Journal of Multidisciplinary Healthcare

Dovepress
open access to scientific and medical research

Open Access Full Text Article

ORIGINAL RESEARCH

Assessing staff awareness and effectiveness of educational training on IT security and privacy in a large healthcare organization

This article was published in the following Dove Press journal:
Journal of Multidisciplinary Healthcare

Mubashir Aslam Arain
Rima Tarraf
Armghan Ahmad

Health Systems Evaluation and Evidence, Alberta Health Services, Calgary, AB, Canada

Background: The increased use of health information systems and information technology (IT) in healthcare heightens the risk of security and privacy breaches. Necessary measures such as effective IT training and education are required to meet the challenges of protecting patient information.

Purpose: The objective of the study was to determine the effectiveness of existing educational and awareness modules in delivering the key messages around IT security and privacy.

Methods: The study was conducted in a large healthcare organization in Western Canada from September 2016 to March 2017. Using proportionate stratified random sampling, an online survey was distributed to all professional groups including clinical and non-clinical staff. In total, 586 participants responded to questions pertaining to whether or not they were aware of the IT education material, common potential breaches, and knowledge in preventing IT security and privacy breaches. Data were analyzed in SPSS version 19.

Results: The study found that most of the participants (80.9%) completed the online IT training. Staff perceived the online training as effective (57.5%). There was a significant positive correlation between staff perception about the effectiveness of IT security educational material and satisfaction with IT security in the organization (r=0.34, P<0.01). Those who completed the training were 4.2-times (CI=2.0–8.8) more likely to correctly report the action upon receiving spam emails than those who had not completed the training. The most common type of breach stated was not knowing how to encrypt emails when sending emails outside the organization. Only a small proportion of clinical (25.5%) and non-clinical staff (30.4%) reported knowing how to encrypt emails. Also, participants identified various strategies for improving the module content and compliance.

Conclusion: Online training provides a basic understanding of IT security and privacy concepts to prevent potential breaches. The training should be an integral part of healthcare staff continuing education to protect patient information.

Keywords: IT security modules, privacy in healthcare, healthcare staff and IT breaches, information storage & retrieval, IT security & privacy, computerized medical records system

Introduction

Electronic health information systems and information technology (IT) are increasingly being used in healthcare.[1–3] Although electronic information systems offer numerous benefits, health information stored in an electronic system poses unique risks to privacy and security.[2,3] Risks to IT security and privacy can include things such as copying or sharing of username/password, accidental disclosure of patient information, abuse of permission or insider curiosity of an employee, or visible patient information on

Correspondence: Mubashir Aslam Arain
Health Systems Evaluation and Evidence, Innovation and Research Management, Systems Innovations and Programs, Alberta Health Services 10301 Southport Lane SW, Calgary, AB T2W 1S7, Canada
Tel +1 403 943 0783
Fax +1 403 943 2875
Email mubashiraslam.arain@ahs.ca

submit your manuscript | www.dovepress.com
Dovepress
http://dx.doi.org/10.2147/JMDH.S183275

device screens.[4,5] Personal health information thefts and data security breaches are a growing concern. In 2013, the office of Civil Rights in the US had more than 77,000 complaints of breaches related to health information privacy violating the Health Insurance Portability and Accountability Act (HIPAA).[6]

In healthcare, these risks are especially pertinent, as personal health information contains sensitive and intimate details of patients' life. The theft, loss, or unauthorized use and disclosure of personal health information can have dire consequences. Some of these consequences are discrimination, stigmatization, and psychological or economic harm to the individual.[7–9] Additionally, if patients are not confident that their information will be kept secure, they may refrain from disclosing critical information or from seeking treatment.[3,10] Despite the risks to IT security of patient information, it is important for healthcare providers to have easy access to patient information for timely delivering and effective healthcare. In one report, 87% of 2,469 Canadians agreed that timely and easy access to personal health information is crucial for quality healthcare.[11]

In Canada, the Personal Information Protection and Electronic Documents Act (PIPEDA) grants individuals the right to know the reasons for collection or use of personal information. Healthcare organizations are responsible for the security, privacy, and confidentiality of information in their custody, and should protect this information reasonably and securely.[12] The healthcare organization included in this study was a large fully integrated health system consisting of five geographical zones with over 100,000 employees. The organization offers services at more than 650 facilities including hospitals, clinics, continuing care facilities, cancer centers, mental health facilities, and community health sites.[13] The organization developed a number of online education and awareness modules that target key points staff need to be aware of to understand their requirements for compliance based on legislative policies and Acts. E-learning enables knowledge management by simplifying the collaborative process with ease of content capture, continuous learning, and reuse.[14] E-learning has been widely adopted by many organizations to offer learning opportunities to employees as a cost-effective and time-saving method.[15] Although e-learning interventions are more effective than no training programs,[16] healthcare professional's attitude, satisfaction, and experience using computers and e-learning could be problematic, requiring further understanding and research.[17] The objective of the study was to determine the effectiveness and staff awareness of the IT security and privacy educational modules in a large healthcare organization.

