Colloquium 2(62)/2026
ISSN 2081-3813, e-ISSN 2658-0365
CC BY-NC-ND.4.0
DOI: http://doi.org/10.34813/29coll2026

POLSKA ADAPTACJA NARZĘDZI DO POMIARU BEZPIECZEŃSTWA INFORMACYJNEGO WŚRÓD PERSONELU MEDYCZNEGO

Polish adaptation of tools for measuring information security among healthcare employees

Andrzej Piotrowski
Uniwersytet Gdański/Uniwersytet Pomorski w Słupsku
e-mail: andrzej.piotrowski@ug.edu.pl
ORCID 0000-0003-1192-2695

Streszczenie

Naruszanie prawa związane z ujawnianiem tzw. danych wrażliwych pacjentów jest niezwykle ważnym problemem. Przyczyną większości przypadków jest zaniedbanie i/lub niedbalstwo pracowników. Przeprowadzono adaptację kulturową kwestionariusza *Information Security Climate Scale oraz Safety Indicators to the Information Security Domain* służących od oceny klimatu organizacyjnego dbania o bezpieczeństwo informacji. Badanie przeprowadzono na grupie 238 pielęgniarek. Dokonano analizy rzetelności skal oraz przeprowadzono czynnikową analizę konfirmacyjną. Analizy wykazały, że kwestionariusze mają zadowalające właściwości psychometryczne. W *Information Security Climate Scale α Cronbacha* wynosi 0,78, a dla skali *Safety Indicators to the Information Security Domain* ma wartość 0,94. Wykonane analizy konfirmacyjne odpowiadają pozytywnie na pytanie, czy hipotetycznie założony model może być zweryfikowany rozkładem wyników pochodzących z macierzy danych. Dobre właściwości psychometryczne sprawiają, że adaptowane skale są dokładnymi i rzetelnymi narzędziami, które mogą być wykorzystywane do diagnozy bezpieczeństwa informacyjnego w organizacjach medycznych.

Słowa kluczowe: ochrona informacji, bezpieczeństwo informacji, analiza ryzyka.

Abstract

Unlawful disclosure of the so-called *sensitive personal data* of patients is a very significant problem. Employee carelessness is the cause in most instances. A cultural adaptation of the *Information Security Climate Scale* and *Safety Indicators to the Information Security Domain* questionnaire has been carried out. The questionnaire measures the organizational information security climate. The study was carried out on a sample of 238 female nurses. Reliability analyses and confirmatory factor analyses have been carried out. Analyzes have shown that the questionnaires have satisfactory psychometric properties. Cronbach's α for the *Information Security Climate Scale* was 0.78 and 0.94 for *Safety Indicators to the Information Security Domain*. The confirmatory factor analysis has confirmed that the hypothetical model can be verified by the distribution of results from the data matrix. Good psychometric properties make the adapted

questionnaires an accurate and reliable tool which can be used to diagnose information security in medical organizations.

Keywords: information protection, information security, risk analysis.

Wprowadzenie

Pomimo nieustannego postępu technicznego w zakresie informatyzacji (Samy i in., 2010) oraz wprowadzania restrykcyjnych przepisów prawnych (Štarchoň i Pikulík, 2019) następuje wzrost poziomu naruszania wrażliwych danych osobowych (Schatz i Bashroush, 2019). Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych służy implementowaniu rozporządzenia Parlamentu Europejskiego i Rady (UE) z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych. Przepisy szczegółowe w ochronie zdrowia dotyczą tajemnicy lekarskiej, pielęgniarskiej, tajemnicy obowiązującej u pracowników administracji medycznej, obejmują prawo administracyjne, cywilne, karne, pracy (Jackowski, 2018).

Koszt naruszenia danych osobowych w sektorze opieki medycznej w USA szacuje się na 7 biliona dolarów rocznie (Fernández-Alemán i in., 2015). Dane te mogą być niedoszacowane z powodu niewykrycia utraty danych osobowych przez organizację (lub przeciwnie – chęci ukrycia tego faktu przed opinią publiczną z obawy przed utratą reputacji i pacjentów).

