu sestra oz. delavec medij – transportni medij, zato, da se nekaj teh podatkov izve. Nekaj podatkov lahko dobi, da ga nekaj vpraša, nekaj jih dobi tako, da nekaj podatkov pogleda. Potem je že ona dokaj dober serviser zato, da nekomu obrazloži situacijo za tega pacienta. Če Marina in Matjaž vesta, da imata dostop – torej nimata neke prepreke, ampak istočasno vesta, da tega ne smeta početi … Bi bilo zanimivo vedeti, v kakšnem odstotku je to lahko razlog, da tega ne bosta storila. Ona dva si želita to pogledat, vendar po drugi strani se zavedata posledic. Če sta še malo bolj osveščena in se zavedata, da potencialno obstaja neka revizijska sled, je tukaj lažja zgodba pogledam papir. Papir zagotovo nima kamere, pogledam … In nimam nobenega dokaza proti sebi, da sem to pogledal. Če pa se bojim revizijske sledi in se zavedam, da potencialno obstaja oz. da celo mora biti, v takem primeru je to še dodaten motiv, da ne bom pač pogledal. Zdaj pa še primer, ko jim je v resnici tudi to preprečeno … Da bi pa šla v zaklenjeno omaro, kjer vesta, da nimata ključa iskat možnost oz. zaobit svoje pravice uporabnika in izrabit zdravnika, za to, da bi to pogledala … Bi morali biti motivi že zelo, zelo veliki … Ki pa si jih v resnici v sedanjem življenju niti ne predstavljam. Da se nekdo odloči, da posodi geslo – vedno izhajamo iz situacije, da se uporabnik ne zaveda v resnici vseh tveganj, ki jih povzroči z izposojo lastnega gesla. Ko on tehta morebitno škodo pri izposoji ali pa pri izročitvi svojega gesla in korist, ki jo v tistem trenutku vidi za sam proces dela, se velikokrat zgodi, da uporabnik enostavno izroči vse svoje uporabniške pravice z namenom, da bi rad pokazal konstruktivno držo do kolega. In to zgleda tako ... Dej ti …, sam lej … Js sm … Ne morem zdej, informatike ni, nimam podpore … Dej mi pomagaj …, moram delat …, meni ne dela moje geslo … In ona reče: glej, tu maš moje, jaz grem domov – tak primer. In on dobi občutek, da je kolegu rešil popoldan in dobi občutek, da kolega bi tudi zanj naredil isto in dobi občutek, da to ni nič takšnega. Ne predstavljam si situacije, ko bi se uporabnik zavedal vseh težkih okoliščin, ki lahko potem sledijo zaradi tega dejanja in tako vseeno ravna. Na to, da Matjaž ali Marina ne posodita gesla, vpliva po moje dvoje … Po eni strani zavedanje, kaj vse lahko počne in kje vse so potem revizijske sledi. Včasih pa je tudi občutek, v smislu – nekateri ljudje pač nečesa svojega enostavno ne dajo, pa niti se ne obremenjujejo s tem ali razumejo prav dobro zakaj ne. Vedo, da je to njihova lastnina in niso voljni jo odstopiti, čeprav morda ne vidijo vseh tistih posledic, ki bi jim potencialno škodile. Ampak enostavno tega ne naredijo. Nikoli ne bo posodil, če bo prebral precej težke pravilnike, če bo bil na izobraževanju, kjer mu bo bilo zelo jasno predstavljeno, da se tega ne sme narediti in da so posledice dovolj hude, dovolj težke. Tudi ne bo posodil, če bo dobil neko navodilo nadrejenega, da tega ne sme narediti v nobenem primeru. Velikokrat se pa zgodi, da samega uporabnika ne moti, da bi nekdo uporabil njegove pravice proti pacientu, ampak zmoti jih to, da uporabi njegove pravice proti njemu samemu. Kje se pa zlomi – to pa vem iz pričevanja drugih kolegov in iz drugih podobnih okolij. Vse je letelo povprek – gesla, user name in tako naprej, v trenutku, ko smo v Kadrisu, ki nima nobene zveze z bolnišničnim informacijskim sistemom, to je informacijski sistem za kadrovsko poslovanje in plačni sistem, uporabili isto geslo. Ko smo tam notri uporabnikom dali digitalne plače in ohranili isto geslo, ki je bilo pogoj za dostop do vseh podatkov pacientov in pa tudi do lastne plače, se je kultura drastično spremenila. To je izjemno lep pokazatelj…

Se nadaljuje

	Njega ni zanimalo, da on malo ne škodi pacientu. Ni se počutil niti ogroženega. Ampak to, da sedaj ima nekdo možnost prebrati mogoče njegov mail ali pa pravico pogledat njegovo plačno listo zelo podrobno … – to pa je spremenilo kulturo. To se mi zdi zelo zanimiv psihološki, realen moment. Dosti več boš naredil za zavarovat sebe, kot pa recimo druge.
Šifra: BV **Datum:** 5. 12. 2019 **Spol:** moški **Leto rojstva:** 1976 **Najvišja dosežena izobrazba**: magisterij **Zaposlitev:** informatik v bolnišnici	Pri tem, da Matjaž in Marina ne dostopata do podatkov pacientov, za katere ne skrbita je ključna etična drža. Da onadva ne dostopata do podatkov za katere tehnično imata dostop – zato ker se to ne sme. Taka drža mora biti v ponos. Onadva se morata počutiti dobro oz. ona dva se počutita dobro, ker sicer imata na razpolago huda orodja, ampak bistvo je v tem, da jih ne zlorabljata. Ta drža ni naravna. Vsekakor morata biti osveščena, izobražena v tej smeri. Nekdo jim mora pojasniti, zakaj to ni v redu odnos do podatkov. Onadva morata nekako to ponotranjiti. Ne gre zgolj za to, da bi se bala posledic. Enostavno morata to jemati, kot nekaj nedostojnega in se to pač ne počne. Motivacija za takšen dostop je lahko firbčnost, ali pa morda to osebo poznata in si zaradi tega najdeta neko moralno opravičilo. V smislu … Pa sej ni nič takega … Ne bi rekel brezbrižnost, bolj radovednost. Nekaj te mora spodbuditi … Vseeno je tukaj 300.000 podatkov pacientov in ne moremo vsakega posebej gledati in nekaj te mora spodbudit, saj ne moreš naključno gledati, npr. kot Google. Greš gledat točno določene osebe … Ali je to neka firbčnost ali pa si s to osebo nekako povezan in si najdeš moralno opravičilo, da je to v redu. Moja soseda je zgubljena in je že starejša in bom jaz pogledala kaj je z njo, ker ona itak ne razume nič. In ne da bi me to ona prosila. Ampak to je v bistvu neka lažna skrb. Marino in Matjaža bi spodbudil k posoji gesla kot pritisk nadrejenih, ampak ne neposreden, temveč posreden – pritisk, da je potrebno za vsako ceno zagotoviti, da proces nemoteno poteka. In to ni nujno, da so le nadrejeni, lahko je to tudi pritisk okolice. Ker vsi tako počnejo v enoti – kdo si ti, da boš ti ravnala drugače. Na delovnem mestu si ne predstavljam drugega razloga, da bi moral nekdo geslo posoditi, če to ne bi bilo povezano z nemotenim procesom dela. To ne opravičujemo, ampak če poteka neko delo, vsi so malo živčni, vsak dan je gužva točno ob treh in dej … Si rešila ali nisi rešila? … Pusti prižgan računalnik … itd. Nekako tako, bi rekel oz. v tem smislu. Ne razumem pa tega vprašanja, da bi en kader posojal gesla nekomu drugemu, ki nima dostopa do teh podatkov … Tega si ne predstavljam. Da se potem tukaj meša in briše revizijska sled, pa se lahko zgodi – iz istovrstnega kadra bi rekel. Na to, da ne bi posodila gesla, vpliva zavedanje svojih pravic in posledic tega. Zato, ker če jaz posodim geslo, tistemu ni treba nekaj misliti oz. se mu ni treba zdaj odjaviti … In on si olajša delo, ampak jaz se moram zavedati, kaj sem s tem povzročil. Če bo kaj narobe, bom kriv jaz. Lahko, da ni pošten, ta moj kolega in s tem ko je vstopil v informacijski sistem, bo npr. vstopil tudi v mojo plačilno listo, mojih osebnih podatkov.
Šifra: DS **Datum:** 9. 12. 2019 **Spol:** moški **Leto rojstva:** 1976 **Najvišja dosežena izobrazba:** mag. zdr. nege **Zaposlitev:** dipl. zn. na primarnem zdravstvenem nivoju	Če ne potrebujemo podatkov pacientov nujno, se pravi da niso pri nas v obdelavi oziroma, da ne skrbiš zanje, torej zaradi njihovega zdravstvenega stanja, ne potrebuješ njihovih podatkov, torej teh podatkov ne boš iskal. To je vsa umetnost. Jaz nikoli ne iščem podatkov in ne gledam podatkov drugih, če jih ne rabim. Če nekdo pride in če rabim npr. pogledati diagnozo oziroma da rabim zaradi njegovega zdravstvenega stanja neke podatke nujno pogledat … Največkrat gre za diagnoze ali pa EKG, zdravila. Takrat pogledaš po računalniku, drugače pa ne. Marina in Matjaž imata lahko vpogled do vseh pacientov, ampak ne dostopata. Ne dostopata zato, ker teh pacientov ne obdelujeta … In zato ne vem, zakaj bi sploh dostopala do teh podatkov … Lahko bi ju matral firbec, pa bi zato pogledala v podatke. Ampak to se ponavadi v zdravstvu ne dela. Jaz osebno ne bi šel nikoli gledat v podatke oziroma samo takrat, če bi me zanimal kakšen rojstni dan, če že ta podatek ne bi mogel dobiti na Facebooku. Jaz ne grem nobene podatke gledat po računalniku in niti najmanj ne zavarovanja in osebnih podatkov, še sploh pa zdravstvenega stanja ne, samo v primeru, če jih nujno rabim.

Se nadaljuje

Marina in Matjaž bi dostopala do podatkov pacientov za katere ne skrbita v primeru, če npr. na Facebooku ne bi dobila podatka o rojstnem dnevu ali pa v primeru, ko bi rada vedela, kaj se je npr. zgodilo sosedi ... Bi šla pogledat, kaj je bilo z njo narobe. Glede gesla … Jaz si geslo vedno sposodim, ker je moje že toliko zastarelo, da ne morem preko njega noter, pa zato vzamem geslo od koga drugega. … Predvsem zato, ker se mi ne da iti v računovodstvo, da bi mi dali novo geslo. … In mi pač nekdo drug posodi svoje geslo ... In zmeraj mi posodijo geslo … ali pa uporabniško ime. To ni nič takega. Meni se ne da geslo vsakič posodabljati in geslo zmeraj pozabim … In še kartico (profesionalno) pozabim. Ma kartice v bistvu niti nimam. Zakaj je nimam? – To ni prav, ampak bi si jo moral narediti, ker jo potrebujem za delo. Pri geslu in uporabniškem imenu mi računalnik zmeraj zablokira – zato se raje prijavim z drugim geslom in uporabniškim imenom. Na urgenci je itak eden prijavljen za stalno in vsi vstopamo na eno geslo v sistem … Kar seveda ni prav, ampak tako je. Se mi pa je že zgodilo, da se je starejša sestra odločila, da mi ne bo posodila gesla, ker se je zavedala nevarnosti … XX sestra mi je iztaknila kartico iz čitalca, ko je šla na prometno in potem sem se jaz zafrkaval eno uro, da sem sploh usposobil računalnik … Najprej sem moral ugotoviti, da sploh ni profesionalne kartice, potem pa dokler sem jo zalaufal, vse, ko je medtem še 20 pacientov čakalo zunaj … Ne vem … kako je to … da bi moral vsak s svojo kartico dostopati … to je malo tako … ??? Na urgenci to ni možno … Vemo vsi, da ni. Če bomo morali vsi uporabljati svojo kartico, naj potem posodobijo informacijski sistem in računalnike, da gre ta stvar hitreje, ker za vsako posodobitev kartice rabiš 10 minut. Se pravi, da če imaš infarkt ... kaj boš zdaj naredil? Vzel kartico ven in vzel od sodelavca drugo??? In spet posodabljal?? In kako bo to šlo? A nimaš časa niti rešilca pripeljat … Kje še kartico posodobit. Mi imamo vsak svoje geslo in kartico, ampak smo prijavljeni na eno.

Šifra: KK
Datum: 10. 12. 2019
Spol: ženski
Leto rojstva: 1989
Najvišja dosežena izobrazba: TZN
Zaposlitev: TZN na sekundarnem zdravstvenem nivoju

Prvi in najbolj pomemben dejavnik, da Marina in Matjaž ne dostopata do podatkov za katere nista pooblaščena je to, da se zavedaš, da ni to dejanje dovoljeno in da je protizakonito konc koncev … Sama od sebe ne grem, zaradi tega, ker v teh sistemih počnem samo tisto, kar je moja domena in naloga pri dotičnem pacientu. Sem pa že šla, to pa priznam, pogledat, ko me je v bistvu zanimalo o poteku zdravljenja ... če je bilo uspešno ali ne oziroma na sploh, kaj se je z dotičnim pacientom, ki je bil nekoč v moji obravnavi … kaj se je v bodoče z njim zgodilo. Jaz mislim, da je tudi odvisno od tega, kakšen si ti kot oseba, če tudi v svojem življenju počneš take stvari in pri tem nimaš nobenih moralnih zadržkov tudi drugače … Načeloma potem tudi v službenem okolju tega ne boš počel. Torej, prvo je to, da se nekdo zaveda, da to ni prav in tega potem ne stori in občutek pri človeku, ko narediš nekaj narobe – morala. Da gresta pogledat podatke pacientov za katere nista pooblaščena … jaz mislim, da je tukaj vedno neka tretja oseba, ki te za to prosi. Ali je to svojec od prijatelja, naš svojec, lahko tudi v bistvu, če dam primer … Te pokliče policaj s policijske postaje in prosi za podatke osebe, ki je bila poškodovana in želi izvedeti, če je bil poškodbeni list izpolnjen in če lahko na kratko navedem ali pa preberem diagnoze. Jaz sem sama to enkrat naredila. Zdaj pa sem se naučila, da jih prevežem odgovorni osebi, ki je načeloma zdravnik, ki ga je pregledoval. In potem zdravnik to predaja. Jaz mislim, da je za to vedno neka tretja oseba oziroma če želiš pogledat za svojce. Jaz mislim, da bi geslo Matjaž in Marina posodila samo zaradi narave dela. Na primer, pri nas nima vsakdo dostopa do svojega računalnika. Ponavadi sta dva, več je pa zaposlenih in se v sistem prijavi ena oseba ... ni, da bi podala direktno geslo, je pa res, da na nek način dovoli, da preko njegovega portala, skozi celoten delovni dan se izvajajo vse stvari na njegovo uporabniško ime. Če ne bi šlo zato, bi mogoče zaradi tega, ker je nek zaposleni pozabil geslo, pa ga mogoče prosi, da posodi geslo, za tisti dan, da lahko dela preko njegovega uporabniškega imena. Gesla (Matjaž in Marina) po moje ne bi posodila zaradi kazenske odgovornosti in zaradi zavedanja, in da sta storila nekaj narobe in zaradi občutka krivde.

