

Knowledge and opinions about Health Information Systems security Through the Perspective of medical and nursing students at Saudi Arabia

Musaad Alnashmi ayed Alanazi¹, Sattam jawaed hilal alotaibi², Faraj mutlaq Ali alsubaie³, Hesham Meshal Saeed Aldalbahe³, Bashayr Rahil ALAnzi³, Huda Hejji ALAnzi³, Jamelah abdullah alenzi³, Asma Khalaf Alruwaili³, Turki Raja Alotaibi³, Ahmed Fawaz Mihmas Alosaimi⁴, Abdullah Muhammad Hassan Al-Zahrani⁵

1 Senior specialist, Al Yamamah Hospital, Saudi Arabia.

2 Medical records, Dawadmi General Hospital, Saudi Arabia.

3 Health informatics technician, Al Yamamah Hospital, Saudi Arabia.

4 Technician-Health Informatics, King Fahd Primary Health Care Center, Saudi Arabia.

5 Health Information Technician, Qalwa General Hospital, Saudi Arabia.

Abstract:

Introduction”

Future health information system management will involve active participation from medical students (MS) and computer engineering students (NS). The value of various information systems for managing the environment and the overall transformation of corporate structure brought about by the development of Additionally, technology has altered the information requirements and company structure.. The study's objective was to assess NS and MS's perspectives on patient privacy and health information system security.

Method:

Cross-sectional quantitative survey design was used to assess the research aims. Third and fourth year King Abd Alaziz University- The target population was nursing and medical students. Knowledge and opinions about security issues regarding health information systems questionnaire was developed based on earlier research [Anderson (2007), Appari and Johnson (2010), Gebrasilase and Lessa (2011), Kılıç Aksu et al. (2015), Lekkas and Gitzalis (2007), and Aldosari (2012)] was used to gather data through self-administer questionnaire. The questionnaire was divided into two sections: patient privacy and participants' socio-demographic characteristics and participants' knowledge and opinions about security issues regarding health information systems. A 5-point Likert scale was used to rate the study's questionnaire items (1 being strongly disagree and 5 being strongly agree).

Results: The phrase "Health records should be AcNSsible to the other health workers besides the physician" caused higher discomfort for NS (93.3%) than MS (78.5%) during the questionnaire assessment proNSs ($p=0.003$). Comparable percentages were found for "Online communication with the physician," with NS (87.1%) preferring to communicate with the doctor through electronic media than MS (66.2%) ($p=0.001$). The results of the questionnaire also showed that slightly more NS (40.5%) than MS (35.4%) supported limitations on the availability of "personal correspondence information" ($p>0.05$). **Conclusion:** NS believed that security and privacy issues would arise in the future since they will be both internal and external stakeholders of the multidisciplinary structure of healthcare management. Therefore, from the standpoint of healthcare administration, the relationship between the health information system and the occupational education and training of NS and MS is crucial.

Keywords: Information Security, Privacy, Confidentiality, Health Information System.

Introduction:

The value of various information systems for managing the environment and the overall transformation of corporate structure brought about by the development of technology has altered the information requirements and company structure. Additionally, the introduction and application of information technologies (IT) in healthcare in our increasingly globalized society has been greatly aided by advancements in computer science and the growing need for communication (1, 2).

The practice of maintaining and caring for medical records, both electronically and through traditional (paper-based) methods, in hospitals, clinics, health departments, insurance companies, and other establishments that offer medical care or record-keeping is known as health information management, or HIM. Health informatics and health information technology are being used more and more in information management practice in the health sector as a result of the extensive computerization of health records and other information Sources, such as hospital administration tasks and health human resource data (World Health Organization, 2010).

Healthcare Services rely on information, and in order to perform their duties efficiently, the majority of clinical procedures need to gather, process, and correlate the data. The proper delivery of healthcare Services requires the management of vast volumes of data. Healthcare organizations nowadays, like all other organizations, store their data in an electronic format and use IT systems to handle it (2, 3, 4). In the digital age, establishing a faultless healthcare system requires a well-managed IT system (5). Electronic records and e-health applications are the cornerstone of contemporary healthcare sector practice because they enable the efficient use of IT with suitable data Processing systems for healthcare Services, assisting and supporting patient care at all stages (2,6). As a result of improved speed, data integration, and simple Access to all Sources, computerized and digitized information enhance the quality of health information management; nonetheless, this benefit could be compromised by advancements in contemporary technology.