Media przytaczają spektakularne przypadki nieuprawnionego dostępu hakerów do informacji medycznych pacjentów, jednak prawie 60% naruszeń ochrony medycznych danych osobowych wynika z nieostrożności i niedbałości personelu i/lub nieprzestrzegania zasad i procedur bezpieczeństwa informacji (Verizon Risk Team, 2022). Za taki stan odpowiada brak kultury, postaw i konkretnych zachowań w obszarze bezpieczeństwa (Simmonds, 2021). Praktyki z obszaru cyberbezpieczeństwa w opiece medycznej są na znacznie niższym poziomie w porównaniu z innymi branżami, jak np. finansowa (Apkan, 2016). Zapobieganie naruszania danych wiąże się ze zmianą zachowań i postaw personelu opieki zdrowotnej oraz podmiotów z nimi współpracujących (Blumenthal i McGraw, 2015).

Branża medyczna jest jedyną, która ma więcej podmiotów wewnętrznych niż zewnętrznych odpowiedzialnych za naruszanie wrażliwych danych osobowych. Problemem stają się ataki typu *ransomware*, które stanowią ponad 80% wszystkich złośliwych oprogramowań w ochronie zdrowia. Niskie ryzyko wykrycia przestępcy, łatwość przeprowadzenia ataku, niski poziom zabezpieczeń, nieprzestrzeganie procedur, a także możliwość uzyskania wysokiego okupu powodują, że instytucje medyczne są bardzo narażone na utratę kontroli nad danymi osobowymi pacjentów i personelu. Dodatkowo wysokie koszty ewentualnych odszkodowań i możliwa utrata reputacji powodują, że są one bardziej skłonne zapłacić okup. Dane medyczne należą do informacji szczególnie

wrażliwych z uwagi na swoją wartość. Konsekwencje nielegalnego ich pozyskania może być niewłaściwe wykorzystanie przez nieuprawnione podmioty (Anderson i in., 2017).

Największa ilość danych medycznych tracona jest poprzez kanał elektroniczny (hakowanie) (McCoy i Perlis, 2018) oraz kradzieże sprzętu, takiego jak laptopy czy tablety, na których znajdują się niezabezpieczone informacje (Liu i in., 2015). Utrata danych spowodowana jest brakiem przestrzegania procedur, przekazywaniem informacji nieuprawnionym osobom i nieostrożnym zachowaniem personelu (Peikari i in., 2018). W celu właściwego diagnozowania i leczenia pacjenci muszą przekazywać wszystkie kluczowe informacje dostarczycielom usług medycznych. Obawy pacjentów o nieuprawnione ujawnienie i niewłaściwe wykorzystanie wrażliwych danych medycznych, a także informacji o wstydliwych chorobach mogą spowodować, że pacjenci odmówią przekazania w procesie leczenia ważnych informacji. W rezultacie takie obawy i nieujawnienie istotnych informacji pogorszyć mogą stan zdrowia pacjentów, narażając ich na ryzyko niewłaściwej diagnozy oraz stosowanych procedur medycznych.

Opierając się na wynikach badań i analiz nad bezpieczeństwem informacji w ochronie zdrowia, skupiamy się na postawach i zachowaniach pracowników, analizując je w kontekście klimatu organizacyjnego często utożsamianego z kulturą organizacyjną. Klimat organizacyjny zdefiniowany może być wąsko jako „wspólne postrzeganie tego, jak funkcjonuje organizacja" (Reichers i Schneider, 1990) lub szerzej jako „wspólne postrzeganie i znaczenie przywiązywane do zasad, praktyk i procedur, których doświadczają pracownicy, oraz zachowania, które są nagradzane oraz wspierane i oczekiwane" (Schneider i in., 2013). Tak rozumiane podejście do klimatu organizacyjnego zostało z powodzeniem zastosowane do zmiany postaw i zachowań pracowników. Przykłady odnoszą się do klimatu bezpieczeństwa (Potter i in., 2017), klimatu różnorodności (Madera i in., 2016), klimatu przepracowania (Piotrowski i Jurek, 2019), klimatu etycznego (Chen i in., 2019) i klimatu sprawiedliwości (Nicholas i Breakey, 2017). Cechą wspólną wymienionych obszarów jest to, że pomimo istnienia właściwych zasad, procedur szkolenia i ocen nie były one wystarczające do wprowadzenia trwałych zmian zachowań pracowników. Zastosowanie podejścia klimatu organizacyjnego umożliwia identyfikację kluczowych obszarów oraz wskazanie pożądanych zmian w zakresie postaw i zachowań (Piotrowski, 2014).