Methods

We conducted a cross-sectional survey from September 2016 to March 2017 in a Western Canadian healthcare organization. Proportionate stratified random sampling methodology was used to ensure representation from different types of healthcare facilities and staff from different occupations. Our sampling framework also aimed to collect the highest responses from nursing staff, followed by clerical staff, and other non-regulated healthcare professionals.

The survey was developed by the authors; the questions were based on the exploratory qualitative study conducted prior to the survey.[13] The authors aligned survey questions with the key learning objectives from the educational modules and consulted e-learning literature.[18,19] Prior to distributing the survey, the authors shared it with key stakeholders to ensure questions were adequate and representative and piloted the survey with four management staff.

The survey was sent in two waves. As per our sampling framework, we randomly selected staff names from a master list using Excel's random number generator function. Staff received a brief description of the project and a personalized link to the survey. The email also emphasized that participation was voluntary, and all information provided was anonymous and confidential. In the first wave, we sent invitations to 2,000 staff. Staff were given 2 weeks to complete the survey; two emails were sent out as reminders. The first reminder was sent a week prior to the deadline, and the second reminder 2 days before the deadline. We collected 333 responses from the first wave, thus necessitating the need for a second wave of data collection. The target minimum sample required was 400 for this survey. The second invitation was sent to 1,000 staff following the same procedure and sampling framework as the first wave. The second sample excluded the 2,000 staff who were invited during the first wave. Module compliance was not an inclusion criteria, as we were interested in noting whether or not there would be any significant difference between those who had completed the training and those who had not. Figure 1 highlights the above-mentioned methodology and sampling framework visually.

We analyzed data using IBM SPSS Statistics version 19 (IBM Corporation, Armonk, NY, USA). We tested the effectiveness of current educational material and whether there were any differences in IT security and privacy awareness among different professional groups and between those who had and had not completed the training using descrip-