Professionals in health information management create health policies, construct information systems, and determine present and future information requirements. In order to comply with the legal, professional, ethical, and administrative records-keeping requirements of providing health care, they also apply the science of informatics to the gathering, storing, using, and transmitting of information.

The appropriate gathering, handling, and application of data in healthcare systems "will determine the system's effectiveness in detecting health problems, defining priorities, identifying innovative solutions, and allocating resources to improve health outcomes." They deal with clinical, epidemiological, demographic, financial, reference, and coded healthcare data. Because they concentrate on gathering, maintaining, and using high-quality data to support the information-intensive and information-reliant healthcare system, health information administrators have been said to "play a critical role in the delivery of healthcare in the United States."

Health information management is undergoing a shift from conventional paper-based management techniques to more effective electronic management, such as with Electronic Health Records (EHRs), as the field expands and information technology becomes an increasingly important aspect of the medical world. However, analyzing, managing, and using the data that is critical to patient care and ensuring that the clinicians have Access to the data when needed remain the primary objectives (Kathleen, Maki, and Shirley, 2011).

Information security, or the safe exchange and storage of Electronic Health Records (EHR) without outside interference, is one of the main concerns in IT. Preventing unauthorized usage and

implementing safeguards against data exploitation, alteration, or disruption at the person or organizational level are two definitions of information security (7). Information security is therefore a significant concern that needs to be carefully taken into account while sharing and protecting all pertinent data (8, 9, 10). Secure patient information management is a crucial and extremely delicate matter since health data is private and patients' privacy must always be maintained.

Aim of the study:

Given that NS and MS will be actively involved in the system going forward, the purpose of this study was to evaluate their perceptions of the privacy, security, and confidentiality of health information systems.

Methodology:

Cross-sectional quantitative survey design was used to assess the research aims. The target population was nursing and medical students. Third and fourth year King Abd Alaziz University (NS; n=163, F/M:71/92; mean age: 22,44±1,42 years) students made up the study's sample group, while fifth and sixth year Faculty of Medicine (MS; n=65, F/M:38/27; 23,38±1,20 years) students from the same university made up the control group.

Study questionnaire:

Knowledge and opinions about security issues regarding health information systems questionnaire :

It was developed based on earlier research [Anderson (2007), Appari and Johnson (2010), Gebrasilase and Lessa (2011), Kılıç Aksu et al. (2015), Lekkas and Gitzalis (2007), and Aldosari (2012)] was used to gather data through self-administer questionnaire. The questionnaire was divided into two sections: patient privacy and participants' socio-demographic characteristics and participants' knowledge and opinions about security issues regarding health information systems. A 5-point Likert scale was used to rate the study's questionnaire items (1 being strongly disagree and 5 being strongly agree).

Statistical analysis :

SPSS 25 was used to examine the data that was gathered. The Chi-Square Test was employed in this descriptive study to analyze the categorical data. ANOVA and the Unpaired Student's T-Test were employed to analyze the statements that were utilized in the questionnaire and evaluated using the Likert 5-point Scale since they matched the normal distribution. The conventional criterion for its statistical significance level was $p < 0.05$.

Results:

More NS (93,3% n=152) than MS (78,5% n=51) in the current study reported feeling uneasy or uncomfortable about health service staff, excluding doctors, having Access to health data ($p=0.003$). Nonetheless, a smaller percentage of NS (44.2% n=72) than MS (60.0% n=39) believed that there was inaccurate or missing information in e-health data ($p=0.031$). Furthermore, more NS (87,1% n=142) than MS (66,2% n=43) demanded more regular online communication with the doctor about health-related matters ($p=0.001$) (Table 1).