Cel badań

Celem prezentowanego badania jest dostarczenie badaczom oraz praktykom zarządzania w obszarze medycznym polskiej wersji kwestionariuszy do oceny klimatu bezpieczeństwa informacyjnego. Zastosowanie takiego narzędzia wskaże obszary, na które powinny być ukierunkowane interwencje w celu podniesienia poziomu bezpieczeństwa.

Materiał i metody

Udostępnione przez autorów za pisemną zgodą kwestionariusze *Information Security Climate Scale* (18 itemów, np.: „Dokładam dodatkowych starań, aby chronić poufne dane w miejscu pracy") oraz *Safety Indicato to the Information Security Domain* (9 itemów, np.: „Mój przełożony udziela pochwały za każdym razem, gdy widzi działania podjęte w celu ochrony prywatnych danych") (Kessler i in., 2020), poddano procedurze tłumaczenia. Osoba będąca psychologiem i jednocześnie anglistą przetłumaczyła kwestionariusz na język polski. Następnie inna osoba o takich samych kwalifikacjach przetłumaczyła zwrotnie kwestionariusz na język angielski. Ustalono następnie przez dwóch ekspertów ostateczną wersję polskiego tłumaczenia. W każdej ze skal osoba badana odnosi się do stwierdzeń na 5-punktowej skali typu Likerta od 1 *zdecydowanie nie zgadzam się* do 5 *zdecydowanie zgadzam się*.

Charakterystyka grupy badanej

Zbadano 238 pielęgniarek (kobiet) w wieku M = 42,74; SD = 9,62; min. 22 lata, max. 67 lat. Wykształcenie średnie miało 16% osób, 42% osób ukończyło studia licencjackie, a 42% pielęgniarki miały tytuł magistra.

Statystyczna analiza danych

W pierwszej kolejności zanalizowano statystyki opisowe i korelacje między poszczególnymi pozycjami kwestionariusza (r Pearsona). Następnie wykonano konfirmacyjną analizę czynnikową przy użyciu programu Amos. Ocenę psychometrycznych właściwości uzyskanych w ten sposób skal przeprowadzono, obliczając statystyki opisowe i korelacje oraz dokonując analizy zgodności wewnętrznej i trafności kryterialnej skal kwestionariusza. Do tych analiz wykorzystano program Statistica 13.1 i IBM SPSS Amos 25.

Wymagania etyczne

Badanie było dobrowolne i anonimowe. Respondenci świadomie wyrazili zgodę na udział w badaniu. Badania przeprowadzono zgodnie z wytycznymi Deklaracji Helsińskiej oraz Polskiego Towarzystwa Psychologicznego.

Wyniki

Statystyki opisowe i korelacje między pozycjami

Analiza statystyk opisowych dla poszczególnych pozycji polskiej wersji (Tab. 1) pozwala stwierdzić, że najwyższą średnią *Information Security Climate Scale* (ISCS)

osiągnęła pozycja *znaczenie* (*M* = 9,33; *SD* = 5,05), natomiast najniższą pozycja *rozluźnienie* (*M* = 5,72; *SD* = 3,69).