Se nadaljuje

Če gremo lahko na privat zadeve … Ker se na primer s tisto osebo ne razumeš sploh, ji pač ne posodiš gesla. Če se vrnem nazaj, zakaj bi dostopala do podatkov (Marina in Matjaž) pacientov za katere ne skrbita … Ne vem še, koliko je to sporno oziroma dovoljeno, ko te zdravnik prosi, da v njegovem imenu preko svojega uporabniškega imena dostopaš do podatkov pacientov, ki niso bili v tvoji obravnavi, zato ker pač on potrebuje neke informacije in jih v tistem času pač ne more dobiti. Dodala bi še, zakaj bi posodila geslo … Zato, ker nekdo sploh nima uporabniškega imena in gesla do določenih programov, ki so nujno potrebni za njegovo delo, in potem prosi sodelavca, da geslo posodi, da lahko ta opravi svoje delo. Kljub temu, da opozoriš svoje nadrejene, da gesla nimaš, je odgovor bil, da si lahko sposodiš od drugih … in zato si jih kar nekaj sposoja geslo od drugih. Zato je konec koncev dobronamerno in potrebno, da se delo opravi.

Šifra: TMS
Datum: 15. 12. 2019
Spol: ženski
Leto rojstva: 1972
Najvišja dosežena izobrazba: mag. zdr. nege
Zaposlitev: glavna medicinska sestra specialistične bolnišnice

V kolikor onadva, če nimata potrebe po gledanju teh podatkov, naj v te podatke niti ne vstopata. To je naša etika – kodeks etike, ki se ga moramo držati. Ne smemo posegati v zasebnost oz. podatke nekoga, katerega mi sploh ne obravnavamo. To je najbolj ključna stvar. In če mi njih ne obravnavamo, zakaj bi do njihovih podatkov sploh dostopali – tu lahko pride samo do izrabe. Mi imamo tak poklic, da tega ne smemo početi. Tudi če imata pooblastilo dostopati do vseh podatkov v bazi, v določeni ustanovi, ma če pacienta ne obravnavata in če z njim nimata kaj počet, nimata kaj gledat. Mi smo zavezani h kodeksu etike in to je prva stvar, če pacienta ne obravnavata sploh, nimata kaj gledat, saj na ta način zlorabljata. Ampak če se držita kodeksa etike, tega sploh ne bosta počela. Dostopala bi zato, ker jih velikokrat matra firbec … Vemo, da imamo v ustanovi nekoga, ki je medijska osebnost in zaradi radovednosti gresta gledat. Ponavadi je v vsaki ustanovi, npr. mi imamo Birpis in smo vsi pooblaščeni, zdravstveni delavci za vstop v Birpis. Nimamo pa vsi enakih pooblastil, odvisno od profila. Npr. jaz če sem dežurna in mi pride en pacient, pride z napotnico … in tudi če sem jaz dežurna in ga prej nisem nikoli obravnavala, moram pogledat podatke. To je vezano na delo. Zaradi radovednosti lahko pride do zlorab. V nekaterih ustanovah je do zlorab že prišlo in so podatke dajali navzven. Gesla so posojali, ker si nekdo ni zapomnil gesla. To se je zgodilo tudi pri nas. Vsak se mora prijavit, je pa res problem v temu, kako je sistem nastavljen. Jaz se zjutraj prijavim in sem prijavljena. Jaz se ne odjavim. Torej, ti prideš za mano in boš nekaj delala na računalniku in boš delala na mojem geslu. To je problem, ki mislim, da je v teh enotah, kjer nisi sam v službi, kot npr. na oddelku. Nekdo se prijavi, ponavadi je to vodja oddelka, ki ima največ pooblastil … in potem ti prideš za mano in boš nekaj delala na računalniku in boš delala na isto. Ker ne moreš se vsakokrat izklapljat, lahko pa se naredi varne mehanizme, nekatere ustanove jih imajo, mi pri nas nimamo, da se avtomatsko če dve minuti nisi aktiven, da se izklopi. Gesla ne bosta posodila, da ga ne bo kdo drugi zlorabil in da ne bo on kriv za nekaj, kar je nekdo drugi naredil. Ker je tukaj vsa sledljivost. Če posodiš geslo je tukaj sledljivost, samo je vedno kriv tisti, ki je prijavljen. Jaz trenutno ne delam na oddelku. Mi pa preusmerijo veliko klicev pacientov. Jaz se prijavim v Birpis in kliknem ime in priimek pacienta in se mi odpre. Jaz lahko pogledam za vsakega. Sicer pa jaz podatkov ne dam … sedaj pa komu se podatke daje in komu se jih ne … telefonsko naj ne bi nobenemu, ker bi moral preverjati. To je sedaj druga zgodba GDPR-ja. Podatkov po telefonu ne smemo dajati, če nimamo nekega varnostnega mehanizma in običajno imajo nekateri tako, da pacient pove kako se ga potem preveri, npr. da da geslo. Na to geslo se potem da preverit. Svojci, ko pridejo, pridejo do zdravnika in zdravniku povejo, da npr. podatke o njem lahko dajo samo njemu (sinu). Preverite pa tako in tako … na geslo. In svojec ti najprej mora dati geslo … ma po telefonu praviloma ne bi smel dati podatkov. Ko jaz pogledam kje človek je, potem preusmerim klic, jaz se ne spuščam v te stvari. Lahko mi pustijo tudi telefonsko številko in jih potem (osebje) pokliče nazaj.

Šifra: KT
Datum: 15. 12. 2019
Spol: ženski
Leto rojstva: 1990
Najvišja dosežena izobrazba: mag. zdr. nege
Zaposlitev: dipl. m. s. na primarnem zdravstvenem nivoju

Kaj po mojem mnenju vpliva na to, da dostopata do podatkov za katere nista pooblaščena? … Po mojem mnenju so tukaj pomembni varovalni mehanizmi, ki na nek način … oz. če izhajam iz svojega okolja zavarujejo paciente in pa tudi zaposlene, ki imajo npr. kartone ali kartoteke pri osebnem zdravniku. Če bi mi zaposleni imeli dostop do vseh podatkov, bi to lahko pomenilo tudi nezmožnost omogočanja anonimnosti. Tako bi lahko vsak, tudi če bi jaz osebno šla na bolniško, bi lahko nekdo prišel do podatka, zakaj sem jaz na bolniški in tudi če gre za kakšno diagnozo, ki je mogoče pogojena s stigmatizacijo … In to, v takem primeru se jaz ne bi počutila najboljše. Dobra stvar je tukaj, da nimamo vsi dostopa do vsega, ampak samo tiste osebe, ki delujemo na določenem področju, sektorju, ambulanti itd. Dejstvo pa je, da imajo tudi pacienti možnost do vpogleda, kdo je dostopal do njihovih podatkov – to lahko pridobijo prav poimensko, tako, da lahko tukaj nastane že problem … se pa za to ne odloča veliko ljudi, vendar možnost obstaja. Niti ni potrebno, če človek deluje na nekem področju, da ima dostop do vseh podatkov … Ta masa podatkov mora biti zavarovana, tudi na tak način, da dostopajo do njih ljudje, ki delujejo na določenem delovišču. Nepooblaščeno dostopata zaradi tega, ker se želijo dokopati do informacij, ki bi jih mogoče neprofesionalno izkoristila. Ali pa če bi želeli ugotoviti, npr. zakaj je sodelavec na bolniški, na daljši bolniški, saj je dandanes problem, kako je s tem nadomeščanjem, da je veliko nadurnega dela, veliko je odrekanj, zato, ker ljudi ni. Pomanjkanje kadra je in zakaj je nekdo na bolniški … marsikoga to zanima. .. zakaj pa moram jaz delat… kaj pa dela tisti na bolniški? ... Če izhajam iz svojega področja, je to ta glavna stvar. Mogoče bi tukaj lahko rekla npr. še kakšna diagnoza, da jih zanima, ali pa da zanima nekoga drugega – diagnoza kakega pacienta, ki mogoče ni direktno v sorodu. Glede gesel – pri nas imamo narejeno tako, da vsak zaposleni ima svoje uporabniško ime in geslo, ki ga seveda naj ne bi posojal sodelavcem. Dejstvo pa je, da kje se pa zgodi, da se kakšen krat odločijo, da posodijo geslo profesionalne kartice, ki jo mi pri našem delu uporabljamo … ker ali je kakšna nedelujoča ali pa je nekdo pozabil geslo in mu drugi gre na roko, s tem, da posodi svojo, s tem, da je pod vsemi aktivnostmi on podpisan – kar se tiče zdravstvene nege. To osebno se je že zgodilo tudi pri meni, bom priznala, tudi zdaj nedavno, ker sem vskočila, ker je mogla sodelavka nujno iti, ker je imela težavo doma, in da ne bi zdaj vse te paciente, ki smo jih imeli v programu – v čakalnici dali ven in spet notri, zaradi moje profesionalne kartice, mi je pustila svojo in njeno geslo. Ampak to je pač izjema in ne pravilo in se je to zgodilo v mojem primeru zgolj enkrat. Vem pa, da si drugače tudi zapišejo geslo kartice na profesionalno kartico, saj se velikokrat zgodi, da je teh gesel preveč. Konstantno posodabljanje računalnikov, ki ga imamo mi na pol leta, je za marsikoga to že problem … in ker je teh številk preveč, si jih zapišejo direktno na kartico … in vemo, v štartu, da to ni v redu, ampak ja … Gesla ne bi posodila, ker bo računalnik pod vsako aktivnost napisal ime tistega katerega kartica je vstavljena, tudi če ne bo aktivno deloval. Jaz osebno ne posojam nobenemu svoje kartice, ker vedno se zavedam rizika, da če bi bilo kaj ... tudi recimo npr. izdajanje računov za samoplačniške storitve, ki jih mi imamo, si podpisan ti, da si prejel denar, tudi če nisi. Torej kartica, ki je vstavljena je ime od nosilca kartice ... torej in če nekdo drugi to dela in pride do kakšnih problemov ... ali pa tudi ... bog ne daj, pri kakšnih mrliških ogledih je lahko že problem. Bodo poiskali osebo, katere kartica je bila vstavljena, ne bodo pa mogli vedeti, da ta oseba ni delovala. Jaz mislim, da je tukaj zelo pomembno, da se vsak zaveda, da ni najbolj smotrno in niti pametno, da se to dela – da bi posojal geslo. Zdaj izjemoma, ne rečem, kot se je zgodilo pri meni, ampak je načeloma to tudi stvar zaupanja. Ampak zaupanje, mislim ni tisto, kar je zelo krhko. Vsi dobimo svoje kartice, svoje geslo in uporabniška imena zato, da jih uporabljamo, ne pa zato, da bi jih posojali drugim. Je pa to stvar vsakega posameznika oziroma profesionalnost osebe, če bo s tem ravnala pametno in se zavedala, kaj vse lahko to nosi s seboj ali pa ne. Vsak ima pravico reči ne. To je zelo pomembno, samo to je velikokrat ljudem težko.

Šifra: LF
Datum: 30. 12. 2019
Spol: moški
Leto rojstva: 1976
Najvišja dosežena izobrazba: ni podatka
Zaposlitev: informatik v bolnišnici

Nimam predstave, zakaj bi nekdo ne-službeno dostopal do podatkov … razen v primeru, če potrebuje neke informacije na drugem nivoju. Mi smo v naši ustanovi raziskovali, kako so zaposleni kaj dostopali do podatkov strokovnega direktorja … in smo ugotovili, da zaposlene v glavnem zanimajo rojstni dnevi, torej rojstni datumi. V internih nadzorih nismo opazili hujših kršitev, gre za bolj nedolžne stvari. Zakaj se ne dostopa do podatkov … to je že iz osnove etičnega načela, saj nimaš kaj dostopati. To te najbolj ovira … Potrebno je, da v življenju delaš stvari, kot je prav … načeloma, ali ne? Tukaj smo tudi zakonsko zavezani. Zaposleni so podpisali izjavo, čeprav so verjetno že pozabili, da so jo. Preventivno, pa [da se ne dostopa do podatkov] pa so lahko tudi ukrepi preverjanja … Nekdo posodi geslo, če nekdo drug ga vpraša, če mu ga posodi, ker svojega ne ve ali pa ga nima in zato ne more dostopati ... to je ena varianta. Drugi možnosti pa se reče skupinska gesla oz. timska gesla. Eden se prijavi v računalnik in tudi zakon to dopušča. Eden se prijavi na oddelke recimo in potem dela cel tim. Ker prijave in odjave ne peljejo nikamor. Drugače, ne vem zakaj bi nekdo dal geslo. Potem pa ostanejo ljudje prijavljeni, ker se pozabijo odjaviti. Na obisku smo imeli pooblaščena [informacijski pooblaščenec] in smo ga vprašali, kako je s skupinskimi gesli in je bilo v redu, če so gesla na tim. Je potem pa zoprno glede sledljivosti. Prijavi [v sistem] se samo eden, po urniku se pa vidi, kdo je bil v službi. So pa [informacijski pooblaščenec] bolj togi, kakor so bili na začetku, saj se v praksi ne izkaže. Ko smo skupinske prijave dali na dotičen oddelek X, se še niti ena sestra ni prijavila samostojno, ampak je vedno prijavljena Y [vodja oddelka]. In ona je prijavljena, delajo vsi na njeno prijavo. Zato pa sem jih tudi avtomatsko deaktiviral, saj se niso [zaposleni na oddelku] prijavili v sistem že šest mesecev. Z istim geslom se dostopa do lastnih podatkov ... potem pa gesla ne posoja več nobeden; primer je Kadris, recimo ali pri e-receptih. Ko so začeli z e-recepti, so se zdravniki nehali kar tako prijavljati.