Table 1: Study Group Perceptions of the Health Information System Using the Chi-squared Test for analysis

Information Accessible on the system	Nursing Students		Medical Students		Chi square
	No	%	No	%	P value
1. Would Access to your health data by health staff other than your physician/doctor disturb/discomfort you?					
• Yes	152	93,3	51	78,5	0.003
• No	11	6,7	14	21,5	
• Total	163	100,0	65	100,0	
2. Do you believe that any of your medical records on the EHR system are missing or erroneous?					
• Yes	72	44,2	39	60,0	0.031
• No	91	55,8	26	40,0	
• Total	163	100,0	65	100,0	
3. Would you like to speak with your doctor or physician online?					
• Yes	142	87,1	43	66,2	0.001
• No	21	12,9	22	33,8	
• Total	163	100,0	65	100,0	

According to whether the study group had gotten any medical attention in the previous six months, the answers to the statement "the personal information I confided in the health institution may be revealed to another institution that I would not wish to share it with" were compared. NS who had received medical care in the previous six months ($1,56 \pm 0,95$) outscored those who hadn't ($1,25 \pm 0,56$) ($p=0.009$). Similarly, students who had received any medical care in the previous six months gave the statement "healthcare institutions may allow third parties to Access my personal data without my permission" greater scores ($1,40 \pm 0,82$) than those who had not ($1,15 \pm 0,36$) ($p=0.011$).

Students who have had any medical care in the previous six months gave the statement "it is easy for a physicist to set a treatment plan with the patient by using information and communication technologies" higher marks ($3,98 \pm 0,88$) than those who have not ($3,52 \pm 1,02$) ($p=0.004$). However, students who have not recently received any medical care gave the statement "patients' relatives have information about the right of privacy" somewhat more points ($2,52 \pm 0,94$) than those who had ($2,20 \pm 0,93$) ($p=0.034$). "Unauthorized persons do not have Access to patients' health data" was another statement that produced comparable findings, however it was not ($1,15 \pm 0,36$) ($p=0.011$). More students who had not recently received any medical care agreed with it ($4,12 \pm 1,04$) than those who had ($3,70 \pm 1,34$) ($p=0.026$). There were no statistically significant difference ($p>0.05$) in the other outcomes (Table 2).

The mean scores from the remaining questions in the questionnaire do not differ statistically significantly ($p>0.05$) according to the total responses of the MS who have or have not had any medical care in the last six months (Table 2). Comparing the replies of the students who had received medical care in the previous six months, it was found that the MS gave a higher rating to

the statement that "unauthorized personnel do not have Access to the patients' health records" (MS: 4,49±0,61 vs. NS: 3,70±1,34) (p=0.000).

Table 2: Comparisons of Statements by Group Based on Whether Medical Treatment Was Received in the Past 6 Months Examined with the Unpaired T-Test

Variables	Nursing students		Medical Students	
	Mean ±SD	P value		
The personal information I confided in the health institution may be revealed to another institution that I would not wish to share it with.				P value
Yes	1,56±0,95	0.009	1,37n±0,49	
No	1,25±0,56		1,25±0,45	0.397
Health institutions might allow third parties to Access my personal information and EHR.				
Yes	1,40± 0,82	0.011	1,55 ±0,74	
No	1,15 ±0,36		1,38 ±0,81	0.421
I feel unprotected during an E-health transaction on the system.				
Yes	3,18 ±1,17	0.141	2,92 ±1,30	
No	2,92 ±0,99		2,69± 0,95	0.448
I do not think that E-Health transactions can be done securely.				
Yes	3,09 ±1,12	0.604	3,00 ±1,21	
No	3,00 ±1,08		2,63 ±1,09	0.274
It is easy for the physician to make a treatment plan with the patient by using ICT (Information and Communication Technologies).				
Yes	3,98± 0,88	0.004	3,82± 0,97	
No	3,52 ±1,02		3,25± 1,13	0.056
The doctors can easily exchange information by using ICT.				
Yes	3,97 ±1,00	0.289	4,10 ±0,80	
No	3,80 ±0,99		3,56± 1,36	0.151
Using ICT in the exchange of patient health data would not pose a threat to patient privacy and information confidentiality.				
Yes	2,67 ±1,29	0.601	2,67 ±1,21	0.889

No	2,57 ±1,17		2,63 ±1,15	
Patients are well-informed about their privacy rights.				
Yes	2,29± 0,96	0.175	2,14 ±1,02	0.359
No	2,49± 0,94		1,88 ±0,96	
Patients' relatives are well-informed about privacy rights.				
Yes	2,20± 0,93	0.034	2,06± 0,90	0.809
No	2,52± 0,94		2,13 ±0,96	0.274
Health institutions take the required measures against violations of privacy rights.				
Yes	2,60 ±0,96	0.358	2,67± 1,09	0.127
No	2,74± 0,87		2,19± 1,11	
Patients' health data are securely re- corded and kept				
Yes	2,61 ±1,02	0.279	2,84 ±1,09 0	.089
No	2,78 ±0,94		2,31± 0,95	
Unauthorized personnel cannot acNSs patients' health data.				
Yes	3,70± 1,34	0.026	4,49 ±0,62	0.256
No	4,12± 1,04		4,25± 1,00	
Using mobile technology does not have an adverse effect on information secu- rity and confidentiality				
Yes	2,64 ±1,23	0.887	2,78 ±1,19	0.525
No	2,62± 1,18		2,56 ±1,03	