W skali *Safety Indicators to the Information Security Domain* (SIISD) najwyższą średnią w skali bezpieczeństwa informacji osiągnęła pozycja *Motywacja – bezpieczeństwo* (*M* = 11,76; *SD* = 5,53), natomiast najniższą pozycja *Udział – bezpieczeństwo informacji* (*M* = 10,25, *SD* = 5,10).

Rzetelność skal

W celu oszacowania zgodności wewnętrznej dokonano analizy rzetelności za pomocą współczynnika α Cronbacha. Zgodność wewnętrzna, inaczej określana jako homogeniczność metody, oznacza stopień, w jakim dany test można uznać za miarę jednego konstruktu. W polskiej wersji dla skali *Information Security Climate Scale* α Cronbacha wynosi 0,78, zaś dla skali *Safety Indicators to the Information Security Domain* ma wartość 0,94. Statystyki opisowe i wartości α Cronbacha przedstawiono w tabeli nr 1.

Tabela 1

Statystyki opisowe i współczynniki rzetelności pozycji dla polskiej wersji Skali klimatu bezpieczeństwa informacji *oraz* Wskaźnika bezpieczeństwa zabezpieczenia informacji

Zmienne	*M*	*SD*	S	K	α
Skala klimatu bezpieczeństwa informacji					
Praktyki	7,44	4,68	–0,19	–1,11	0,86
Znaczenie	9,93	5,05	–1,06	–0,24	0,76
Niedbałość	5,72	3,69	0,10	–0,63	0,70
Wskaźnik bezpieczeństwa zabezpieczenia informacji					
Motywacja – bezpieczeństwo	11,76	5,53	–1,54	0,55	0,84
Motywacja – bezpieczeństwo informacji	11,82	5,51	–1,56	0,65	0,87
Udział – bezpieczeństwo	10,36	5,12	–1,22	0,05	0,84
Udział – bezpieczeństwo informacji	10,25	5,10	–1,14	–0,05	0,85
Spełnienie – bezpieczeństwo	11,16	5,26	–1,46	0,52	0,89
Spełnienie – bezpieczeństwo informacji	11,07	5,29	–1,39	0,36	0,94

Źródło: opracowanie własne.

Trafność teoretyczna – konfirmacyjna analiza czynnikowa

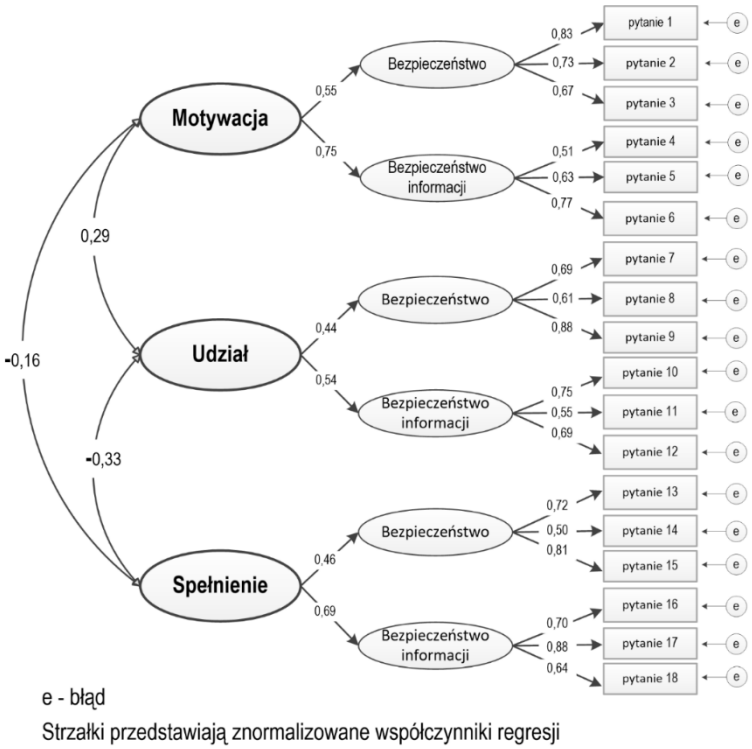
Najważniejszym, podstawowym i koniecznym rodzajem trafności jest trafność teoretyczna, czyli ocena, w jakim stopniu dany test odzwierciedla latentną cechę psychologiczną. Jedną z metod szacowania trafności teoretycznej jest badanie wewnętrznej struktury testu za pomocą konfirmacyjnej analizy czynnikowej, która ma na celu

sprawdzenie, czy dany test składa się z określonej – na podstawie teorii psychologicznej – liczby czynników. Użyto metody asymptotycznie wolnej od rozkładu, która nie wymaga założenia wielowymiarowego rozkładu normalnego.