Šifra: PP
Datum: 23. 1. 2020
Spol: moški
Leto rojstva: 1980
Najvišja dosežena izobrazba: doktorat znanosti
Zaposlitev: visokošolski učitelj na visoki zdravstveni šoli

Marina in Matjaž ne dostopata do podatkov pacientov za katere ne skrbita, ker nimata uporabniškega računa in verjetno tudi dostopa in pa tudi zaradi socioloških in kulturnih situacij. Ne smeta dostopat in gledat podatke za katere ona dva nimata dostopa. Da dostopata do podatkov, pa je več variant … jih matra firbec ali pa jih je kdo prosil, da pogledajo te podatke, pa čeprav nimajo dostopa – tako s sociološkega vidika … ali pa jim reče šef, naj pogledajo podatke. Verjetna sta ta dva vidika. Ali pa se odločijo pogledat podatke, ker jih ti podatki zanimajo ali pa da jim nekdo reče, da si te podatke morejo pogledat, ker jih potrebujejo … In po vsej verjetnosti, če so dovolj čisti, bodo to primorani narediti, narediti uslugo svojemu šefu. Da se odločita posoditi geslo, je več variant. Prva je hiarhija. Če je Matjaž šef in prosi Marino, da posodi geslo, je čisto možno, da bo Marina rekla, da posodi. Ker če pravi, da ga nujno rabi, ga posodi. Po mojem se to dogaja. In jasno je, da je na celotnem oddelku prijavljen samo en, ker pač nimajo časa, da bi vnašali gesla. Če je to geslo fizično geslo, ki ga je potrebno vpisati ali kaj drugega, npr. kartica oz. vse druge rešitve, kjer nekdo ne more pozabiti gesla – klasično obliko gesla, ki je besedilno zapisano geslo. Potem verjetno teh problemov ne bi bilo oziroma takih želja s strani sodelavcev verjetno ne bi bilo. Nadrejeni morda psihološko vplivajo na to zadevo, ampak sami bodo rekli, da ne. Zakaj rečejo, da ne bodo posodili gesla … je po moje spet odvisno od podatkov, do katerih imajo dostop. Če nekdo zahteva dostop do podatkov, do katerih ima dostop samo ta oseba, ki ima geslo, verjetno se odločijo, da ne bodo posodili gesla, ker ta drugi nima dostopa … to je, če gledamo iz takega zornega kota, ki se zdi najbolj logičen … Nekako ignoriram zlobno dejanje. O tem sploh ne bi rad razmišljal … Načeloma prodaja podatkov oziroma bi se reklo izkoriščanje uporabniških računov, mislim, da tega ni preveč. Čisto možno, da poleg čistih namenov Matjaž in Marina razmišljata, da bo nastal kakšen problem zaradi posoje gesla oziroma uporabniškega računa.

Šifra: HS **Datum:** 3. 2. 2020 **Spol:** ženski **Leto rojstva:** 1960 **Najvišja dosežena izobrazba:** univerzitetna **Zaposlitev:** visokošolski učitelj, več let izkušenj na sekundarnem zdr. nivoju	Da se Marina in Matjaž ne odločita za dostop do podatkov pacientov za katere nista pooblaščena, vpliva znanje o varovanju podatkov in o tem, da to sploh ni potrebno. Zakaj bi dostopal do podatkov nekoga, za katere nisi pooblaščen? Mogoče imajo oz. mislijo, da imajo neke visoke kompetence oziroma pasejo neko radovednost. Toliko si obremenjen z vsemi podatki, da so ti podatki odveč. Več stvari kot poveš, večja je možnost, da ti podatki pridejo ven – ali si v skušnjavi, ali pa te po krivem obtožijo, da si nekaj povedal naprej. Da bi dostopala do podatkov za katere nista pooblaščena, je lahko zaradi neznanja o svojih kompetencah in o tem katere podatke sploh potrebujeta. Gre pogledat v tuje podatke, ker se počuti pomemben – ima neko moč, čuti, da ima pravico. Glede posoje gesel. V praksi si najbrž posojajo gesla. Eni ja, drugi ne. Ne vsi. Da posodijo geslo, velja zaupanje oziroma se ne zavedajo kaj se lahko zgodi. Posodijo, v duhu timskega dela, kar ni prav. Ker to je enako, kot če bi ti pripravil terapijo in bi jo nekdo drugi apliciral pacientu in odgovarjal, če je kasneje kaj narobe. Če posodiš, misliš, da si dober – dobrota, prijateljstvo. Zaupanje je v redu, ampak v nekih okvirjih. Gesla ne posodita, če poznata odgovornost. Nimam konkretnega primera. V tistih časih, ko smo imeli svoja gesla, nismo imeli znanja o tem, stvari niso bile dodelane. Se pa to res lahko primerja z izvajanjem postopkov, za katere nisi kompetenten.
Šifra: SM **Datum:** 4. 2. 2020 **Spol:** ženski **Leto rojstva:** 1984 **Najvišja dosežena izobrazba:** mag. zdr. nege **Zaposlitev:** visokošolski učitelj, več let izkušenj na sekundarnem zdr. nivoju	Če sta Marina in Matjaž zaposlena na oddelku, ne smeta niti videti podatke pacientov za katere ne skrbita, ker nista zadolžena za pacienta in ga ne negujeta. To jima brani njuna poklicna skrivnosti in njihov poklic, zaveza dela. Na vsakem oddelku imaš določene dolžnosti, ki jih moraš opraviti kot sestra in si odgovorna za tisti oddelek oziroma za tiste paciente. Če pa bi ona dva na primer šla pomagati oziroma sta skočila na pomoč in če jih zanima neka stvar, pa bi morala imeti vpogled. Zaradi tega, da vesta kako pomagat. Do nepooblaščenih podatkov dostopata, ker nikoli ne vesta, kdaj bi bila potrebna pomoč in je prav, da mogoče imata te podatke. Če bosta šla samo mimo in bo pacient vprašal: »Kaj mi date za pit?« in če bosta bila ona dva seznanjena, da mora pacient biti tešč, mu pač ne bosta dala za pit. To se je meni tudi dogajalo na oddelku. Na primer, da je nekdo zaposlen v bolnišnici in da povprašuje po določenih podatkih. Je prav, da nima dostopa, ker nikoli ne veš, kakšno izkušnjo je kdo imel in pa poznanstva in kakorkoli, pa da ne bi kdo govoril o zdravstvenem stanju nekoga, ker mogoče mu ni dal pooblastila, da govori o njemu. Gesla ne posojata, ker sta tako potem v kazenskem postopku. Posodita mogoče zato, ker hočeta nekomu pomagat, samo to ni v redu. Če grejo v kontrolo in vidijo, da je bil nekdo prijavljen s tem geslom, potem ga bodo zasliševali – v kolikor bi bilo kaj narobe in bo v kazenskem postopku. Gesla ne posojata, ker sta imela taka navodila. Ko ti dodelijo geslo, moraš podpisati tudi alineje v katerih je zapisano kaj smeš in kaj ne smeš. Torej pravilnik. Držijo se varovanja pacientovih podatkov, kar je normativa. Kodeks etike ima točke, ki te zavezujejo.
Šifra: DZ **Datum:** 22. 4. 2020 **Spol:** moški **Leto rojstva:** 1987 **Najvišja dosežena izobrazba:** mag. zdr. nege **Zaposlitev:** dipl. zn. na primarnem zdr. nivoju	Na to, da Marina in Matjaž ne dostopata do podatkov pacientov, za katere nista pooblaščena, najbolj vpliva to, da imata vest, moralo, neko profesionalno etiko ali pa to, da vesta, da vse kar naredita na omrežju je sledljivo in se točno ve, kdaj in s katere naprave je kdo kaj pogledal. Na to, da dostopata do podatkov, za katere nista pooblaščena – je del človeške narave. Brskaš, včasih zbiraš informacije od drugih. To je zaradi genetike. To smo ljudje in to imamo v sebi, da se zanimamo kaj je z drugimi. Največkrat pa dostopata do podatkov zato, ker jih zanima s profesionalnega vidika, npr. kakšen je bil izid neke bolezni ali pa kakšni so bili izvidi pred boleznijo. Večina takih dostopanj je s profesionalnega vidika, ostalo iz firbca. Na to, da dostopata vpliva, da imata vse na dosegu roke in da sta prijavljena pod drugim imenom – izkoristita drug log in in drugo geslo, kar se v praksi dosti uporablja. Npr. jaz v praksi ne vidim, da bi se veliko gledalo v podatke, vidim pa, da se uporablja drug log in in druga gesla. Ampak to je zaradi narave dela, da se stvari stalno ne prepletajo. Ne moremo mi biti kot nek policijski sistem – tam se usedejo za računalnik in obravnavajo enega človeka – in gledajo informacije tega človeka. To v našem sistemu ne bi šlo.

Se nadaljuje

Mi obdelamo od 50 do 100 pacientov na dan. Tega pacienta obravnavajo naenkrat štiri ljudje in je toliko prepletanja teh štirih ljudi in še ostalih izvajalcev, npr. ambulante, rentgena, da je to praktično nemogoče. Z mojega vidika, je pomembna edino etika. Potrebno jo je vzdrževati in to je to. Dinamika dela pač je taka – edino če bi prišlo do tega, da bi imeli prenosne naprave, v smislu, da bi imel vsak svojo tablico in bi se nanjo prijavljal in bi potem z njo delal naprej. Pri tehnologiji, ki jo imamo na razpolago trenutno, ta stvar ni izvedljiva. To je dejstvo. Ali pa da bi imeli kartico ali pa čip, s katerim bi vsak potrjeval, kar je naredil, v smislu, da bi na hitro obkljukal kar je naredil. Naša tehnologija zaenkrat tega ne omogoča – da bi lahko kaj takega izpeljali, da ne bi trpelo delo. Glede posoje gesel jaz osebno nimam nekih zlonamernih izkušenj na to temo. V smislu, da bi kdorkoli zlorabljal in bi jaz bil priča vsemu temu – tega se ne spomnim. Tukaj se gremo profesionalnega odnosa in profesionalne etike in te naj bi se držali vsi. In zakaj posodijo geslo? – posodijo zato, ker se gesla včasih pozabi ali pa nimajo svojega. Sej če pa ima svoje geslo, si ga ne rabi posojat. Se ne spomnim, da bi se zgodilo, da bi mi kdo rekel, dej posodi mi geslo. Bolj je problem to, da se eden priloggira na drugo geslo. To je bolj problem. Ampak zakaj se to dogaja? – To se dogaja zaradi samega dela. Že tako je naš program počasen in da bi se vsak stalno logiral na svoje geslo, to ni mogoče. Nisem pa še doživel, da nekdo ne bi posodil gesla. Razen ena na novo zaposlena noče dajati svoje kartice, svoje profesionalne kartice.

Šifra: RC
Datum: 15. 5. 2020
Spol: moški
Leto rojstva: 1990
Najvišja dosežena izobrazba: dipl. zn.
Zaposlitev: dipl. zn. na primarnem zdr. nivoju

Da Marina in Matjaž ne dostopata do podatkov pacientov za katere nista pooblaščena, v prvi vrsti vplivajo pravila, ki so postavljena na oddelku. V bolnici smo imeli vedno načeloma pravila, da nisi smel dostopat do podatkov pacientov, ki niso v tvoji obravnavi. Čeprav so se ta pravila dostikrat prekršila. Sam sem bil priča, ko so se pravila tudi kršila. Pravila so, ampak so zelo ohlapna. Zato se jih tudi krši. Pravila so zapisana v statutu bolnišnice. Že v pogodbi moraš podpisati člen o varovanju in zajema tudi to zraven. Pred zaposlitvijo smo bili tudi s tem seznanjeni. Tudi na tem delovnem mestu načeloma ne smemo vpogledat v podatke po GDPR-ju. Pa moralno sporno je. Načeloma ne bi smeli dostopati do podatkov. Brigat se je treba zase in ne za druge. Do podatkov se dostopa zaradi radovednosti, pa zato, da imaš nekaj za opravljat in da se pohvališ, da imaš neko informacijo, ki jo nekdo drug nima. Do podatkov sta dostopala mogoče zaradi tega, ker jih je nekdo drug prosil za informacije. Obstaja torej možnost, da je nekoga drugega, svojce, prijatelje zanimalo, kaj se z nekim pacientom dogaja. Ali pa je neka slavna oseba in hočeš biti seznanjen z njegovimi podatki. Geslo se posoja, če včasih kak sodelavec pozabi svoje geslo. Pri nas v službi se samo eden prijavi, da se skozi ne prijavlja. Zjutraj se eden prijavi, potem pa vsi dostopajo preko njegovega gesla, čeprav to ni prav. Praviloma vemo vsi, da bi vsakič moral vsak sam se prijaviti s svojim geslom, zato da je omogočena sledljivost – kaj je kdo gledal. Ker jaz lahko npr. tudi zlorabim. Če si ti npr. prijavljena, grem lahko jaz gledat podatke tretje osebe – kriva boš pa ti. In jaz ne bom šel v zapor, ampak ti. Ker ne bodo vedeli, da sem bil jaz tam. Torej glavni problem glede izposoje gesel je ta, da geslo pozabiš ali da se nekomu ne da prijaviti s svojim geslom. In pusti kar prijavljenega drugega uporabnika. Ma mislim, da je to povsod tako. Na to, da nekdo ne bi posodil gesla, bi imela vpliv na to zelo zelo stroga pravila in stroge kazni. V prvi vrsti bi moral biti zagotovljen interni nadzor na mesečni ravni. Npr. se izbere nekaj zaposlenih in se pogleda do kakšnih podatkov so dostopali. In potem bi morale biti tudi sankcije in ne samo ustavna opozorila. Če bi bilo tako, kot sem povedal, bi vsi bolj delali po pravilih. Preden sem šel iz starega delovnega mesta, so v bolnišnici začeli delati interne nadzore enkrat na mesec. So izbrali nekaj pacientov, ki so bili obravnavani in potem so pregledali kdo in kaj je klikal na obravnavo. In se je takoj vedelo. Se je dotične kar poklicalo in vprašalo, zakaj si dostopal do tega in tega pacienta – utemelji oz. podaj razlog. Pravila so. Vendar če jih bolj okrepiš, potem trpi delo. Zato je tukaj pomembno, da je vsak pri sebi dovolj inteligenten in ima zavedanje ter profesionalen odnos. Mi uporabljamo samo eno geslo.