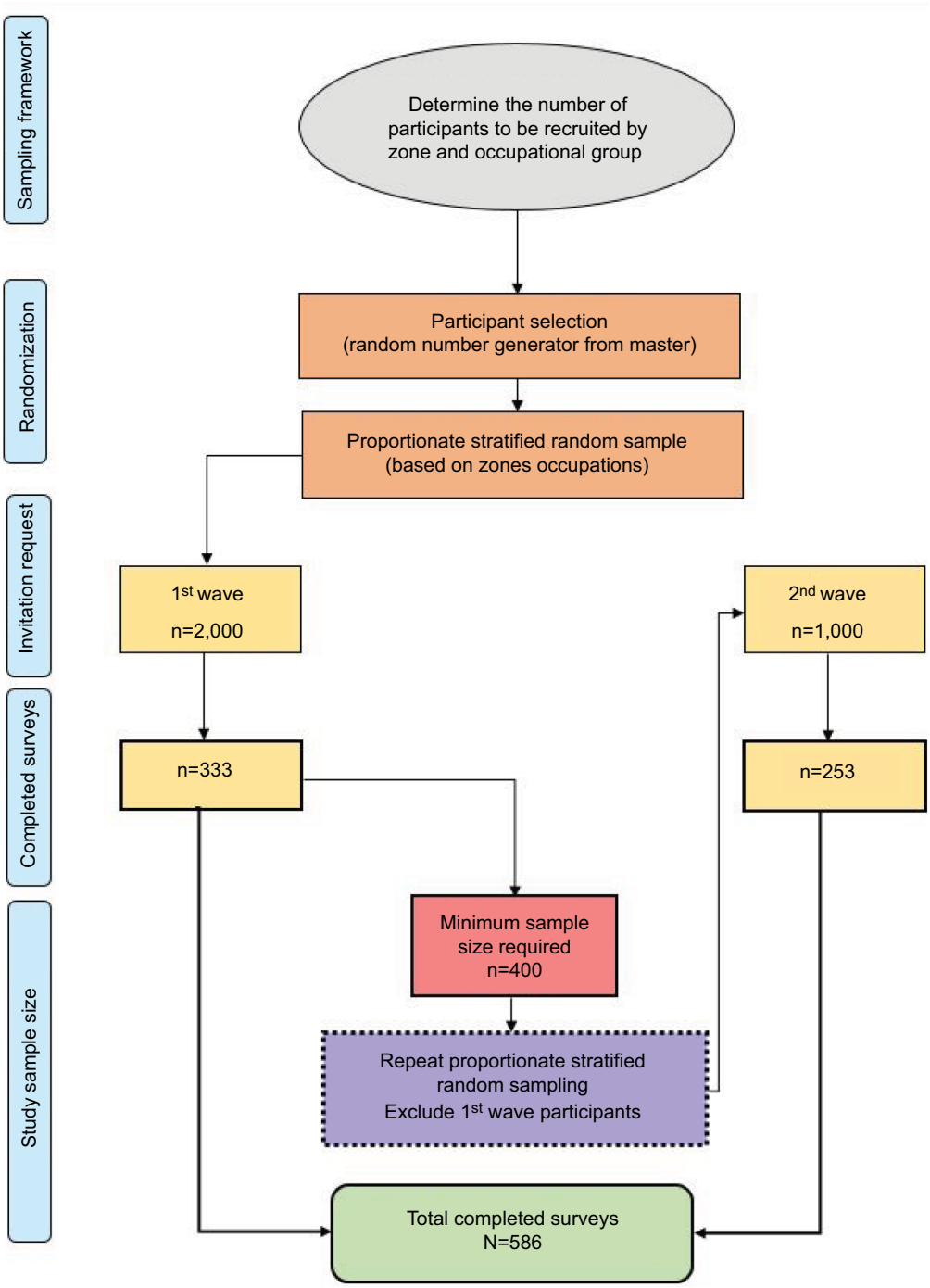

Figure 1 Overview of study methodology and sampling framework.

tive and inferential statistics. We used the chi-squared test for proportions/test for trends for categorical data and the Mann–Whitney U test for continuous data at 95% confidence level.

Description of modules

This study evaluates two specific IT training modules: Module I (Annual Continuing Education (ACE) Secure – Collect IT, Protect IT) and Module II (Information Privacy and IT Security Awareness).[13]

Module I: This module fulfilled requirements for Information Privacy and IT security training for all employees. It was a short online course that provided an overview of the privacy legislation, the responsibilities of workers to protect the privacy of individuals, confidentiality of information, and the security of IT resources.

Module II: This was a 60-minute training module that provided an overview of privacy legislation. It outlined staff responsibility to protect the privacy of individuals, confidentiality of information, and security of IT resources. Completion of the module was required within the first 3 months of employment or as designated by the employees' program.

Protection of human and animal subjects

This evaluation was considered a Quality Improvement project and did not require approval by an ethics review board. However, all data collection, management, and storing procedures complied with the Health Information Act and the Freedom of Information and Privacy Act. All participants were provided with information on the project and how the data would be used.

Results

In total, 586 staff participated in the study (20% response rate). Demographic information is presented in Table 1. There was an approximately equal distribution of clinical (51.5%) and non-clinical (47.6%) staff. A large proportion of participants were employed full-time (64.2%) and had worked in the organization for over 10 years (44.5%). Most of the participants were aware of (87.4%) and had completed the IT training modules (80.9%). To determine the representativeness of the sample, we compared the proportion of each professional group in the organization (Figure 2A) to their proportions in our sample (Figure 2B).

Around 25% of staff were very satisfied with IT security at the organization and around half of the survey participants were satisfied with IT security at the organization; others were either neutral or not satisfied (Figure 3). Most of the

Table 1 Demographic information of participants who completed the survey (N=586)

Demographic question	Number (%)
Participant groups	
Clinical	302 (51.5%)
Non-clinical	279 (47.6%)
No response	5 (0.9%)
Work pattern	
Full-time	376 (64.2%)
Part-time	202 (34.5%)
No response	8 (1.4%)
Number of years in the organization	
<5	180 (30.7%)
5–10	136 (23.2%)
>10	261 (44.5%)
No response	9 (1.5%)