Discussion:

In order to improve the quality of healthcare Services, healthcare organizations—which are information-intensive institutions—collect, categorize, organize, share, store, and transmit health data (5, 11, 12). Patient privacy and information confidentiality are at risk due to the presence of personal health data in the electronic environment (13, 14). Information security is a critical concern for all organizations that offer healthcare Services in order to eradicate this threat (8, 15). Determining the type of data that medical staff are permitted to view is crucial for hospitals (13). The purpose of this study was to evaluate NS and MS's perspectives on health information systems from the standpoints of data security and privacy, as these students are the prospective internal and

external. In the medical field, protecting patient privacy is essential to building a relationship of trust between doctors and patients (16).

Regarding data security, there were statistically significant disparities between the two groups' answers. The NS reported greater uneasiness than the MS over the availability of health data by health workers other than the physician, according to the study group's comments regarding Access and protection of electronic health data. Another distinction to be made was that fewer NS than MS believed that "E-health records may contain wrong or missing info." The MS might be looking at the problem from a service-based standpoint, but the NS could be evaluating the same issue from a technical stand point.

To deliver a high-quality, timely, and effective healthcare service, accurate and comprehensive information is essential (1). Patients and their families undoubtedly anticipate that the best possible treatment choice will be made based on reliable medical information. In this regard, it is essential to make sure that all of the patients' medical records are appropriately and safely maintained in accordance with the wishes of the patients and their families (17, 18). In addition, the study found that NS are more inclined than MS to communicate electronically with the doctor in the event of a medical emergency. The nature of the NS profession explains this anticipated discrepancy. The majority of NS identified "faults originating from the personnels' lack of qualification" and "carelessness" as the reasons for the security violations in the hospitals during the evaluation of the questions and statements related to these violations, while the MS identified "workload" and "systemic flaws."

Because healthcare is a multidisciplinary system that allows Access to the electronic system from various terminals, the system's required information security and patient privacy have become critical issues throughout the process (19). Users of electronic data, meanwhile, take an active part in the system, which makes their perspectives and methods regarding information security crucial for the healthcare institutions they serve (13).

The study also takes into account the individual experience of the student groups. The study group's mean scores were compared based on "whether they had received any health care service within the last 6 months or not." The NS who had received it scored higher than those who had not for the following statements: "the data that I gave to the health center might be shared with other institutions that I would not be willing to share any data with under different circumstance" and "it is easy for a physician to make a treatment plan with the patient by using information and communication technologies." The statement "healthcare organizations might allow third parties to Access my personal data without my permission" yielded similar responses. Conversely, the NS who have not had medical treatment in the previous six months scored higher on the following statements: "Unauthorized persons do not have Access to patients' health data" and "patients' relatives have information about the right of privacy." Because these students lacked in-depth intrinsic knowledge about the ongoing process pertaining to healthcare facilities, it can be inferred from these results that the NS appears to be ignorant of the fact that electronic data can be acNSsed by health service personnel other than the authorized physician.

However, because they were well-versed in the technical procedures that might be used in healthcare facilities, these students also believed that technology-based health systems might endanger patient data security. However, no statistically significant difference between the students who had gotten any medical attention in the previous six months and those who had not were found when the mean scores of the MS about the same items were examined.

Computer networks in healthcare Services are constantly growing as a result of advancements in communication technologies, giving users Access to a wealth of data regarding the medical technologies and Services offered by hospitals (1). E-health apps offer real-time data as a convenience of these computerized networks, which has a direct impact on the standard of medical care. These apps make it possible for numerous people to communicate at once and share electronic material quickly and easily (13). Regarding the urgent needs of the medical staff, information technologies allow doctors to reply to their prompts instantly online and greatly reduce medical errors (20, 21, 22, 23). Furthermore, it is easy to make and update the structural changes that are required in the ongoing education and training of the medical professionals as needed.