Eksplorację rozpoczęto od sprawdzenia układu zależności, który przedstawiono w modelu teoretycznym (rysunek 1). W pierwszym modelu ścieżkowym znalazły się trzy zmienne latentne: *Motywacja*, *Udział* oraz *Spełnienie*. Wszystkie trzy zmienne składały się z dwóch czynników *Bezpieczeństwo* oraz *Bezpieczeństwo Informacji*. Dla każdej zmiennej – *Motywacja*, *Udział, Spełnienie* – czynniki składały się z innych pytań.

Rysunek 1

Model analizy konfirmacyjne dla Wskaźnika bezpieczeństwa zabezpieczenia informacji

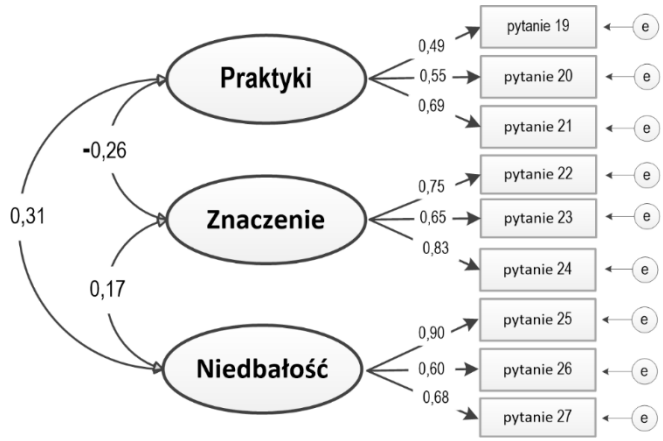


Źródło: opracowanie własne.

W drugim modelu ścieżkowym znalazły się trzy zmienne latentne: *Praktyki*, *Znaczenie* oraz *Niedbałość*. Na rysunku 2 przedstawiono wzajemne relacje w obu modelach występujące pomiędzy zmiennymi.

Rysunek 2

Model analizy konfirmacyjne dla Skali klimatu bezpieczeństwa informacji



Źródło: opracowanie własne.

W tabeli 2 zaprezentowano wskaźniki dopasowania modeli.

Tabela 2

Wskaźniki dopasowania modeli

Model	Chi^2	p	RMSA	LO	HI	GFI	AGFI	p–close
WBZI	55,54	< 0,001	0,035	0,025	0,052	0,95	0,90	0,23
SKBI	475,3	0,070	0,058	0,040	0,069	0,72	0,93	0,07

WBZI – *Wskaźnik bezpieczeństwa zabezpieczenia informacji*, SKBI – *Skala klimatu bezpieczeństwa informacji*;

p – poziom istotności; RMSEA – średni błąd aproksymacji; LO – niski RMSA; HI – wysoki RMSE; GFI – wskaźnik dobroci dopasowania; AGFI – wskaźnik dobroci dopasowania z poprawką; p–close – test dobroci dopasowania

Źródło: opracowanie własne.

Według Steingera (2007) oraz Browne'a i Cudecka (1993) model jest dobrze dopasowany do danych, jeśli wartość RMSEA wynosi między 0,006 a 0,008. Jeśli wartość jest większa niż 0,008, model źle pasuje do danych. Następnie GFI (wskaźnik dobroci dopasowania) powinien przekraczać 0,90 (McDonald i Marsh, 1990). Miara ta nie jest bezpośrednio związana z wielkością próbki. Dostarcza informacji, czy testowany model znacznie lepiej pasuje do danych niż żaden model (Joreskog i Sorbom, 1993).