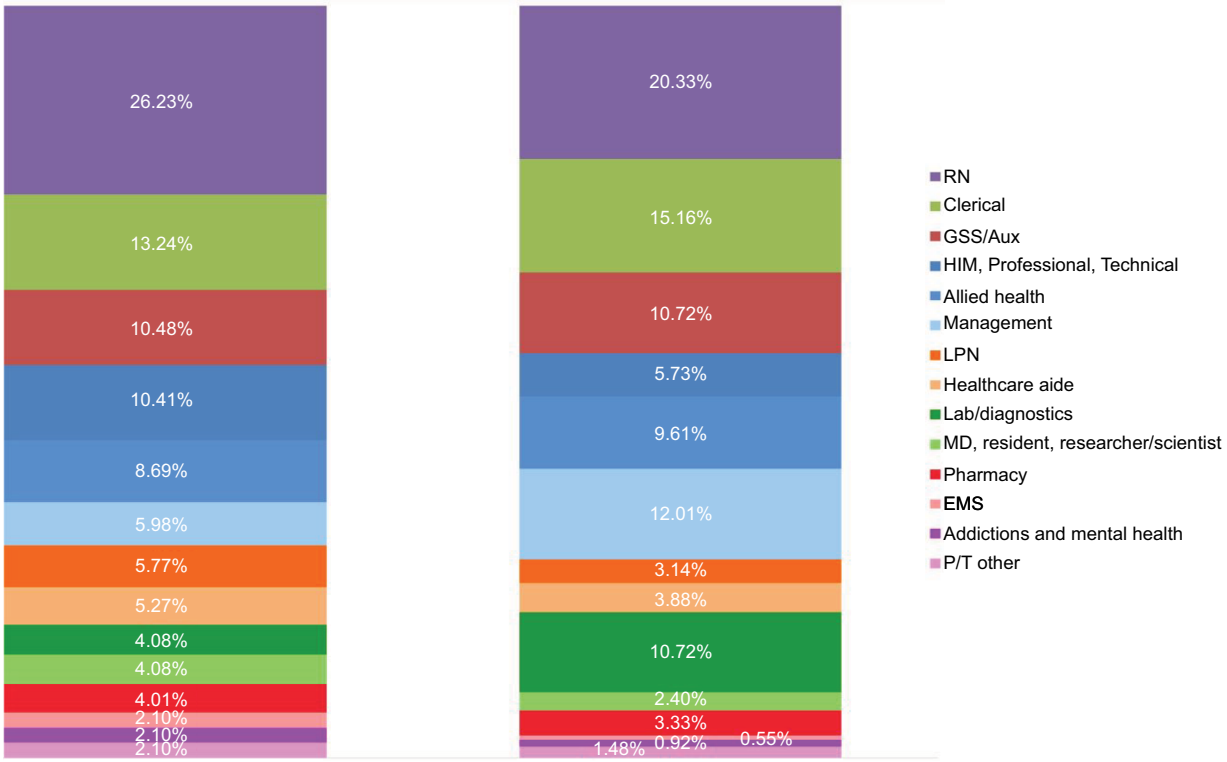

Figure 2 (**A**) Proportion of AHS staff members in different occupational groups. (**B**) Proportion of survey participants in different AHS occupational groups.
Abbreviations: AHS, Alberta Health Services; EMS, Emergency Medical Services; GSS/Aux, General Support Services/Auxiliary Nursing; HIM, Health Information Management; Lab, Laboratory; LPN, Licensed Practical Nurse; MD, Medical Doctor; P/T, Professional Technical; RN, Registered Nurse.

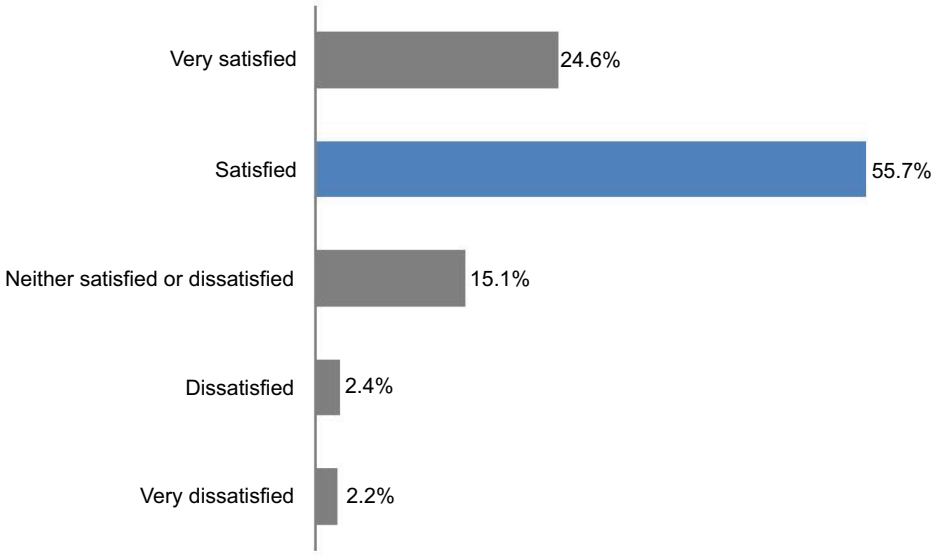

Figure 3 Participant satisfaction with IT security (n=582).
Abbreviation: IT, information technology.