Se nadaljuje

Zato moraš biti vsaj toliko fer. Da se je nekdo prijavil in da ne boš ti delal na njegovo ime neumnosti. Potem bo šel tisti, ki je prijavljen v zapor ali pa bo ob licenco, ti pa ne. Razen če boš ti priznal, da si delal na njegovo geslo. V porodnišnici XY se je prav to tudi zgodilo. Ena sestra je šla za svojo žlahto gledat v sistem – če je že rodila. In veš kaj je naredila? Odprla je porodni protokol, da je otrok že rojen. Otrok se je pa rodil komaj naslednji dan. In to, ko enkrat to odpreš oziroma, ko enkrat to zabeležiš grejo podatki online, takoj naprej. Ona je odprla uradni dokument. Potem je šel primer na sodišče. Če so hoteli to aktivnost stornirat, so mogli to narediti na Ministrstvu in tam tudi upravičiti. Mislim, da sestra ni izgubila licence. Je pa bilo blizu temu. Mislim, da je dobila kazni in pogoje ter nadzore. Nekaj je pač kliknila in se je avtomatsko odprl porodni protokol. Jaz osebno ne vem kako to zgleda. In je bilo konec. Aja in še to … vse to je naredila pod imenom sodelavke. Sodelavka je šla zjutraj domov in je bila doma. In so jo klicali domov. Ta je pa rekla – ne jst sem doma. Ta je dobila kazen, ker se ni odjavila iz sistema. Ti ko zapustiš delovno mesto, si dolžen se odjaviti. Ta druga pa je bila sankcionirana prvo, ker je uporabila drugo uporabniško ime in geslo oz., ker se ni na novo prijavila in drugič, ker je sploh gledala noter. Pacientka ni v tem primeru nobenega tožila. Ker je bila ta sestra njena žlahta. Problem je nastal, ko je babica hotela zabeležiti rojstvo, je ta protokol bil že odprt ... halo… protokol odprt že en dan prej? To je bil največji problem, ker ga ne moreš izbrisati, gre takoj v online sistem. To gre potem vse preko Ministrstva in en kup odločb in potrebno je upravičiti, da boš protokol brisal in pojasniti. To je bilo problematično. To gre direktno v statistiko.

Šifra: PD
Datum: 22. 6. 2020
Spol: ženski
Leto rojstva: 1993
Najvišja dosežena izobrazba: mag. zdr. nege
Zaposlitev: dipl. m. s. na sekundarnem in terciarnem zdravstvenem nivoju

Da Marina ali Matjaž ne dostopata do podatkov, najbolj vpliva njihova etika ali morala oz. kaj ona dva prinašata s seboj, npr. od doma, v smislu, kaj sta se ona dva doma naučila. Najbolj vpliva njihova vest. Njihova vest jim ne dopušča, da bi te podatke gledala ali da bi dostopala do teh podatkov. Ona dva tudi vesta, da to dejanje ni po zakonodaji, da ni po njihovih pravilnikih oz. da ni zakonsko dovoljeno. Torej, da zakonsko ni dovoljeno, da jim to ne dopušča etika in da to prinašajo s sabo, v smislu svojih navad, da to ni prav. Tak kot si doma, tak si tudi v službi. Da dostopata do podatkov, vpliva velik firbec – kaj se dogaja z drugimi, kaj se dogaja z ljudmi, katere mogoče poznajo, pa bi radi malo pogledali kaj pa kako, ali pa jih je kdo drugi vprašal, npr. kakšen sodelavec ali pa kdo drug, da naj do teh podatkov dostopajo in da naj jim povejo kaj in kako. Mogoče do teh podatkov dostopajo tudi zaradi tega, ker bi s temi podatki želeli videti, kako bodo nekomu drugemu na ta način pomagali. Npr. pri enem pacientu je bila naročena neka preiskava, za katero ne poznaš več šifre za naročanje. In si potem pomagaš, da pogledaš podatke za nazaj za nekega drugega pacienta. In te podatke potem uporabiš za naprej, da si olajšaš delo pri sedanjih obravnavah. Zakaj bi Marina in Matjaž posodila geslo? Mogoče ta, ki prosi, je pozabil profesionalno kartico in jo potrebuje, ker bi rabil nekaj narediti in s tem bi nekomu pomagal, če posodiš, čeprav to ni prav. Ker ko ti posojaš geslo, lahko nekdo drugi nekaj naredi v tvojem imenu in v kolikor je kaj narobe, se lahko marsikaj zgodi. Geslo posodiš, zaradi pomoči. Lahko pa ima nekdo skrit namen ali pa firbec. Npr. Marina vpraša Matjaža za geslo, ker ga mogoče ona nima ali pa nima dostopa do vsega in bi z njegovim geslom, ker on dostopa do vsega, bi ona lahko želela kaj pogledat, kar ne bi smela. Gesla ne posojaš zaradi poklicne etike, vesti, zaradi pravic pacientov. Kot zaposleni ne smemo posegati v informacije, podatke od vsakega pacienta. Ker tukaj se gre za pacienta in njegovo intimo. S tem ko ti gledaš te podatke od drugih pacientov, posegaš v njegovo intimnost in to ni prav. Pri tem najbolj pomembno vlogo igra vest, zakonodaja in etika.

10.3 PROFIL UDELEŽENCEV RAZISKAVE

Tabela: Značilnosti udeležencev raziskave

Kategorija	N = 527	Valid Percent
Starost		
najmlajši	22	
najstarejši	63	
povprečje	42,37	
std. odklon	10,375	
Doba dela v orgaanizaciji (v letih)		
najkrajša	0	
najdaljša	42	
povprečna	16,74	
std. odklon	11,898	
Spol		
moški	70	13,3
ženski	457	86,7
Stopnja dosežene izobrazbe na področju ZN		
SMS/ZT/TZN	124	23,5
viš. med. ses./viš. med. teh	19	3,6
dipl. m. s./dipl. zn	308	58,4
mag. zdr. nege	76	14,4
Stopnja dosežene izobrazbe na področju ZN – rekodirana		
zaposleni v zdravstveni negi brez diplome	143	27,1
zaposleni v zdravstveni negi z diplomo	384	72,9
Izobrazba na drugih področjih	166	100
visoko-strokovna izobrazba	82	49,4
strokovni magisterij	45	27,1
univerzitetna izobrazba	28	16,9
znanstveni magisterij	11	6,6
Zaposlitveni status	527	100
zaposlena za polni delovni čas	486	92,2
zaposlena za polovični delovni čas	15	2,8
bolniško odsotna z dela	6	1,1
porodniški dopust	7	1,3
drugo	13	2,5
Tip organizacije, v kateri delujejo zaposleni		
zdravstveni dom	128	24,3
splošna bolnišnica	100	19
specialistična bolnišnica	24	4,6
klinični center (vključno s klinikami)	109	20,7
klinika (samostojna)	16	3
inštitut	7	1,3
socialnovarstveni zavod	125	23,8
drugo	17	3,2
Nivoji zdravstvenega varstva/socialno-varstveni zavodi		
primarni zdravstveni nivo	128	24,3
sekundarni zdravstveni nivo	124	23,6
terciarni zdravstveni nivo	132	25,1
socialno-varstveni zavodi	125	23,8
drugo	17	3,2
Okolje organizacije		
urbano/mestno	405	76,9
ruralno/podeželje	122	23,1

10.4 VPRAŠALNIK

Spoštovani!

Sem Samanta Mikuletič, študentka Fakultete za zdravstvo Angele Boškin. V okviru doktorske disertacije, pod mentorstvom izr. prof. dr. Boštjana Žvanuta ter somentorstvom red. prof. dr. Brigite Skele-Savič izvajam presečno raziskavo na slovenski populaciji zaposlenih v zdravstveni negi. Fenomen, ki ga preučujem je informacijska varnostna kultura in ravnanje zaposlenih v zdravstveni negi z zdravstvenimi podatki.

Seznanjam vas, da z anketo merim vedenjsko namero nepooblaščenega dostopa do zdravstvenih podatkov in ne dejanskega vedenja – kršitve, ter da številne raziskave in Teorija načrtovanega vedenja (Ajzen, 1991) obravnavajo vedenjsko namero kot dober prediktor vedenja samega.

Rada bi poudarila, da je sodelovanje v tej anketi anonimno in prostovoljno ter ga lahko kadarkoli prekinete. Podrobnosti o raziskavi si lahko preberete na naslednji povezavi.

V vprašalniku uporabljeni izrazi, zapisani v slovnični obliki ženskega spola, so uporabljeni kot nevtralni in veljajo enakovredno za oba spola. Predviden čas izpolnjevanja ankete je 15 minut.

V kolikor anketo izpolnjujete na pametnem telefonu, ga postavite v vodoravni položaj.

Vljudno vas naprošam k sodelovanju.

Kontaktna oseba: Samanta Mikuletič, samanta.mikuletic@gmail.com

Fakulteta za zdravstvo Angele Boškin
Angela Boškin Faculty of Health Care

17. 3. 2021

Povezanost dimenzij informacijske varnostne kulture z namero izvedbe kršitev informacijske varnosti s strani zaposlenih v zdravstveni negi – presečna raziskava

Spoštovani respondenti,

Po podatkih raziskav je stanje kršitev varnosti osebnih podatkov alarmantno. V zadnjih letih se kršitve povečujejo tudi na področju zdravstvenega sektorja. V zvezi z zagotavljanjem varnosti informacijskih virov so tehnološke metode varovanja informacij učinkovite le do določene mere. Ključno vlogo ima še vedno človeški dejavnik.

Na področju zdravstvene nege je po nam znanih podatkih malo raziskav, ki preučujejo obravnavano temo, predvsem takih, ki bi v zadostni meri pojasnjevale povezave s samo namero kršitve informacijske varnosti. Problematika informacijske varnosti je med populacijo zaposlenih v zdravstveni negi premalo obravnavana. Gre za področje, ki je pomembno za stroko, saj imajo zaposleni opravka z zaupnimi podatki pacientov, katerih zloraba lahko pomeni tako moralno kot finančno škodo.

V okviru doktorske disertacije, pod mentorstvom izr. prof. dr. Boštjana Žvanut ter somentorstvom red. prof. dr. Brigite Skele-Savič, na Fakulteti za zdravstvo Angele Boškin izvajam presečno raziskavo na slovenski populaciji zaposlenih v zdravstveni negi, s katero bomo pridobili dragocene informacije.

Izvedena raziskava bo dala eksplorativni vpogled v opisan raziskovalni problem. Tako izvedena raziskava in spoznanja le-te so primerna osnova za zasnovo eksplikativne raziskave v izbranih kliničnih okoljih, ki vključuje metodo sistematičnega opazovanja in nadzora neodvisnih in odvisnih spremenljivk v neposrednem okolju na randomiziranem vzorcu. Naša raziskava bo prispevala nabor neodvisnih in odvisnih spremenljivk, ki bi jih bilo smiselno opazovati s prospektivnimi raziskovalnimi metodami v naslednjih raziskavah.

Fakulteta za zdravstvo Angele Boškin
Angela Boškin Faculty of Health Care

Ugotovili bomo obseg, količino in značilnosti pojava, prepoznali povezane dejavnike v zvezi s katerimi je smiselno uvajati ukrepe izboljšav pri delu z zaposlenimi in procesom dela, da bi lahko zmanjšali incidenco kršenja informacijske varnosti. Na ta način bomo identificirali, katere vzvode, ki se nanašajo na informacijsko varnostno kulturo, lahko uporabijo zdravstvene in socialnovarstvene ustanove za zmanjšanje tveganja za kršitev zaupnosti zdravstvenih podatkov s strani zaposlenih v zdravstveni negi ter tako identificirali priporočila namenjena managementu zdravstvenih ustanov, kako izboljšati stanje na tem področju. Pomembno bomo prispevali k razvoju stroke tako, da bodo izsledki predstavljali kakovostno izhodišče za nadgradnjo formalnih in neformalnih izobraževalnih programov, namenjenih zaposlenim v zdravstveni negi in tako stroko zdravstvene nege oplemenitili z dodatnim praktičnimi znanji, ki so nepogrešljiva pri uporabi sodobne informacijsko-komunikacijske tehnologije.

Z anketo bomo merili vedenjsko namero nepooblaščenega dostopa do podatkov zaposlenih v zdravstveni negi in ne dejanskega vedenja - kršitve. Poudariti pa je potrebno, da Teorija načrtovanega vedenja in številne raziskave obravnavajo vedenjsko namero kot dober prediktor vedenja samega.

Raziskava je 16. februarja 2021 s strani Komisije Republike Slovenije za medicinsko etiko dobila soglasje, da je raziskava etično sprejemljiva (št. 0120-583/2020/7). Po navodilu Komisije Republike Slovenije za medicinsko etiko respondente vnaprej opozarjamo, da utegnete s svojimi odgovori razkriti prekrške in kazniva dejanja (v zvezi z varstvom zasebnosti), ki se preganjajo po uradni dolžnosti.

Sodelovanje v tej anketi je anonimno in prostovoljno ter ga lahko kadarkoli prekinete. Pridobljeni podatki bodo uporabljeni izključno za raziskovalne namene.