W pierwszym modelu test RMSEA przyjął wartość 0,035, RMSEA LO (*low*) wynosił 0.025, a RMSEA HI (*high*) wynosił 0,052 i jest mniejsze o zalecanej wartości 0,08.

Wyliczona wartość w teście p–close wynosi 0,23, co świadczy o dobrym dopasowaniu modelu do danych. Współczynnik GFI wynosi 0,95 i jest mniejszy od zaleconej wartości 0,90.

W drugim modelu test RMSEA przyjął wartość graniczną 0,058. Nie przekroczył jednak wartości 0,08 i jest jeszcze akceptowalny. RMSEA LO (*low*) wynosił 0,040, a RMSEA HI (*high*) wynosił 0,069, co i tak mieści się w podanym zakresie (mniejszym od 0,08). Wyliczona wartość w teście p–close wynosi 0,11 co świadczy również o dobrym dopasowaniu modelu do danych. Z kolei współczynnik GFI opisuje, na ile kowariancje w próbie są wyjaśniane przez kowariancje wynikające w modelu. Dla modelu nasyconego wartość przyjmuje 1 i przyjmuje się, że GFI powinno przekraczać 0,90 i właśnie tyle, bo 0,92, wynosi wyliczona wartość tego miernika dopasowania modelu. Własności rozkładu chi–kwadrat sprawiają, że przy dużych próbach test łatwo odrzuca hipotezę zerową i tym samym dyskredytuje model, gdy tymczasem model może być jak najbardziej akceptowalny. W analizowanym przypadku model nie jest odrzucony, bowiem chi-kwadrat wynosi 32,36, zaś p = 0,07.

Podsumowując, można uznać, że przedstawione testy dobroci dopasowania modelu 1 i 2 odpowiadają pozytywnie na pytanie, czy hipotetycznie założony model może być zweryfikowany rozkładem wyników pochodzących z macierzy danych (Hornowska i Paluchowski, 2004).

Dyskusja wyników

Naruszanie wrażliwych danych medycznych wiąże się z dużymi problemami zarówno dla pacjentów, jak i instytucji świadczących opiekę medyczną. Brak było do tej pory polskich rzetelnych narzędzi identyfikujących poziom bezpieczeństwa informacji. Dziedziną, w której przetwarza się ogromną ilość wrażliwych informacji, jest branża medyczna. Aby dokonać adaptacji uznanych narzędzi służących do pomiaru bezpieczeństwa informacji, przeprowadzono badanie na jednorodnej grupie 238 pielęgniarek. W wyniku dokonanych analiz zaadaptowano dwie skale: 1) *Information Security Climate Scale,* 2) *Safety Indicators to the Information Security Domain*. Jak wspomniano uprzednio, przyczyną większości naruszeń jest zaniedbanie i/lub niedbalstwo pracowników związane z bezpieczeństwem informacyjnym, czego nie można w pełni naprawić poprzez środki prawne lub technologiczne. Aby móc skoncentrować się na zmianie zachowań personelu medycznego, wcześniej należy dokonać diagnozy problemu. Do tego służą adaptowane narzędzia. Narzędzia te mogą być wykorzystywane przez dostarczycieli opieki medycznej do szybkiej i niedrogiej oceny jakości bezpieczeństwa

informacyjnego. Pozwalają na podejmowanie decyzji dotyczących naruszeń przepisów i standardów tzw. danych wrażliwych.