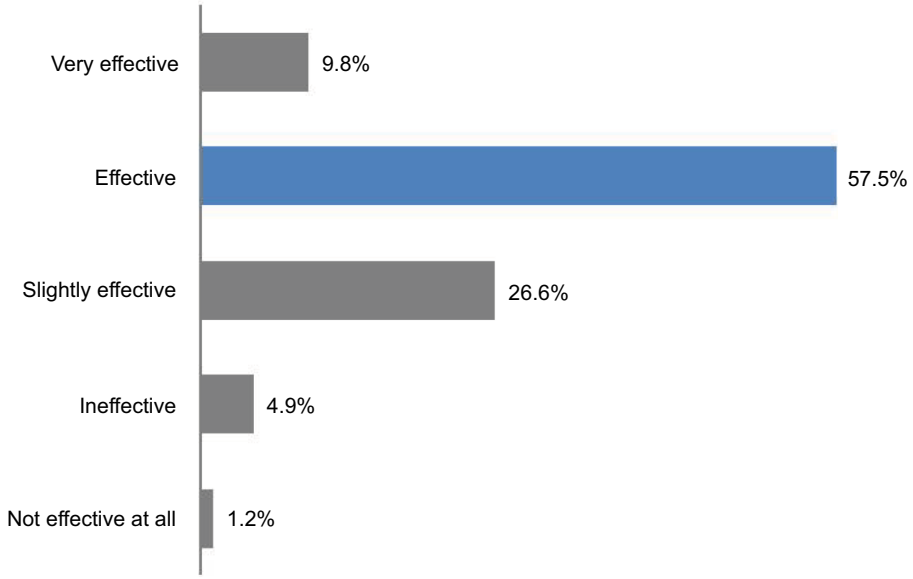

Figure 4 Participant perceptions of the two IT modules' effectiveness (combined) (n=492).
Abbreviation: IT, information technology.

Table 2 Comparing the knowledge and staff satisfaction level with IT security between those who had completed Module I at the time of survey and those who had not completed the module

Question	Those who completed the module	Those who had not completed	*P*-values
Correct action upon receiving spam emails (n=583), n (%)	196 (41.6)	15 (13.4)	<0.01[a]
Understand how to encrypt emails (n=537), n (%)	134 (29.6)	15 (17.6)	0.02[a]
Shared login information with other employees (n=538), n (%)	29 (6.4)	6 (7.1)	0.82
Ever reported an IT security incident (n=583) , n (%)	94 (19.9)	13 (11.8)	0.05
Average satisfaction score (1–5) with IT security (n=582), score (SD)	4.01 (0.80)	3.85 (0.95)	0.09
Average number of years worked in the organization (n=577), n (SD)	12.28 (9.46)	10.79 (10.28)	0.14

Note: [a]Significant differences at the 95% confidence level ($P<0.05$).
Abbreviation: IT, information technology.

participants perceived the two modules as effective (57.5%) in delivering the key messages around IT security and privacy (Figure 4). We found a significant positive correlation between staff perception about the effectiveness of IT security educational material and satisfaction with IT security in the organization (r=0.34, P<0.01).

Tables 2 and 3 show that those who had completed the IT security and privacy module were significantly more likely to know how to respond to spam and how to encrypt emails compared to those who had not completed the module. Those who completed the module were also more likely to report IT security incidences. The average satisfaction with the organizational IT security was also slightly higher among those who had completed the module than among those who had not completed it; however, this difference was not significant (P>0.05).

Overall, there was little difference between clinical and non-clinical staff (Table 4). The majority of clinical and non-clinical staff were aware of the IT modules; of those, most

Table 3 Comparing the knowledge and staff satisfaction level with IT security between those who had completed Module II at the time of survey and those who had not completed the module

Question	Those who had completed the module	Those who had not completed	*P*-values
Correct action upon receiving spam emails (n=478), n (%)	178 (40.4)	8 (21.6)	0.03[a]
Understand how to encrypt emails (n=452), n (%)	124 (29.7)	9 (26.5)	0.69
Shared login information with other employees (n=452), n (%)	26 (6.2)	3 (8.8)	0.47
Ever reported an IT security incident (n=480), n (%)	87 (19.6)	4 (10.8)	0.19
Average satisfaction score (1–5) with IT security (n=479), score (SD)	3.99 (0.84)	3.95 (0.78)	0.51
Average number of years worked in the organization (n=473), n (SD)	12.27 (9.45)	10.00 (10.16)	0.16

Note: [a]Significant differences at the 95% confidence level (P<0.05).
Abbreviation: IT, information technology.

Table 4 Comparing the awareness level of IT security and privacy modules between clinical and non-clinical staff

Question	Participant groups		*P*-values
	Clinical	Non-clinical	
Aware of Module I (n=575), n (%)	269 (89.7)	233 (84.5)	0.08
Completed Module I (n=581), n (%)	248 (82.1)	221 (79.2)	0.38
Aware of Module II (n=570), n (%)	248 (83.5)	231 (84.6)	0.72
Completed Module II (n=477), n (%)	229 (92.3	211 (92.1)	0.94
New employees receive login information within the first week of work (n=514), n (%)	196 (72.3)	193 (79.4)	0.06
Understand how to encrypt emails (n=533), n (%)	73 (25.5)	75 (30.4)	0.21
Shared login information with other employees (n=534), n (%)	18 (6.3)	17 (6.9)	0.78
Correct action upon receiving spam emails (n=579), n (%)	98 (32.6)	111 (39.9)	0.07
Average satisfaction score (1–5) with IT security in the organization (n=578), score (SD)	3.99 (0.79)	3.97 (0.88)	0.87

Abbreviation: IT, information technology.