Za dodatna vprašanja se lahko obrnete neposredno name, na e-naslov: samanta.mikuletic@gmail.com.

Hvala.

Samanta Mikuletič, mag. zdr. nege

Prosimo, da v anketi odgovarjate izključno za **organizacijo**, v kateri **delate** ali ste delali **nazadnje**.

Izkušnje z delom v zdravstveni negi (obkrožite številko): 1 Da
2 Ne

Zaposlitveni status (obkrožite številko):
1 Zaposlena za polni delovni čas
2 Zaposlena za polovični delovni čas
3 Bolniško odsotna z dela
4 Porodniški dopust
5 Drugo: _____

Doba dela v organizaciji (napišite število): _____ let

Tip organizacije (obkrožite številko):
1 Zdravstveni dom
2 Splošna bolnišnica
3 Specialistična bolnišnica
4 Klinični center (vključno s klinikami)
5 Klinika (samostojna)
6 Inštitut
7 Socialnovarstveni zavod
8 Drugo: _____

Okolje organizacije (obkrožite številko): 1 Urbano / mestno
2 Ruralno / podeželsko

Pri delu uporabljam računalnik (obkrožite številko): 1 Da
2 Ne

Scenarij
Ga. Novak je medicinska sestra v bolnišnici. Pri svojem delu uporablja informacijski sistem, ki ji omogoča rokovanje z zdravstvenimi podatki, ki se nanašajo na telesno ali duševno zdravje pacientov. Bolnišnica ima stroga pravila, ki prepovedujejo zaposlenim dostop do zdravstvenih podatkov pacientov, za katere ne skrbijo. Pred kratkim je bil v bolnišnico sprejet znan pevec. Kljub temu, da ni bil njen pacient, je ga. Novak v informacijskem sistemu preverila, zakaj je bil pevec sprejet.

V nadaljevanju označite, koliko SE STRINJATE ali SE NE STRINJATE za **vsako** od **trditev** glede **scenarija.**

S1_AtB	Močno se ne strinjam	Se ne strinjam	Delno se ne strinjam	Nevtralno	Delno se strinjam	Se strinjam	Močno se strinjam
Ravnati kot ga. Novak bi bila zelo dobra ideja.	1	2	3	4	5	6	7
Ravnati kot ga. Novak bi bilo zelo koristno.	1	2	3	4	5	6	7
Ravnati kot ga. Novak bi bilo zelo pametno.	1	2	3	4	5	6	7

S1_SN	Močno se ne strinjam	Se ne strinjam	Nevtralno	Se strinjam	Močno se strinjam
Večina meni pomembnih ljudi meni, da bi morala ravnati kot ga. Novak.	1	2	3	4	5
Večina ljudi, katere cenim, meni, da bi morala ravnati kot ga. Novak.	1	2	3	4	5
Od mene se pričakuje, da ravnam kot ga. Novak.	1	2	3	4	5

S1_PBC	Močno se ne strinjam	Se ne strinjam	Delno se ne strinjam	Nevtralno	Delno se strinjam	Se strinjam	Močno se strinjam
Zmožna sem, da se samostojno odločim, da ravnam kot ga. Novak.	1	2	3	4	5	6	7
Pod nadzorom imam, da se odločim, da ravnam kot ga. Novak.	1	2	3	4	5	6	7
Menim, da imam sredstva, znanje in sposobnosti, da se odločim, da ravnam kot ga. Novak.	1	2	3	4	5	6	7

V nadaljevanju označite, koliko SE STRINJATE ali SE NE STRINJATE za vsako od navedenih trditev.

S1_BI	Močno se ne strinjam	Se ne strinjam	Nevtralno	Se strinjam	Močno se strinjam
Če bi se znašla v primerljivih okoliščinah, bi ravnala kot ga. Novak.	1	2	3	4	5
Ravnati enako kot ga. Novak je nekaj, kar bi naredila tudi sama, če bi se znašla v primerljivih okoliščinah.	1	2	3	4	5
Predstavljam si, da bi ravnala enako kot ga. Novak, če bi se znašla v primerljivih okoliščinah.	1	2	3	4	5

Zasebnost se v tej anketi nanaša izključno na zasebnost glede **zdravstvenih podatkov** in NE drugih oblik zasebnosti pacientov (npr. zasebnost pri preoblačenju).

S1_NB

	Močno se ne strinjam	Se ne strinjam	Delno se ne strinjam	Nevtralno	Delno se strinjam	Se strinjam	Močno se strinjam
Moji nadrejeni menijo, da bi morala ravnati kot ga. Novak.	1	2	3	4	5	6	7
Moji sodelavci menijo, da bi morala ravnati kot ga. Novak.	1	2	3	4	5	6	7
Moj vodja izmene meni, da bi morala ravnati kot ga. Novak.	1	2	3	4	5	6	7

Informacijski sistem se v tej anketi nanaša na sistem, ki omogoča zbiranje, obdelavo, shranjevanje, distribucijo ter uporabo podatkov in informacij. Gre za računalniški sistem, kjer vnašate, spremljate zdravstvene in ostale podatke o pacientu ter ostale aktivnosti v organizaciji (Islovar, 2016).
Informacijski vir se v tej anketi nanaša na zapise o pacientu, dokumente, podatkovne zbirke, kjer lahko uporabnik dobi informacijo (Islovar, 2016).
Varnost podatkov se v tej anketi nanaša na **osebne** podatke pacientov (npr. rojstni datum, naslov, številka KZZ) in podatke o njihovem **fizičnem** ter **duševnem zdravju**.

V nadaljevanju označite, koliko SE STRINJATE ali SE NE STRINJATE za **vsako** od navedenih **trditev**.

PO	Močno se ne strinjam	Se ne strinjam	Nevtralno	Se strinjam	Močno se strinjam
V naši organizaciji smo zavezani k poklicni molčečnosti.	1	2	3	4	5
V naši organizaciji smo zavezani k zagotavljanju zasebnosti pacientov.	1	2	3	4	5
V naši organizaciji varujemo zasebnost pacientov.	1	2	3	4	5
V naši organizaciji zagovarjamo pravice pacientov do zasebnosti.	1	2	3	4	5
V naši organizaciji se držimo pravila "ne delaj drugim, kar ne želiš, da bi drugi naredili tebi" glede zasebnosti pacientov.	1	2	3	4	5

SO	Močno se ne strinjam	Se ne strinjam	Nevtralno	Se strinjam	Močno se strinjam
V naši organizaciji je prisotna kultura spodbujanja dobrih praks za varovanje podatkov o pacientih.	1	2	3	4	5
Varnost podatkov o pacientih je od nekdaj pomembna vrednota naše organizacije.	1	2	3	4	5
Zagotavljanje dobre varnosti podatkov o pacientih je sprejet način dela v naši organizaciji.	1	2	3	4	5
Zagotavljanje varnosti podatkov o pacientih je ključna norma, ki velja za vse zaposlene.	1	2	3	4	5
V naši organizaciji je varnost podatkov o pacientih kolektivna odgovornost.	1	2	3	4	5

V nadaljevanju označite, koliko SE STRINJATE ali SE NE STRINJATE za **vsako** od navedenih **trditev**.

PCM	Močno se ne strinjam	Se ne strinjam	Delno se ne strinjam	Nevtralno	Delno se strinjam	Se strinjam	Močno se strinjam
Naša organizacija ima pravila, ki zaposlenim prepovedujejo dostopati v informacijski/-e sistem(e), za katerega/-e niso pooblaščeni.	1	2	3	4	5	6	7
Naša organizacija ima vzpostavljena pravila obnašanja glede uporabe informacijskih virov.	1	2	3	4	5	6	7
Naša organizacija ima izdelane smernice dela z računalniki in ostalimi napravami.	1	2	3	4	5	6	7
Naša organizacija ima izdelane smernice o primerni uporabi elektronske pošte.	1	2	3	4	5	6	7

RM	Močno se ne strinjam	Se ne strinjam	Nevtralno	Se strinjam	Močno se strinjam
Naša organizacija primerno nadzoruje grožnje informacijskim virom.	1	2	3	4	5
Menim, da ima naša organizacija ustrezno vzpostavljene postopke prepoznavanja morebitnih tveganj povezanih z izgubo zaupnosti, celovitosti in razpoložljivost informacijskih virov.	1	2	3	4	5
Menim, da naša organizacija dobro prepoznava šibke točke svojih informacijskih virov.	1	2	3	4	5

SETA	Močno se ne strinjam	Se ne strinjam	Delno se ne strinjam	Nevtralno	Delno se strinjam	Se strinjam	Močno se strinjam
Zaposleni v naši organizaciji so seznanjeni s posledicami nepooblaščenega spreminjanja podatkov.	1	2	3	4	5	6	7
Zaposleni v naši organizaciji so seznanjeni s posledicami nepooblaščenega dostopanja do informacijskih sistemov.	1	2	3	4	5	6	7
Naša organizacija izobražuje zaposlene o odgovornosti zaposlenih glede varnosti podatkov.	1	2	3	4	5	6	7
Naša organizacija zagotavlja usposabljanja, kjer lahko zaposleni izboljšajo svojo varnostno ozaveščenost.	1	2	3	4	5	6	7

Informacijska varnost se v tej anketi nanaša na izvajanje varnostnih ukrepov in postopkov za zaščito celovitosti in razpoložljivosti komunikacijskih, informacijskih ali drugih elektronskih sistemov ter podatkov, ki se v njih obdelujejo, shranjujejo ali prenašajo (Islovar, 2016).

V nadaljevanju označite, koliko SE STRINJATE ali SE NE STRINJATE za **vsako** od navedenih **trditev**.

TMC	Močno se ne strinjam	Se ne strinjam	Nevtralno	Se strinjam	Močno se strinjam
Menim, da ima višje vodstvo naše organizacije jasno vizijo o informacijski varnosti.	1	2	3	4	5
Menim, da ima višje vodstvo naše organizacije jasno oblikovano strategijo doseganja visoke stopnje informacijske varnosti.	1	2	3	4	5
Menim, da je višje vodstvo naše organizacije postavilo jasne cilje za doseganje visoke stopnje informacijske varnosti.	1	2	3	4	5
Višje vodstvo naše organizacije smatra informacijsko varnost kot prioriteto.	1	2	3	4	5

MON	Močno se ne strinjam	Se ne strinjam	Delno se ne strinjam	Nevtralno	Delno se strinjam	Se strinjam	Močno se strinjam
Menim, da naša organizacija izvaja redne revizijske presoje, katerih cilj je odkrivanje uporabe nepooblaščene programske opreme na službenih računalnikih oz. napravah.	1	2	3	4	5	6	7
Menim, da naša organizacija spremlja aktivnosti zaposlenih pri delu z informacijskimi sistemi.	1	2	3	4	5	6	7
Menim, da naša organizacija redno nadzira zgodovino aktivnosti, ki jih izvedejo zaposleni v informacijskem sistemu (npr. prijava/odjava v sistem, vnos, sprememba, brisanje podatkov).	1	2	3	4	5	6	7

ISK	Močno se ne strinjam	Se ne strinjam	Nevtralno	Se strinjam	Močno se strinjam
Naša organizacija ima na voljo kompetentne(ga) strokovnjaka/-e (zunanje oz. notranje), ki zagotavljajo izvajanje nadzora nad informacijsko varnostjo.	1	2	3	4	5
Menim, da ima naša organizacija na voljo ustrezno znanje (zunanje oz. notranje), da lahko skladno z veljavno zakonodajo izvede notranji nadzor stanja informacijske varnosti.	1	2	3	4	5
Menim, da ima naša organizacija na voljo ustrezno znanje (zunanje oz. notranje kadre), da lahko izvede/organizira programe/promocije na področju informacijske varnosti (npr. izobraževanja, seminarji, tečaji).	1	2	3	4	5

V nadaljevanju označite, koliko SE STRINJATE ali SE NE STRINJATE za **vsako** od navedenih **trditev**.

ISKS	Močno se ne strinjam	Se ne strinjam	Delno se ne strinjam	Nevtralno	Delno se strinjam	Se strinjam	Močno se strinjam
V naši organizaciji si zaposleni medsebojno izmenjujejo znanja in izkušnje glede informacijske varnosti.	1	2	3	4	5	6	7
Vsi zaposleni so aktivno vključeni v izmenjavo znanja in izkušenj o informacijski varnosti.	1	2	3	4	5	6	7
Menim, da obstoječa izmenjava znanja in izkušenj med zaposlenimi o informacijski varnosti učinkovito pomaga razumeti obstoječa pravila naše organizacije na tem področju.	1	2	3	4	5	6	7
Menim, da je izmenjava znanja in izkušenj med zaposlenimi o informacijski varnosti, običajna utečena praksa.	1	2	3	4	5	6	7

Starost (napišite število): let

Spol (obkrožite številko): 1 Moški
2 Ženski

Stopnja dosežene izobrazbe na področju zdravstvene nege (obkrožite številko):

1. SMS/ZT/TZN
2. viš. med. ses./viš. med. teh
3. dipl. m. s./dipl. zn
4. mag. zdr. nege

V kolikor ste poleg izobrazbe v zdravstveni negi dosegli še izobrazbo na drugih področjih, Vas prosimo, da jo označite (obkrožite številko):

1 visoko-strokovna izobrazba

2 strokovni magisterij

3 univerzitetna izobrazba

4 znanstveni magisterij

SD	Močno se ne strinjam	Se ne strinjam	Nevtralno	Se strinjam	Močno se strinjam
Vedno sem vljudna tudi do tistih, ki so zoprni.	1	2	3	4	5
V določenih primerih sem nekoga izkoristila.	1	2	3	4	5
Včasih raje poskušam poravnati račune kot odpustiti in pozabiti.	1	2	3	4	5
Če ni po moje, včasih zamerim.	1	2	3	4	5
Ne glede na to, s kom govorim, sem vedno dobra poslušalka.	1	2	3	4	5

10.5 FAKTORSKA ANALIZA ZA TPB KONSTRUKTE

Tabela: Kaiser-Meyer-Olkin (KMO) merilo in Bartlettov test sferičnosti za konstrukte TPB

KMO and Bartlett's Test		
Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		0,886
Bartlett's Test of Sphericity	Approx. Chi-Square	7543,721
	df	105
	Sig.	< 0,001