Wnioski

Polskie wersje wskaźnika *Skali klimatu bezpieczeństwa informacji* i *Wskaźnika bezpieczeństwa zabezpieczenia informacji* to dobre narzędzia do pomiaru bezpieczeństwa informacji wśród pracowników ochrony zdrowia. Wskaźniki statystyczne pokazują, że modele dobrze pasują do danych, potwierdzając tym samym dokładność narzędzi. Akceptowalna (alfa Cronbacha dla *Skali klimatu bezpieczeństwa informacji* = 0,79 i *Wskaźnika bezpieczeństwa zabezpieczenia informacji* = 0,94) wewnętrzna spójność i rzetelność powodują, że *Skala klimatu bezpieczeństwa informacji* i *Wskaźnik bezpieczeństwa zabezpieczenia informacji* są przydatnymi narzędziami praktycznymi i badawczymi. Zwiększają one tym samym pulę nowoczesnych narzędzi przydatnych w badaniach w opiece medycznej (Ludwikowska-Świeboda i Lachowska, 2019; Szymańska-Pytlińska, 2019; Karasiewicz i in., 2004).

Zaadaptowane narzędzia mają ogólną konstrukcję pytań – mogą być stosowane w branżach innych niż medyczne. Mogą być stosowane w trakcie audytu identyfikującego obszary zagrożenia naruszania bezpieczeństwa danych osobowych oraz jako narzędzia interwencyjne po incydencie ujawnienia naruszenia procedur. Osoby pragnące skorzystać z zaadaptowanych skal proszone są o kontakt z autorem.

BIBLIOGRAFIA

Anderson, C., Baskerville, R. L., Kaul, M. (2017). Information security control theory: Achieving a sustainable reconciliation between sharing and protecting the privacy of information. *Journal of Management Information Systems, 34*(4), 1082–1112. https://doi.org/10.1080/07421222.2017.1394063

Apkan, N. (2016). *Hacking health care records reaches epidemic proportions.* https://www.scientificamerican.com/article/hacking-health-care-records-reaches--epidemic-proportions/ (dostęp: 29.12.2022).

Blumenthal, D., McGraw, D. (2015). Keeping personal health information safe: the importance of good data hygiene. *JAMA, 313*(14), 1424. https://doi.org/10.1001/jama.2015.2746

Browne, M. W., Cudeck, R. (1993). Alternative ways of assessing model fit. W: K.A. Bollen, J.S. Long (Eds.), *Testing structural equation models* (136–162). Sage.

Chen, H., Chau, P. Y. K., Li, W. (2019). The effects of moral disengagement and organizational ethical climate on insiders' information security policy violation behavior. *Information Technology & People, 32*(4), 973–992. https://doi.org/10.1108/ITP-12-2017-0421

Fernández-Alemán, J. L., Sánchez-Henarejos, A., Toval, A., Sánchez-García, A. B., Hernández-Hernández, I., Fernandez-Luque, L. (2015). Analysis of health professional security behaviors in a real clinical setting: an empirical study. *International Journal of Medical Informatics, 84*(6), 454–467. https://doi.org/10.1016/j.ijmedinf.2015.01.010

Hornowska, E., Paluchowski, J. (2004). Kulturowa adaptacja testów psychologicznych. W: J. Brzeziński (red.), *Metodologia badań psychologicznych. Wybór tekstów* (151–191). PWN.

Jackowski, M. (2018). *Ochrona danych medycznych. RODO w ochronie zdrowia*. Wolters Kluwer.

Joreskog, K., Sorbom, D. (1993) *LISREL 8: Structural Equation Modelling with the SIMPLIS Command Language*. Scientific Software International Inc.

Karasiewicz, K., Lewandowska-Walter, A., Godlewska-Werner, D., Piotrowski, A. (2004). Równowaga praca-dom według Polaków: prezentacja konstruktu i właściwości psychometrycznych kwestionariusza WLB. W: T. Rostowska, W. Budziński (red.), *Zawodowe i zdrowotne problemy człowieka w różnych okresach dorosłości: perspektywa psychologiczna* (38–63). Wydawnictwo Adam Marszałek.