Table 5 Comparing the awareness level of IT security and privacy modules between full-time and part-time staff members

Question	Staff work pattern		*P*-values
	Full-time	Part-time	
Aware of Module I (n=572), n (%)	331 (88.7)	170 (85.4)	0.25
Completed Module I (n=578), n (%)	316 (84.0)	155 (76.7)	0.03[a]
Aware of Module II (n=567), n (%)	309 (84.0)	166 (83.4)	0.87
Completed Module II (n=473), n (%)	290 (94.2)	149 (90.3)	0.12
New employees receive login information within the first week of work (n=511), n (%)	255 (75.9)	131 (74.9)	0.80
Understand how to encrypt emails (n=530), n (%)	106 (30.5)	42 (23.1)	0.07
Shared login information with other employees (n=530), n (%)	22 (6.3)	12 (6.6)	0.92
Correct action upon receiving spam emails (n=576), n (%)	153 (40.9)	56 (27.7)	<0.01[a]
Average satisfaction score (1–5) with IT security in the organization (n=575), score (SD)	3.98 (0.85)	3.98 (0.79)	0.91

Note: [a]Significant differences at the 95% confidence level (P<0.05).
Abbreviation: IT, information technology.

participants had completed them. A few participants reported sharing their login information (6.6%). Clinical staff (32.9%) were slightly less likely to correctly identify how to deal with spam emails than non-clinical staff (39.9%). Moreover, only a small proportion of clinical (25.5%) and non-clinical staff (30.4%) reported knowing how to encrypt emails.

Full-time staff members were more likely to have completed Module I than part-time staff members (Table 5). Also, full-time staff were more likely to correctly report the action required upon receiving spam emails. No other differences were found between the full-time and part-time staff.

Table 6 shows that those who completed Module I were 4.2-times (CI =2.0–8.8) more likely to correctly report the action required upon receiving spam emails than those who had not completed Module I. Other variables in the model did not show any significant difference.

Content improvement

Many participants expressed the need for instructions on how to encrypt emails and for tips on how to recognize spam. Some participants identified the lack of information with regard to the risks and consequences of breaches. Another recurring "missing" feature from the module was information on breaches and how often they occur in the organization. Several participants also conveyed interest in learning about the risk of breach when using social media.

Participants offered several suggestions on how to improve IT security modules:

1. Updating module content with new examples/content (n=7);
2. Incorporating a grading system as opposed to the pass/fail system currently in place (n=4);
3. Include relevant and role-specific examples (n=5);
4. Include more interactive components (n=14);
5. Provide how-to documents and IT tips and cheat sheets (eg, how-to encrypt emails) (n=3);
6. Provide more mediums for learning (eg, lunch and learns, in-classroom training) (n=3); and
7. Provide staff the time to complete the modules (n=5).

Similarly, participants suggested various ways to promote IT security and compliance with the modules:

1. Hold poster campaigns (n=6);
2. Send reminders to complete the annual modules (n=13);
3. Have managers review IT security information in team meetings (n=6);
4. Email a weekly or monthly bulletin highlighting recent security issues or breaches (n=4); and
5. Ensure information is accessible and easy to find (n=7).

Table 6 Logic regression of explanatory variables against the outcome "correct action upon receiving spam emails"

Question	Odds Ratio	CI
Completed Module I		
No	1	(2.0–8.8)
Yes	4.2	
Completed Module II		
No	1	(0.4–3.0)
Yes	1.2	
Staff type		
Clinical	1	(0.9–2.1)
Non-clinical	1.4	
Work pattern		
Part-time	1	(0.9–2.1)
Full-time	1.3	
Number of years in the organization		
<5	1	(0.5–1.5)
5–10	0.8	(0.9–2.2)
>10	1.4	

Note: Odds ratios are calculated after adjusting for other variables in the model.

The study examined the effectiveness of existing educational and awareness training in delivering the key messages around IT security and privacy. The results of the study indicated that a large majority of participants were aware of Module I and had completed them. Staff were mostly satisfied with the educational and awareness programs, and found the modules effective in delivering the key messages around IT security and privacy. Specifically, we found that Module I was effective in improving IT security knowledge. Participants who had completed the Module I training were significantly more likely to know how to correctly respond to potential security breaches (eg, how to react to spam emails or how to report IT security incidents). Although module completion was mandatory, not all staff had completed the training. This could be attributed to a number of reasons that might be associated with being a large healthcare organization. Participants cited several challenges to completing the modules, such as the unavailability of dedicated and uninterrupted time, outdated computers, lack of follow-up from managers, and difficulty in accessing the module. Also, it was found that the most common breaches reported were (1) walking away from a computer without logging off and (2) not knowing how to encrypt emails when sending emails outside the organization.