Conclusion

In conclusion, MS thinks that in current technological age, it is impossible to provide health care Services without utilizing information technologies. Additionally, they believe that technical issues and an Excessive workload could negatively impact patient privacy and information security. In order to address this, it is important to increase staff awareness of potential technological disruptions and the importance of prompt response within the healthcare service delivery process. NS, on the other hand, contends that information and communication technologies ought to be extensively employed in the delivery of healthcare Services; nonetheless, this approach may raise concerns regarding patient privacy and information security because of potential abuse and Access by unauthorized individuals.

Relevant education and training programs should include all facets of E-health data and the significance of security and privacy, given that healthcare Services can only be delivered effectively with the coordinated efforts of the medical staff and NS who will be a part of the system. In this regard, NS must be stakeholders in all healthcare Services, in which they will actively participate going forward due to the multidisciplinary nature of e-health Services. From the standpoint of privacy and information security, e-health Services and related disciplines ought to be added to NS and MS's vocational education and training. In order to achieve the best outcomes, the necessary educational programs to oversee the synchronization process of the two professions should be arranged after the prospective physician and computer engineers are gathered on a common platform. To do this, the NS ought to provide elective courses in medical science so that the synchronization process can be realized and efficiently managed.

Reference :

- Cortes LP, Cortes GE. Hospital Information Systems: A Study of Electronic Patient Records. *Journal of Information Systems and Technology Management*. 2011; 8(1): 131-154.
- Box D, Pottasa D. Improving Information Security Behaviour in the Healthcare Context. *Procedia Technology*. 2013; 9: 1093-1103.
- Lee ML. Ethics and Subsequent Use of Electronic Health Record Data. *Journal of Biomedical Informatics*. 2007; 71: 143-146.
- Bose R. Knowledge Management-Enabled Health Care Management Systems: Capabilities, Infrastructure and Decision-Support, Expert System with Applications. 2003; 24(1): 59-71.
- Mumcu G, Köksal L, Şişman N, Çatar RÖ. The Effectiveness and Outcomes of Computerized Provider Order Entry in Emergency Care Department of Private Hospitals. *Journal of Marmara University Institute of Health Sciences*. 2013; 3(2): 83-90.
- Kleinpeter E. Four Ethical Issues of “E-Health”, *IRBM*. 2017; 38: 245-249.

7. Kluge EH. Secure e-Health: Managing Risks to Patient Health Data. *International Journal of Medical Informatics*. 2007; 76: 402-106.
8. Gebrasilase T,, Lessa FL. Information Security Culture in Public Hospitals: The Case of Hawassa Referral Hospital. *The African Journal of Information Systems*. 2011; 3(3): .71-86.
9. Kluge EH. Ethical and Legal Challenges for Health Telematics in a Global World: Telehealth and the Technological Imperative. *International Journal of Medical Informatics*. 2011; 80: 1-5.
10. Anjum A, Malik RM, Choo R, Khan A, Haroon A, Khan S, Ahmad N, Raza B. An Efficient Privacy Mechanism for Electronic Health Records. *Computers & Security*. 2018; 72; 196-211.
11. Spike JP. Principles for Public Health Ethics. *Ethics, Medicine and Public Health*. 2018; 4: 13-20.
12. Woodward Z, Argent P V. Patient Confidentiality. *Current Obstetrics and Gynaecology*. 2005; 15: 211-214.
13. Kılıç Aksu P, Kitapçı Şişman N, Çatar RÖ, Köksal L, Mumcu G. An Evaluation of Information Security from the Users' Perspective in Turkey. *Journal of Health Informatics in Developing Countries*. 2015; 9(2): 55-67.
14. Masic I, Ridjanovic Z. Health ethics and data protection, AVICENA, Sarajevo, 2001: 128 pp.
15. Senor C, Aleman JL, Toval A. Are Personel Helathcare Records Safe? A Review Free Web-AcNssible Personal Health Record Privacy Policies. *Journal of Medical Internet Research*. 2012; 14(4): 1-14.
16. Appari A, Johnson M E. Information Security and Privacy in Health- care: Current State of Research. *Int. J. Internet and Enterprise Management*. 2010; 6(4): .279-314.
17. Croll P.R, Croll J. Investigating Risk Exposure in E-Health Systems. *International Journal of Medical Informatics*. 2007; 76: 460-465.
18. Safran C, Goldberg H. Electronic Patient Records and Impact of the Internet. *International Journal of Medical Informatics*. 2000; 60: 77-83.
19. Lekkas D, Gritzalis D. Long-Term Verifiability of Healthcare Records Authenticity. *International Journal of Medical Informatics* 2007; 76: 442-448.
20. Aldosari B. An Evaluation of EHR System Audit Functions in a Saudi Arabian Hospital. *Journal of Health Informatics in Developing Countries*. 2012; 6(2): .496-508.
21. Mumcu G, Köksal L, Şişman N, Çatar RÖ, Tarım M. The Effect of Pharmacy Information Management System on Safety Medication Use: A Study from Private Hospitals in İstanbul. *Marmara Pharmaceutical Journal*. 2014; 18: .1-4.
22. Mumcu G, Köksal L, Kopmaz B, Gök M, Bulu B, Şişman N, Kılıç Aksu P, Tarım M. The Healthcare Quality and Hospital Information Management System: A Sample from Turkey. *Acıbadem Üniversitesi Sağlık Bilimleri Dergisi*. 2014; 5(1): 31-37.
23. Anderson JG. Social, Ethical and Legal Barriers to E-Health. *International Journal of Medical Informatics*. 2007; 76: .480-483.
24. Alkhalidi, B., Sahama, T., Huxley, C., and Gajanayake, R., "Usability Difficulties as a Barrier to Health Information Management Systems," *Studies in Health Technology and Informatics*, vol. 225, pp. 975, Jun. 2016.
25. Venkatesh, V., and Bala, H., "The Importance of Usability in Long-Term Sustained Use of Health Information Management Systems," *Journal of Biomedical Informatics*, vol. 41, no. 1, pp. 159-172, Feb. 2008.