Tabela: Faktorska analiza za TPB konstrukte – prikaz lastnih vrednosti

Initial Eigenvalues			Extraction Sums of Squared Loadings			Rotation Sums of Squared Loadings		
Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
7,794	51,957	51,957	7,794	51,957	51,957	2,752	18,349	18,349
2,177	14,516	66,473	2,177	14,516	66,473	2,748	18,320	36,669
1,180	7,869	74,343	1,180	7,869	74,343	2,591	17,273	53,942
1,030	6,865	81,208	1,030	6,865	81,208	2,474	16,490	70,432
0,822	5,481	86,689	0,822	5,481	86,689	2,439	16,257	86,689
0,427	2,846	89,535						
0,319	2,123	91,658						
0,277	1,844	93,503						
0,201	1,338	94,841						
0,178	1,187	96,028						
0,146	0,970	96,998						
0,134	0,897	97,895						
0,124	0,827	98,722						
0,106	0,706	99,428						
0,086	0,572	100,000						

Extraction Method: Principal Component Analysis

10.6 FAKTORSKA ANALIZA ZA DIMENZIJE

Tabela: Kaiser-Meyer-Olkin (KMO) merilo in Bartlettov test sferičnosti za konstrukte ISC

KMO and Bartlett's Test		
Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		0,952
Bartlett's Test of Sphericity	Approx. Chi-Square	21915,799
	df	595
	Sig.	0,000

Tabela: Faktorska analiza za konstrukte dimenzij – prikaz lastnih vrednosti

	Initial Eigenvalues			Extraction Sums of Squared Loadings			Rotation Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	18,265	52,186	52,186	18,098	51,708	51,708	4,501	12,860	12,860
2	4,045	11,558	63,744	3,856	11,017	62,725	3,766	10,759	23,619
3	1,654	4,726	68,470	1,448	4,136	66,861	3,743	10,696	34,315
4	1,299	3,711	72,181	1,127	3,221	70,082	3,525	10,070	44,385
5	1,050	3,000	75,181	0,920	2,629	72,710	3,116	8,902	53,287
6	0,986	2,819	78,000	0,809	2,311	75,021	2,597	7,419	60,705
7	0,961	2,747	80,746	0,797	2,278	77,300	2,497	7,134	67,839
8	0,853	2,437	83,183	0,725	2,070	79,370	2,009	5,741	73,581
9	0,708	2,022	85,205	0,546	1,559	80,929	1,774	5,069	78,650
10	0,660	1,886	87,091	0,502	1,435	82,365	1,300	3,715	82,365
11	0,468	1,336	88,427						
12	0,399	1,139	89,567						
13	0,365	1,043	90,609						
14	0,263	0,750	91,359						
15	0,257	0,734	92,094						
16	0,237	0,677	92,771						
17	0,232	0,662	93,432						
18	0,211	0,604	94,036						
19	0,200	0,571	94,607						
20	0,189	0,541	95,148						
21	0,186	0,532	95,680						
22	0,170	0,485	96,164						
23	0,148	0,423	96,587						
24	0,148	0,422	97,009						
25	0,140	0,400	97,409						
26	0,135	0,387	97,796						
27	0,120	0,343	98,139						
28	0,116	0,331	98,470						
29	0,101	0,287	98,757						
30	0,091	0,260	99,018						
31	0,089	0,254	99,272						
32	0,078	0,222	99,494						
33	0,071	0,202	99,696						
34	0,057	0,162	99,858						
35	0,050	0,142	100,000						

Extraction Method: Principal Axis Factoring.

10.7 FACTOR LOADINGS

Tabela: Cross loadings among items (discriminant validity)

	ATB	BI	ISK	ISKS	MON	NB	PBC	PCM	PO	RM	SETA	SN	SO	TMC
SN1	0,533	0,530	-0,115	-0,144	-0,171	0,567	0,273	-0,184	-0,220	-0,148	-0,174	**0,826**	-0,257	-0,158
SN2	0,574	0,575	-0,120	-0,159	-0,148	0,611	0,272	-0,210	-0,220	-0,141	-0,197	**0,867**	-0,242	-0,155
SN3	0,535	0,574	-0,136	-0,145	-0,111	0,624	0,285	-0,163	-0,232	-0,138	-0,176	**0,849**	-0,249	-0,162
PBC1	0,287	0,373	-0,152	-0,091	-0,116	0,324	**0,990**	-0,101	-0,076	-0,091	-0,189	0,308	-0,101	-0,152
PBC2	0,235	0,346	-0,132	-0,090	-0,124	0,292	**0,912**	-0,101	-0,060	-0,077	-0,150	0,298	-0,103	-0,144
PBC3	0,274	0,338	-0,118	-0,070	-0,092	0,281	**0,838**	-0,086	-0,092	-0,074	-0,129	0,290	-0,068	-0,121
BI1	0,646	**0,944**	-0,118	-0,114	-0,110	0,660	0,351	-0,162	-0,180	-0,090	-0,156	0,633	-0,204	-0,140
BI2	0,636	**0,942**	-0,131	-0,120	-0,122	0,669	0,374	-0,142	-0,177	-0,096	-0,156	0,613	-0,204	-0,124
BI3	0,622	**0,942**	-0,160	-0,155	-0,148	0,681	0,365	-0,170	-0,195	-0,120	-0,170	0,622	-0,231	-0,154
NB1	0,639	0,633	-0,166	-0,128	-0,129	**0,811**	0,280	-0,212	-0,313	-0,148	-0,200	0,639	-0,295	-0,186
NB2	0,436	0,577	-0,167	-0,188	-0,211	**0,853**	0,288	-0,205	-0,247	-0,251	-0,286	0,629	-0,363	-0,217
NB3	0,517	0,625	-0,208	-0,207	-0,204	**0,913**	0,277	-0,220	-0,320	-0,216	-0,279	0,566	-0,387	-0,207
PO1	-0,263	-0,167	0,205	0,257	0,184	-0,252	-0,012	0,417	**0,824**	0,253	0,294	-0,224	0,526	0,288
PO2	-0,264	-0,168	0,239	0,272	0,202	-0,269	-0,053	0,416	**0,870**	0,271	0,309	-0,234	0,560	0,310
PO3	-0,209	-0,189	0,320	0,408	0,309	-0,357	-0,113	0,444	**0,984**	0,370	0,434	-0,270	0,672	0,377
PO4	-0,262	-0,204	0,297	0,357	0,271	-0,331	-0,109	0,408	**0,976**	0,308	0,385	-0,243	0,664	0,356
PO5	-0,133	-0,117	0,269	0,411	0,272	-0,284	-0,063	0,391	**0,708**	0,334	0,382	-0,182	0,640	0,364
SO1	-0,151	-0,181	0,423	0,533	0,446	-0,366	-0,064	0,527	0,646	0,503	0,577	-0,251	**0,880**	0,558
SO2	-0,134	-0,209	0,448	0,544	0,480	-0,371	-0,095	0,547	0,620	0,521	0,604	-0,267	**0,903**	0,531
SO3	-0,174	-0,210	0,442	0,534	0,444	-0,366	-0,066	0,549	0,642	0,517	0,591	-0,292	**0,934**	0,543
SO4	-0,144	-0,236	0,391	0,512	0,396	-0,377	-0,086	0,488	0,593	0,448	0,552	-0,282	**0,930**	0,495
SO5	-0,103	-0,137	0,418	0,471	0,395	-0,284	-0,138	0,469	0,530	0,432	0,500	-0,175	**0,687**	0,436
PCM1	-0,177	-0,171	0,446	0,432	0,440	-0,205	-0,080	**0,934**	0,421	0,546	0,548	-0,226	0,470	0,510
PCM2	-0,197	-0,195	0,505	0,494	0,495	-0,274	-0,092	**1,085**	0,457	0,576	0,610	-0,229	0,571	0,574
PCM3	-0,076	-0,083	0,510	0,499	0,566	-0,173	-0,116	**0,666**	0,338	0,645	0,610	-0,140	0,481	0,582
PCM4	-0,065	-0,079	0,530	0,527	0,593	-0,160	-0,077	**0,564**	0,373	0,661	0,631	-0,113	0,502	0,595
RM1	-0,063	-0,123	0,583	0,546	0,641	-0,220	-0,043	0,612	0,292	**0,924**	0,675	-0,177	0,482	0,662
RM2	-0,059	-0,105	0,607	0,579	0,686	-0,245	-0,104	0,637	0,338	**1,006**	0,716	-0,157	0,519	0,675
RM3	-0,047	-0,059	0,629	0,639	0,718	-0,178	-0,095	0,625	0,318	**0,757**	0,703	-0,116	0,510	0,719

	ATB	BI	ISK	ISKS	MON	NB	PBC	PCM	PO	RM	SETA	SN	SO	TMC
SETA1	-0,118	-0,167	0,546	0,588	0,584	-0,319	-0,103	0,600	0,384	0,671	**0,974**	-0,224	0,563	0,591
SETA2	-0,094	-0,139	0,552	0,600	0,601	-0,288	-0,092	0,618	0,376	0,679	**0,859**	-0,193	0,562	0,610
SETA3	-0,127	-0,159	0,604	0,669	0,633	-0,216	-0,204	0,599	0,346	0,628	**0,862**	-0,181	0,588	0,699
SETA4	-0,068	-0,107	0,566	0,664	0,652	-0,166	-0,208	0,519	0,276	0,648	**0,664**	-0,115	0,484	0,657
TMC1	-0,116	-0,133	0,670	0,672	0,682	-0,223	-0,151	0,629	0,366	0,692	0,698	-0,169	0,558	**0,941**
TMC2	-0,108	-0,132	0,674	0,682	0,705	-0,229	-0,147	0,609	0,364	0,709	0,703	-0,169	0,556	**0,941**
TMC3	-0,116	-0,150	0,686	0,673	0,713	-0,207	-0,151	0,613	0,362	0,725	0,719	-0,173	0,553	**0,918**
TMC4	-0,123	-0,142	0,649	0,685	0,709	-0,233	-0,125	0,591	0,358	0,710	0,688	-0,191	0,552	**0,967**
MON1	-0,058	-0,131	0,689	0,684	**0,968**	-0,205	-0,130	0,562	0,264	0,722	0,690	-0,158	0,477	0,717
MON2	-0,088	-0,138	0,695	0,666	**0,965**	-0,195	-0,111	0,555	0,264	0,695	0,667	-0,172	0,454	0,695
MON3	-0,052	-0,104	0,661	0,654	**0,862**	-0,194	-0,098	0,536	0,261	0,679	0,655	-0,140	0,455	0,675
ISK1	-0,140	-0,169	**0,990**	0,615	0,684	-0,204	-0,119	0,522	0,258	0,613	0,598	-0,155	0,413	0,625
ISK2	-0,103	-0,124	**0,936**	0,616	0,631	-0,190	-0,148	0,528	0,292	0,603	0,580	-0,135	0,457	0,663
ISK3	-0,041	-0,091	**0,762**	0,672	0,671	-0,175	-0,133	0,495	0,278	0,594	0,630	-0,100	0,452	0,647
ISKS1	-0,078	-0,158	0,618	**1,042**	0,610	-0,223	-0,064	0,523	0,385	0,574	0,651	-0,183	0,534	0,649
ISKS2	-0,045	-0,110	0,650	**0,935**	0,707	-0,190	-0,106	0,510	0,328	0,615	0,714	-0,158	0,534	0,675
ISKS3	-0,036	-0,110	0,631	**0,750**	0,627	-0,139	-0,079	0,498	0,337	0,559	0,638	-0,146	0,547	0,639
ISKS4	-0,040	-0,114	0,635	**0,858**	0,658	-0,177	-0,088	0,493	0,348	0,590	0,659	-0,147	0,548	0,652
ATB1	**0,857**	0,583	-0,075	-0,050	-0,022	0,514	0,246	-0,138	-0,249	-0,054	-0,081	0,523	-0,146	-0,077
ATB2	**0,906**	0,593	-0,126	-0,057	-0,078	0,573	0,270	-0,162	-0,234	-0,073	-0,127	0,609	-0,140	-0,141
ATB3	**0,883**	0,606	-0,088	-0,043	-0,087	0,537	0,250	-0,139	-0,205	-0,039	-0,115	0,576	-0,147	-0,105

Opombe: Analiza v programu SmartPLS4: analiza Consistent PLS-SEM algorithm settings: initial weights: 1.0; max. number of iterations: 3000; stop criterion:10^{-7}; type of results: standardized; Lohmoeller settings? No; weighting scheme: factor

10.8 CROMBAH ALPHA

Tabela: Izračun notranje skladnosti (n = 527)

Construct	CA	Item	CA if Item deleted	Item-total correlation	Inter-item correlations* (range)
ATB	0,911	ATB1	0,895	0,798	[0,723; 0,811]
		ATB2	0,838	0,866	
		ATB3	0,885	0,807	
SN	0,885	SN1	0,815	0,801	[0,608; 0,856]
		SN2	0,753	0,867	
		SN3	0,922	0,672	
NB	0,877	NB1	0,858	0,754	[0,635; 0,801]
		NB2	0,881	0,746	
		NB3	0,739	0,861	
PBC	0,939	PBC1	0,917	0,864	[0,809; 0,852]
		PBC2	0,894	0,893	
		PBC3	0,920	0,861	
BI	0,960	BI1	0,942	0,913	[0,883; 0,892]
		BI2	0,938	0,918	
		BI3	0,943	0,912	
PCM	0,901	PCM1	0,890	0,729	[0,592; 0,824]
		PCM2	0,862	0,816	
		PCM3	0,863	0,804	
		PCM4	0,874	0,778	
RM	0,925	RM1	0,904	0,832	[0,776; 0,828]
		RM2	0,871	0,873	
		RM3	0,900	0,841	
SETA	0,904	SETA1	0,876	0,791	[0,586; 0,937]
		SETA2	0,876	0,790	
		SETA3	0,862	0,823	
		SETA4	0,889	0,762	
TMC	0,969	TMC1	0,958	0,928	[0,832; 0,933]
		TMC2	0,951	0,952	
		TMC3	0,955	0,939	
		TMC4	0,973	0,873	
MON	0,952	MON1	0,942	0,883	[0,856; 0,891]
		MON2	0,926	0,906	
		MON3	0,922	0,910	
ISK	0,927	ISK1	0,917	0,823	[0,781; 0,847]
		ISK2	0,877	0,873	
		ISK3	0,889	0,857	
ISKS	0,947	ISKS1	0,940	0,839	[0,775; 0,865]
		ISKS2	0,927	0,880	
		ISKS3	0,931	0,866	
		ISKS4	0,920	0,903	
PO	0,940	PO1	0,928	0,827	[0,630; 0,896]
		PO2	0,924	0,858	
		PO3	0,921	0,867	
		PO4	0,915	0,901	
		PO5	0,943	0,763	
SO	0,938	SO1	0,921	0,848	[0,662; 0,839]
		SO2	0,921	0,845	
		SO3	0,911	0,900	
		SO4	0,921	0,845	
		SO5	0,942	0,739	