A recent report by Cavoukian and Alvarex[8] identified the importance of privacy and security training. The authors suggested that awareness regarding privacy and security is key to the reduction of human errors and carelessness, which is often the cause of many privacy breaches. In our study, Module I adopted by the health organization yielded the necessary outcome that led to the reduction of errors and enabled staff

to encrypt their emails and took the necessary action against spam. Additionally, Cavoukian and Alvarex[8] envisaged that training can help to ensure that employees and agents are aware of their obligations under privacy statutes and organizational privacy and security policies and procedures that are applicable to the authorized collection, use, and disclosure of personal health information and the safeguards that must be implemented to protect the personal health information.

Additionally, it was found that the short duration (20 minutes) of Module I made it more effective than the 60-minute Module II. This was attributed to the higher level of knowledge, which was directly related to the information provided in the module. Also, the completion of the module prompted them to look at more IT security resources, such as dealing with spam and encrypting their emails. This is in line with other studies that also found that if training is divided into shorter sessions, staff are more likely to pay attention and retain the information.[20,21] Shorter sessions help to reduce perceptions of information overload and help with developing successful e-learning training modules.[16]

There are multiple benefits to using information systems in healthcare, such as improving quality and providing patient-centric services by linking access to patient information from various sources.[22] However, the data are vulnerable to security threats and risks the privacy of patients. Privacy is a key element in the patient–physician relationship, facilitating a correct diagnosis, treatment, and medication.[3] With growing security threats, there is an increased risk of inappropriate access to patient information when IT security measures are not practiced.[22]

The increased risk of IT breaches results from staff walking away from their computer without logging off, especially in open-plan offices. The automatic logouts mechanism after a few minutes of inactivity provides an electronic safeguard.[6] Also, sometimes staff share login information with other staff. In some cases, staff are forced to share their own information so that the new hires can perform their job; this undermines data protection and patient privacy.[2,23] Daglish and Archer[20] recommend that as much as healthcare providers need to accumulate data about patients to be able to treat them effectively, it is the sole responsibility of the organizations to guard the data against unwanted breaches.

Advances in technology have led to the deployment of automated and efficient healthcare information systems. Also, the use of the Internet enhances information communication of these systems, but increases risk due to multiple networks and heterogonous users involved.[24] This contributes to the challenge of integrating secure and privacy-preserving systems.[25] Hence, a system with high security and excellent protection strategies is required to protect against potential breaches, which benefits the patients and improves overall quality.[24]

Various components need to be embedded for user access control to ensure the integrity of sensitive data.[22] The access control features should include elements of robustness, flexibility, and conformity. First, the system has to be robust enough to prevent the exploitation of sensitive and private data by maintaining inappropriate and unauthorized access.[25] Second, related to emergency cases, access to the control system has to be flexible to allow overriding and delegation access privileges.[25] The coupling of two access control features allows for potential conflicting non-compliance situations. The third feature of conformity tries to address the issues by involving processes related to verifying, validating, and monitoring the compliance of access control policies.[25] The paper by Jaïdi et al[25] discusses the framework for deploying the proposed technique for reliable and efficient access control policies. Moreover, these methods propose optimal security techniques as a way to govern access control policy based on privileges and rights to patient information.[26]

Other technologies used to ensure security and privacy of healthcare data involve encryption, data masking, security monitoring, and auditing.[26] Encryption is a valuable technique to protect sensitive data and prevent misuse.[22] The technique helps to safeguard data in case of breaches like packet sniffing and theft of storage devices. Abouelmehdi et al[26] suggest that the encryption scheme should be efficient, with minimum key holds by each party, and should be extendible to include new data. Data masking fully removes personal identifiers and is different from encryption, as the original value cannot be returned.[26] The monitoring technique involves surveillance, detection, and investigating network events against potential security breaches. The approaches discussed are important elements to consider for protection of healthcare data and computerized patient records.

We identified a few limitations, such as (1) some occupation groups were not as well represented as others, despite our best recruitment efforts and proportionate stratified random sampling methods. Also, our target population included some non-computer users who might not have received the online survey. (2) Due to the nature of the questions, social desirable responding may have biased the results; we tried to minimize this by ensuring confidentiality of the participants and anonymizing the survey.

Conclusions

Information technology security and privacy training should be an integral part of healthcare staff continuing education to prevent potential breaches and protect

patient information. The evaluation of the training program ensures that staff are aware of available resources and understand how to prevent IT security breaches. Staff's lack of awareness related to organizational IT policy and compliance requirements could potentially create more risk for security breaches. Furthermore, more emphasis is required for part-time staff who may not fully understand and comply with IT security protocols and could increase the risk of breaches.

Acknowledgments

Special thanks to all the participants who voluntarily completed the surveys in their busy work schedules and to the stakeholders and senior leadership for their support and engagement for making this study a success.

Disclosure

The authors report no conflicts of interest in this work.