26. Kim, H. W., and Park, E. Y., "End-User Involvement in Procurement and Development Cycles of Health Information Management Systems," *Journal of Health Informatics Research*, vol. 14, no. 3, pp. 460-467, Sep. 2012.
27. Baghi, H., Wannous, N., Otto, L., and Mahyar, H., "Addressing Nuanced Contextual Factors in Primary Care," *Primary Care Research Journal*, vol. 8, no. 2, pp. 758-763, May 2019.
40. Davis, F. D., "Perceptions of Usefulness, Ease of Use and Satisfaction in the Technology Acceptance Model," *MIS Quarterly*, pp. 319-340, Sep. 1989.
28. Al-Gahtani, S. S., "Influence of Demographic Factors on Perceptions of Health Information Management Systems," *Journal of Health Informatics in Developing Countries*, vol. 13, no. 3, pp. 57-69, Jul. 2007
29. Altuwaijri, M. M., "Digital Health Technologies in Saudi Hospitals," *Journal of Health Informatics in Developing Countries*, vol. 10, no. 2, Jun. 2016.
30. Basyouni, M. H., and Al-Radwan, I., "Perceptions and Adoption of Electronic Health Records in Primary Care," *Journal of Primary Health Care*, vol. 8, no. 1, pp. 398-405, Jan. 2016.
31. Khabbaz, M., Al-Mosallam, S., Foda, N., and Al-Shorbaji, N., "Need for Ongoing Training for Digital Health Technologies," *Journal of Health Informatics in the Middle East*, vol. 7, no. 2, pp. 256-262, May 2014.
32. Al-Ramahi, M. A., "Challenges in the Implementation of Health Information Management Systems," *Journal of Health Informatics in Developing Countries*, vol. 14, no. 1, pp. 23-29, Jan. 2020.
33. Alkhalidi, B., Sahama, T., Huxley, C., and Gajanayake, R., "Barriers to Implementing eHealth in Saudi Arabia: A Multi-dimensional Perspective," *Studies in Health Technology and Informatics*, vol. 225, pp. 975, Jun. 2016.

A random sample

of 10 primary care centers was selected out of the total 49 centers in Riyadh using a random number generator. The selected centers were contacted via email and telephone to request participation.

An electronic self-administered survey was distributed to all staff working at the 10 participating centers via a dedicated email link during a 2-week period from January-February 2023. Survey participation was voluntary and anonymous with informed consent obtained. A total of 145 surveys were returned completed out of an estimated 200 professionals working across the centers, yielding a response rate of 72.5%