10.9 PROTOKOL ZA ZAŠČITO PODATKOV

Ime raziskave	Povezanost dimenzij informacijske varnostne kulture z namero izvedbe kršitev informacijske varnosti s strani zaposlenih v zdravstveni negi – presečna raziskava
Kdo zbira podatke	Raziskovalka zgoraj navedene raziskave je avtorica doktorskega dela Samanta Mikuletič, mag. zdr. nege, s šifro 40675 (izven evidenc ARRS). Raziskava nima plačnika oziroma ni sofinancirana. Doktorska disertacija nastaja pod mentorstvom izr. prof. dr. Boštjana Žvanuta ter somentorstvom red. prof. dr. Brigite Skele-Savič, na Fakulteti za zdravstvo Angele Boškin. Podatke pod somentorstvom Samante Mikuletič, mag. zdr. nege, zbira tudi študentka Fatima Halilovič, dipl. m.s.
Recenzija znanstvene veljavnosti raziskave	Komisija za oceno primernosti teme in oceno doktorske disertacije: red. prof. dr. Danica Železnik (predsednica), izr. prof. dr. Uroš Rajkovič (član), izr. prof. dr. Mirna Macur (članica).
Potrebna soglasja	Sklep upravnega odbora Zbornice-Zveze (sodelovanje odobreno 20. 5. 2020). Presoja in odobritev Državne etične komisije za medicinsko etiko (v nadaljevanju KME) (27. 12. 2020).
Namen raziskave/zbiranja podatkov	Preučiti pojav nepooblaščenega dostopa do zdravstvenih podatkov na slovenski populaciji zaposlenih v zdravstveni negi ter povezanost dimenzij informacijske varnostne kulture s stališči do vedenja, subjektivnimi normami, z normativnimi prepričanji, zaznanim vedenjskim nadzorom ter namero za izvedbo omenjene kršitve.
Ocena etičnih in zakonskih vidikov raziskave, tveganja za respondente	KME je raziskavo potrdila kot etično sprejemljivo, vendar je zaradi narave teme raziskave, ki zajema podatke o varovanju zasebnosti in zasebnih podatkov v zdravstveni praksi, svetovala, da vnaprej izdelamo protokol, kako ravnati s podatki, pridobljenimi med raziskavo, ki kažejo na obstoj kaznivih dejanj (v zvezi z varovanjem zasebnosti) po veljavni slovenski kazenski zakonodaji, ki se preganjajo po uradni dolžnosti zoper znanega ali zoper neznanega storilca. KME je svetovala, da se respondente vnaprej nedvoumno opozori, da utegnejo s svojimi odgovori razkriti prekrške in kazniva dejanja (v zvezi z varstvom zasebnosti), ki se preganjajo po uradni dolžnosti. Teorija načrtovanega vedenja in številne raziskave obravnavajo vedenjsko namero kot dober prediktor vedenja samega. Raziskava ne bo imela tveganj ali obremenitev za vključene osebe v raziskavi. Omejitev raziskave je uporaba ankete za vrednotenje vedenjske namere. Z anketo bomo merili vedenjsko namero nepooblaščenega dostopa do podatkov zaposlenih v zdravstveni negi in ne dejanskega vedenja – kršitve. V nagovoru ankete je povezava do podrobnejšega opisa raziskave, v katerem smo respondente opozorili, da s svojimi odgovori lahko razkrijejo prekrške in kazniva dejanja.
Zagotovitev anonimnosti osebnih podatkov	Z anketo ne zbiramo osebnih podatkov pacientov ali osebnih – določljivih podatkov respondentov in predvsem ne elektronskih naslovov ali IP številke računalnika. V demografskih podatkih so vprašanja respondentom naslovljena na zaposlitveni status, dobo dela v organizaciji, tip organizacije in okolje organizacije v kateri je respondent zaposlen, starost, spol, stopnja dosežene izobrazbe na področju zdravstvene nege in dosežena izobrazba na drugih področjih.

Obveščena privolitev respondentov	Respondentom je v nagovoru ankete, na povezavi ponujen v branje podrobnejši opis raziskave, ter možnost, da se neposredno z vprašanji o sami raziskavi obrnejo na avtorja-raziskovalca. S klikom na gumb »naprej« se respondenti strinjajo s sodelovanjem v raziskavi. Nagovor vsebuje tudi opis, da je sodelovanje v raziskavi prostovoljno in da sodelovanje lahko prekinejo na katerikoli točki izpolnjevanja ankete.
Posredovanje informacij o raziskavi	Podrobnejše informacije o raziskavi so respondentom na voljo na dodatni povezavi v nagovoru ankete. Respondentom je na voljo tudi kontakt raziskovalca, na katerega se lahko obrnejo v primeru vprašanj v zvezi s samo raziskavo.
Zagotovitev anonimnosti	Z anketo ne bomo zbirali osebnih podatkov iz katerih bi lahko sklepali na posameznika. Ni vprašanj o imenu in priimku, prebivališču, imenu organizacije zaposlitve.
Udeleženci raziskave	Udeleženci so zaposleni v zdravstveni negi v Republiki Sloveniji.
Na kakšen način se zbira podatke?	Izvedena bo presečna raziskava z enkratnim vzorcem, s pomočjo odprtokodne aplikacije 1KA. Prijava v ARNES račun in dostop do urejanja in objave spletne ankete.
Kdo bo imel dostop do podatkov. Kakšen bo ta dostop in zakaj?	Dostop do podatkovne baze imajo izr. prof. dr. Boštjan Žvanut, Samanta Mikuletič, mag. zdr. nege in Fatima Halilovič, dipl. m.s. Dostop do podatkovne baze je potreben zaradi pregleda števila izpolnjenih anket in koordinacije poteka raziskave.
Koliko časa se bodo hranili podatki?	Podatki se zbirajo dokler ne dobimo velikost vzorca 500 enot.
Kje se bodo hranili podatki?	Podatkovna baza se bo hranila na osebnem računalniku Samante Mikuletič.
Kako se bo uničilo originalne ankete?	Originalna anketa bo uničena po zadostnem številu polno izpolnjenih anket – t.j. vsaj 500 enot.
Objava rezultatov	Rezultati bodo objavljeni v sklopu raziskovalnega dela in ostalih raziskovalnih poročilih. Predstavljeni bodo tudi na sekciji, ki bo organizirana pod okriljem Zbornice – Zveze.

10.10 SKLEP ZBORNICE – ZVEZE

Zbornica zdravstvene in babiške nege Slovenije -
Zveza strokovnih društev medicinskih sester, babic in zdravstvenih tehnikov Slovenije
Ob železnici 30 a, Ljubljana tel: 01/544 54 80; E-mail: tajnistvo@zbornica-zveza.si

Ljubljana, 22. 5. 2020

Samanta Mikuletič
Veliko Brdo 21
6254 Jelšane

samanta.mikuletic@gmail.com

Spoštovani,

sporočamo vam, da se je Upravni odbor Zbornice zdravstvene in babiške nege – Zveze strokovnih društev medicinskih sester, babic in zdravstvenih tehnikov Slovenije (v nadaljevanju Zbornica – Zveza) na svoji redni 45. seji, dne 20. 5. 2020 seznanil z vašo prošnjo.

Posredujemo vam sprejeti sklep:

Sklep UO 615/45

Člani Upravnega odbora Zbornice – Zveze so sprejeli sklep o sodelovanju pri raziskavi doktorske študentke Fakultete zdravstvene vede Angele Boškin Samante Mikuletič z objavo e-ankete v junijskih in julijskih e-novicah. Samanto Mikulič se pozove, da Zbornici – Zvezi posreduje povezavo do omenjene e-ankete. Prav tako se jo pozove, da rezultate ankete predstavi na nacionalnem dogodku Zbornice – Zveze, ki bo organiziran v prihodnosti. Sklep stopi v veljavo takoj.

Z lepimi pozdravi

Anita Prelec,
izvršna direktorica Zbornice – Zveze

Prelec Anita

10.11 OCENA ETIČNOSTI RAZISKAVE

Podpisnik: Božidar Štefan Voljč
Izdajatelj: Republika Slovenija
Serijska številka: b4 b6 55 be 00 00 00 00 56 7b e7 4d
Datum podpisa: 11:08, 25.02.2021
Referenčna številka: 0120-583/2020/7

REPUBLIKA SLOVENIJA
MINISTRSTVO ZA ZDRAVJE
Komisija Republike Slovenije za medicinsko etiko

Samanta Mikuletič, mag. zdr. neg.
Veliko Brdo 21
6254 Jelšane

samanta.mikuletic@gmail.com

Številka: 0120-583/2020/7
Datum: 25. 2. 2021

Zadeva: Ocena etičnosti predložene raziskave
Zveza: vaša vloga z dne 27. 12. 2020

Spoštovani,

Komisija Republike Slovenije za medicinsko etiko (v nadaljevanju KME RS) je dne 27. 12. 2020 prejela vašo vlogo za oceno etičnosti raziskave z naslovom »Povezanost dimenzij informacijske varnostne kulture z namero izvedbe kršitev informacijske varnosti s strani zaposlenih v zdravstveni negi - presečna raziskava«.

Raziskava bo potekala v okviru doktorske naloge Samante Mikuletič, mag. zdr. neg. pod mentorstvom izr. prof. dr. Boštjana Žvanut ter somentorstvom red. prof. dr. Brigite Skele-Savič, na Fakulteti za zdravstvo Angele Boškin. Namen doktorske disertacije je preučiti pojav nepooblaščenega dostopa do zdravstvenih podatkov na slovenski populaciji zaposlenih v zdravstveni negi ter povezanost dimenzij informacijske varnostne kulture s stališči do vedenja, subjektivnimi normami, z normativnimi prepričanji, zaznanim vedenjskim nadzorom ter namero za izvedbo omenjene kršitve.

KME RS je na videokonferenčni seji 16. februarja 2021[1] obravnavala prejeto vlogo in ugotovila, da je vloga popolna ter raziskava etično sprejemljiva. S tem vam za njeno izvedbo izdaja svoje soglasje.
Dodatno pa zaradi narave teme raziskave, ki zajema podatke o varovanju zasebnosti in zasebnih podatkov v zdravstveni praksi, KME RS raziskovalki, mentorju in somentorici svetuje, da vnaprej izdelajo protokol, kako ravnati s podatki, pridobljenimi med raziskavo, ki kažejo na obstoj kaznivih dejanj (v zvezi z varovanjem zasebnosti) po veljavni slovenski kazenski zakonodaji (KZ-1), ki se preganjajo po uradni dolžnosti (ZKP; KZ-1), zoper znanega ali zoper neznanega storilca. KME RS svetuje, da se respondente vnaprej nedvoumno opozori, da

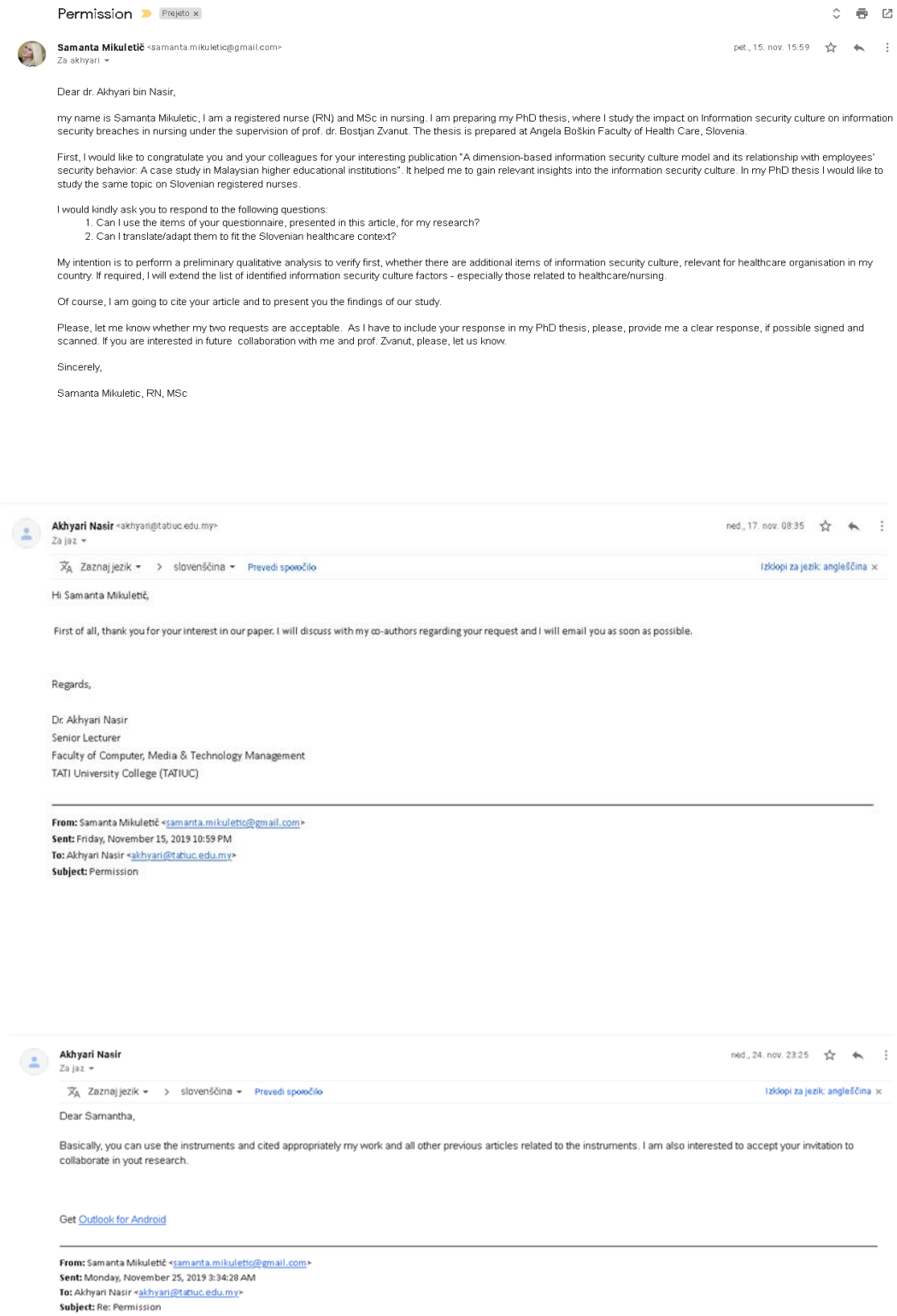
Pri nadaljnjih dopisih v zvezi z raziskavo se obvezno sklicujte na številko tega dopisa.