References

1. Kuo KM, Talley PC, Hung MC, Chen YL. A Deterrence approach to regulate nurses' compliance with electronic medical records privacy policy. *J Med Syst*. 2017;41(12):198.
2. Fernández-Alemán JL, Señor IC, Lozoya PÁ, Toval A. Security and privacy in electronic health records: a systematic literature review. *J Biomed Inform*. 2013;46(3):541–562.
3. Appari A, Johnson ME. Information security and privacy in healthcare: current state of research. *IJIEM*. 2010;6(4):279.
4. Kruse CS, Smith B, Vanderlinden H, Nealand A. Security techniques for the electronic health records. *J Med Syst*. 2017;41(8):127.
5. Lemke J. Storage and security of personal health information. *Ontario Occupational Health Nurses Association*. 2013;32(1):25–26.
6. Taitsman JK, Grimm CM, Agrawal S. Protecting patient privacy and data security. *N Engl J Med*. 2013;368(11):977–979.
7. Omotosho A, Emuoyibofarhe J, Oke A. Securing private keys in electronic health records using session-based hierarchical key encryption. *Journal of Applied Security Research*. 2017;12(4):463–477.
8. Cavoukian A, Alvarez RC. Embedding Privacy into the Design of EHRs to Enable Multiple Functionalities: Win/win; 2012. Available from: https://www.infoway-inforoute.ca/en/component/edocman/338-embedding-privacy-into-the-design-of-ehrs/view-document?Itemid=0. Accessed February 15, 2017.
9. Win KT. A review of security of electronic health records. *Health Inf Manag*. 2005;34(1):13–18.
10. Anderson CL, Agarwal R. The digitization of healthcare: boundary risks, emotion, and consumer willingness to disclose personal health information. *Information Systems Research*. 2011;22(3):469–490.
11. EKOS Research Associates. Electronic health information and privacy survey: what Canadians think – 2007. Final Report. Available from: https://www.infoway-inforoute.ca/en/component/edocman/14-ekos-survey-on-electronic-health-information-and-privacy-full/view-document?Itemid=0. Published March August 2007. Accessed August 1, 2016.
12. Alberta Health Services. Information Security and Privacy Safeguards. Policy, Level 1; 2012. Available from: https://extranet.ahsnet.ca/teams/policydocuments/1/clp-ahs-pol-information-security.pdf. Accessed August 1, 2016.
13. Hepp SL, Tarraf RC, Birney A, Arain MA. Evaluation of the awareness and effectiveness of IT security programs in a large publicly funded health care system. *Health Information Management Journal*. 2018;47(3):116–124.
14. Glaser J, Overhage JM. The role of healthcare IT: becoming a learning organization. *Healthc Financ Manage*. 2013;67(2):56–62.
15. Dafalla TD. *Evaluating the Usability and Usefulness of an E-Learning Module for a Patient Clinical Information System at a Large Canadian Healthcare Organization*. (Master's thesis). Victoria, BC; University of Victoria (Canada); 2013.
16. Ruggeri K, Farrington C, Brayne C. A global model for effective use and evaluation of e-learning in health. *Telemed J E Health*. 2013;19(4):312–321.
17. Wilkinson A, While AE, Roberts J. Measurement of information and communication technology experience and attitudes to e-learning of students in the healthcare professions: integrative review. *J Adv Nurs*. 2009;65(4):755–772.
18. Al-Samarraie H, Teo T, Abbas M. Can structured representation enhance students' thinking skills for better understanding of E-learning content? *Comput Educ*. 2013;69:463–473.
19. Hsieh P-AJ, Cho V. Comparing e-Learning tools' success: The case of instructor–student interactive vs. self-paced tools. *Comput Educ*. 2011;57(3):2025–2038.
20. Daglish D, Archer N. Electronic Personal Health Record Systems: A Brief Review of Privacy, Security, and Architectural Issues. Poster presented at: 2009 World Congress on Privacy, Security, Trust and the Management of e-Business; August 25-27, 2009; Saint John, NB, Canada. Available from: https://www.researchgate.net/publication/224084987_Electronic_Personal_Health_Record_Systems_A_Brief_Review_of_Privacy_Security_and_Architectural_Issues. Accessed July 15, 2018.
21. Thomson ME, von Solms R, Solms RV. Information security awareness: educating your users effectively. *Inf Manag Comp Security*. 1998;6(4):167–173.
22. Pragash K, Jayabharathy J. A survey on big data privacy and security issues in healthcare information system. *Adv Nat Appl Sci* 2017;11(12):95–100.
23. Jannetti MC. Safeguarding patient information in electronic health records. *AORN J*. 2014;100(3):C7–C8.
24. Liu CH, Chung YF, Chen TS, Wang SD. The enhancement of security in healthcare information systems. *J Med Syst*. 2012;36(3):1673–1688.
25. Jaïdi F, Labbene-Ayachi F, Bouhoula A. Advanced techniques for deploying reliable and efficient access control: application to E-healthcare. *J Med Syst*. 2016;40(12):262.
26. Abouelmehdi K, Beni-Hessane A, Khaloufi H. Big healthcare data: preserving security and privacy. *J Big Data*. 2018;5:1.