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), 461–473. https://doi.org/10.1177/1460458219832048

Liu, V., Musen, M. A., Chou, T. (2015). Data breaches of protected health information in the United States. *JAMA, 313*(14), 1471–1473. https://doi.org/10.1001/jama.2015.2252

Ludwikowska-Świeboda, K., Lachowska, B. (2019). Polish version of the Inventory of Complicated Grief – preliminary validation. *Psychiatria Polska, 53*(5), 1069–1086. https://doi.org/10.12740/PP/91729

Madera, J. M., Dawson, M., Guchait, P. (2016). Psychological diversity climate: Justice, racioethnic minority status and job satisfaction. *International Journal of Contemporary Hospitality Management, 28*(11), 2514–2532. https://doi.org/10.1108/IJCHM-06-2015-0304

McCoy, T. H., Jr, Perlis, R. H. (2018). Temporal trends and characteristics of reportable health data breaches, 2010–2017. *JAMA, 320*(12), 1282–1284. https://doi.org/10.1001/jama.2018.9222

McDonald, R. P., Marsh, H. W. (1990). Choosing a multivariate model: Noncentrality and goodness of fit. *Psychological Bulletin, 107*(2), 247–255. https://doi.org/10.1037/0033-2909.107.2.247

Nicholas, P. K., Breakey, S. (2017). Climate change, climate justice, and environmental health: Implications for the nursing profession. *Journal of Nursing Scholarship, 49*(6), 606–616. https://doi.org/10.1111/jnu.12326

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), 102. https://doi.org/10.1186/s12911-018-0681-z

Piotrowski, A. (2014). Stres zawodowy a konflikty pomiędzy pracą a rodziną personelu medycznego Służby Więziennej. *Edukacja dla Bezpieczeństwa*, *2*(7), 295–306.

Piotrowski, A., Jurek, P. (2019). A preliminary adaptation and validation of the *Overwork Climate Scale* by Mazzetti, Schaufeli, Guglielmi and Depolo. *Medycyna pracy*, *70*(2), 177–188. https://doi.org/10.13075/mp.5893.00771

Potter, R. E., Dollard, M. F., Owen, M. S., O'Keeffe, V., Bailey, T., Leka, S. (2017). Assessing a national work health and safety policy intervention using the psychosocial safety climate framework. *Safety Science, 100*, 91–102. https://psycnet.apa.org/doi/10.1016/j.ssci.2017.05.011

Reichers, A. E., Schneider, B. (1990). Climate and culture: An evolution of constructs. W: B. Schneider, (red.), *Organizational Climate and Culture* (5–39). Jossey–Bass.

Samy, G. N., Ahmad, R., Ismail, Z. (2010). Security threats categories in healthcare information systems. *Health Informatics Journal*, *16*(3), 201–209. https://doi.org/10.1177/1460458210377468

Schatz, D., Bashroush, R. (2019). Security predictions – a way to reduce uncertainty. *Journal of Information Security and Applications, 45*, 107–116. https://doi.org/10.1016/j.jisa.2019.01.009

Schneider, B., Ehrhart, M. G., Macey, W. H. (2013). Organizational climate and culture. *Annual Review of Psychology*, *64*, 361–388. https://doi.org/10.1146/annurev--psych-113011-143809

Simmonds, M. (2021). Instilling a culture of data security throughout the organisation. *Network Security*, *2018*(6), 9–12. https://doi.org/10.1016/S1353-4858(18)30055-2

Steiger, J. H. (2007). Understanding the limitations of global fit assessment in structural equation modeling. *Personality and Individual differences*, *42*(5), 893–898. https://doi.org/10.1016/j.paid.2006.09.017

Štarchoň, P., Pikulík, T. (2019). GDPR principles in Data protection encourage pseudonymization through most popular and full-personalized devices-mobile phones. *Procedia Computer Science, 151*, 303–312. https://doi.org/10.1016/j.procs.2019.04.043

Szymańska-Pytlińska, M. (2019). Adaptation of the Body Image Self-Consciousness Scale (BISC-PL) in Polish females. *Psychiatria Polska*, *53*(5), 1087–1101. https://doi.org/10.12740/PP/95085

Verizon Risk Team. (2022). *Data breach investigations report.* https://www.verizon.com/business/en-gb/resources/2022-data-breach-investigations--report-dbir.pdf