S spoštovanjem,

dr. Božidar Voljč, dr. med.,
predsednik KME RS

Vročiti:
- naslovniku – po e-pošti

10.12 DOVOLJENJE ZA UPORABO VPRAŠALNIKA



Permission Prejeto ×

Samanta Mikuletič <samanta.mikuletic@gmail.com> pet., 15. nov. 15:59
Za akhyari

Dear dr. Akhyari bin Nasir,

my name is Samanta Mikuletic, I am a registered nurse (RN) and MSc in nursing. I am preparing my PhD thesis, where I study the impact on Information security culture on information security breaches in nursing under the supervision of prof. dr. Bostjan Zvanut. The thesis is prepared at Angela Boškin Faculty of Health Care, Slovenia.

First, I would like to congratulate you and your colleagues for your interesting publication "A dimension-based information security culture model and its relationship with employees' security behavior: A case study in Malaysian higher educational institutions". It helped me to gain relevant insights into the information security culture. In my PhD thesis I would like to study the same topic on Slovenian registered nurses.

I would kindly ask you to respond to the following questions:

1. Can I use the items of your questionnaire, presented in this article, for my research?
2. Can I translate/adapt them to fit the Slovenian healthcare context?

My intention is to perform a preliminary qualitative analysis to verify first, whether there are additional items of information security culture, relevant for healthcare organisation in my country. If required, I will extend the list of identified information security culture factors - especially those related to healthcare/nursing.

Of course, I am going to cite your article and to present you the findings of our study.

Please, let me know whether my two requests are acceptable. As I have to include your response in my PhD thesis, please, provide me a clear response, if possible signed and scanned. If you are interested in future collaboration with me and prof. Zvanut, please, let us know.

Sincerely,

Samanta Mikuletic, RN, MSc

Akhyari Nasir <akhyari@tatiuc.edu.my> ned., 17. nov. 08:35
Za jaz

Zaznaj jezik > slovenščina Prevedi sporočilo Izklopi za jezik: angleščina ×

Hi Samanta Mikuletič,

First of all, thank you for your interest in our paper. I will discuss with my co-authors regarding your request and I will email you as soon as possible.

Regards,

Dr. Akhyari Nasir
Senior Lecturer
Faculty of Computer, Media & Technology Management
TATI University College (TATIUC)

From: Samanta Mikuletič <samanta.mikuletic@gmail.com>
Sent: Friday, November 15, 2019 10:59 PM
To: Akhyari Nasir <akhyari@tatiuc.edu.my>
Subject: Permission

Akhyari Nasir ned., 24. nov. 23:25
Za jaz

Zaznaj jezik > slovenščina Prevedi sporočilo Izklopi za jezik: angleščina ×

Dear Samantha,

Basically, you can use the instruments and cited appropriately my work and all other previous articles related to the instruments. I am also interested to accept your invitation to collaborate in yout research.

Get Outlook for Android

From: Samanta Mikuletič <samanta.mikuletic@gmail.com>
Sent: Monday, November 25, 2019 3:34:28 AM
To: Akhyari Nasir <akhyari@tatiuc.edu.my>
Subject: Re: Permission

10.13 PREVERJANJE PRISTRANOSTI

Tabela: Kaiser-Meyer-Olkin merilo in Bartlettov test sferičnosti za Harmanov enofaktorski test

KMO and Bartlett's Test		
Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		0,937
Bartlett's Test of Sphericity	Approx. Chi-Square	29995,107
	df	1225
	Sig.	0,000

Tabela: Harmanov enofaktorski test

Total Variance Explained						
	Initial Eigenvalues			Extraction Sums of Squared Loadings		
Factor	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	19,184	38,369	38,369	18,675	37,350	37,350
2	7,242	14,484	52,852			
3	3,876	7,751	60,604			
4	2,161	4,322	64,926			
5	1,688	3,376	68,302			
6	1,498	2,995	71,297			
7	1,087	2,174	73,471			
8	1,069	2,138	75,609			
9	1,044	2,088	77,697			
10	0,978	1,957	79,654			
11	0,908	1,816	81,470			
12	0,861	1,723	83,193			
13	0,754	1,507	84,700			
14	0,676	1,352	86,052			
15	0,630	1,260	87,312			
16	0,465	0,930	88,242			
17	0,434	0,868	89,110			
18	0,389	0,778	89,889			
19	0,348	0,696	90,584			
20	0,321	0,643	91,227			
21	0,290	0,579	91,806			
22	0,270	0,540	92,346			
23	0,246	0,493	92,839			
24	0,242	0,484	93,322			
25	0,232	0,463	93,786			
26	0,216	0,432	94,218			
27	0,203	0,407	94,624			
28	0,187	0,374	94,999			
29	0,186	0,371	95,370			
30	0,178	0,355	95,725			
31	0,173	0,346	96,071			
32	0,157	0,315	96,386			
33	0,153	0,306	96,691			
34	0,147	0,294	96,985			
35	0,139	0,278	97,263			
36	0,134	0,268	97,531			
37	0,129	0,259	97,789			
38	0,122	0,244	98,033			
39	0,117	0,234	98,267			
40	0,107	0,214	98,481			
41	0,102	0,205	98,686			
42	0,098	0,196	98,881			
43	0,088	0,176	99,058			
44	0,086	0,172	99,230			
45	0,082	0,164	99,394			
46	0,076	0,151	99,545			
47	0,065	0,131	99,676			
48	0,061	0,123	99,798			
49	0,053	0,107	99,905			
50	0,048	0,095	100,000			

Legenda: Extraction Method: Principal Axis Factoring.

10.14 IZRAČUN POVEZANOSTI DIMENZIJ IN STAROSTI

Tabela: Povezanost dimenzij in spremenljivke starost

		Starost	PO	SO	PCM	RM	SETA	TMC	MON	ISK	ISKS
Starost	Pearson Correlation	1	-0,011	0,012	0,157**	0,211**	0,159**	0,164**	0,150**	0,075	0,098*
	Sig. (2-tailed)		0,801	0,778	0,000	0,000	0,000	0,000	0,001	0,085	0,024
PO	Pearson Correlation	-0,011	1	0,663**	0,439**	0,334**	0,379**	0,373**	0,271**	0,288**	0,372**
	Sig. (2-tailed)	0,801		0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000
SO	Pearson Correlation	0,012	0,663**	1	0,558**	0,524**	0,600**	0,562**	0,471**	0,460**	0,566**
	Sig. (2-tailed)	0,778	0,000		0,000	0,000	0,000	0,000	0,000	0,000	0,000
PCM	Pearson Correlation	0,157**	0,439**	0,558**	1	0,673**	0,653**	0,633**	0,584**	0,548**	0,543**
	Sig. (2-tailed)	0,000	0,000	0,000		0,000	0,000	0,000	0,000	0,000	0,000
RM	Pearson Correlation	0,211**	0,334**	0,524**	0,673**	1	0,720**	0,724**	0,714**	0,630**	0,618**
	Sig. (2-tailed)	0,000	0,000	0,000	0,000		0,000	0,000	0,000	0,000	0,000
SETA	Pearson Correlation	0,159**	0,379**	0,600**	0,653**	0,720**	1	0,715**	0,684**	0,625**	0,700**
	Sig. (2-tailed)	0,000	0,000	0,000	0,000	0,000		0,000	0,000	0,000	0,000
TMC	Pearson Correlation	0,164**	0,373**	0,562**	0,633**	0,724**	0,715**	1	0,716**	0,679**	0,693**
	Sig. (2-tailed)	0,000	0,000	0,000	0,000	0,000	0,000		0,000	0,000	0,000
MON	Pearson Correlation	0,150**	0,271**	0,471**	0,584**	0,714**	0,684**	0,716**	1	0,692**	0,685**
	Sig. (2-tailed)	0,001	0,000	0,000	0,000	0,000	0,000	0,000		0,000	0,000
ISK	Pearson Correlation	0,075	0,288**	0,460**	0,548**	0,630**	0,625**	0,679**	0,692**	1	0,665**
	Sig. (2-tailed)	0,085	0,000	0,000	0,000	0,000	0,000	0,000	0,000		0,000
ISKS	Pearson Correlation	0,098*	0,372**	0,566**	0,543**	0,618**	0,700**	0,693**	0,685**	0,665**	1
	Sig. (2-tailed)	0,024	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000	

**Correlation is significant at the 0.01 level (2-tailed), *Correlation is significant at the 0.05 level (2-tailed).
n = 527, dimenzije ISC povprečje

10.15 IZRAČUN POVEZANOSTI DIMENZIJ IN DELOVNE DOBE

Tabela: Povezanosti dimenzij in spremenljivke delovna doba v organizaciji

			Delovna doba	PO	SO	PCM	RM	SETA	TMC	MON	ISK	ISKS
Spearman's rho	**Delovna doba**	Correlation Coefficient	1,000	-0,011	-0,011	0,167**	0,123**	0,142**	0,105*	0,117**	0,063	0,056
		Sig. (2-tailed)	.	0,804	0,809	0,000	0,005	0,001	0,016	0,007	0,151	0,196
	PO	Correlation Coefficient	-0,011	1,000	0,711**	0,443**	0,398**	0,451**	0,456**	0,367**	0,351**	0,467**
		Sig. (2-tailed)	0,804	.	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000
	SO	Correlation Coefficient	-0,011	0,711**	1,000	0,564**	0,528**	0,595**	0,560**	0,494**	0,456**	0,572**
		Sig. (2-tailed)	0,809	0,000	.	0,000	0,000	0,000	0,000	0,000	0,000	0,000
	PCM	Correlation Coefficient	0,167**	0,443**	0,564**	1,000	0,679**	0,645**	0,627**	0,591**	0,524**	0,549**
		Sig. (2-tailed)	0,000	0,000	0,000	.	0,000	0,000	0,000	0,000	0,000	0,000
	RM	Correlation Coefficient	0,123**	0,398**	0,528**	0,679**	1,000	0,706**	0,710**	0,710**	0,619**	0,629**
		Sig. (2-tailed)	0,005	0,000	0,000	0,000	.	0,000	0,000	0,000	0,000	0,000
	SETA	Correlation Coefficient	0,142**	0,451**	0,595**	0,645**	0,706**	1,000	0,703**	0,692**	0,617**	0,712**
		Sig. (2-tailed)	0,001	0,000	0,000	0,000	0,000	.	0,000	0,000	0,000	0,000
	TMC	Correlation Coefficient	0,105*	0,456**	0,560**	0,627**	0,710**	0,703**	1,000	0,734**	0,661**	0,694**
		Sig. (2-tailed)	0,016	0,000	0,000	0,000	0,000	0,000	.	0,000	0,000	0,000
	MON	Correlation Coefficient	0,117**	0,367**	0,494**	0,591**	0,710**	0,692**	0,734**	1,000	0,689**	0,693**
		Sig. (2-tailed)	0,007	0,000	0,000	0,000	0,000	0,000	0,000	.	0,000	0,000
	ISK	Correlation Coefficient	0,063	0,351**	0,456**	0,524**	0,619**	0,617**	0,661**	0,689**	1,000	0,670**
		Sig. (2-tailed)	0,151	0,000	0,000	0,000	0,000	0,000	0,000	0,000	.	0,000
	ISKS	Correlation Coefficient	0,056	0,467**	0,572**	0,549**	0,629**	0,712**	0,694**	0,693**	0,670**	1,000
		Sig. (2-tailed)	0,196	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000	.

**Correlation is significant at the 0.01 level (2-tailed), *Correlation is significant at the 0.05 level (2-tailed), n = 527, dimenzije ISC povprečje

10.16 REZULTATI MANN-WHITNEYEVEGA U TESTA

Tabela: Man Whitneyeu U test za razlike v zaznavanju dimenzij med spoloma

Dimenzije ISC	Spol	N	Mean Rank	Sum of Ranks
PO_povprecje	moški	70	253,81	17767,00
	ženski	457	265,56	121361,00
	Total	527		
SO_povprecje	moški	70	241,99	16939,50
	ženski	457	267,37	122188,50
	Total	527		
PCM_povprecje	moški	70	230,06	16104,00
	ženski	457	269,20	123024,00
	Total	527		
RM_povprecje	moški	70	235,16	16461,00
	ženski	457	268,42	122667,00
	Total	527		
SETA_povprecje	moški	70	235,43	16480,00
	ženski	457	268,38	122648,00
	Total	527		
TMC_povprecje	moški	70	223,01	15611,00
	ženski	457	270,28	123517,00
	Total	527		
MON_povprecje	moški	70	207,92	14554,50
	ženski	457	272,59	124573,50
	Total	527		
ISK_povprecje	moški	70	226,62	15863,50
	ženski	457	269,73	123264,50
	Total	527		
ISKS_povprecje	moški	70	217,82	15247,50
	ženski	457	271,07	123880,50
	Total	527		