Risk Management and Healthcare Policy

Dovepress
open access to scientific and medical research

Open Access Full Text Article

ORIGINAL RESEARCH

Patient Data Sharing and Confidentiality Practices of Researchers in Jordan

This article was published in the following Dove Press journal:
Risk Management and Healthcare Policy

Reema A Karasneh[1]
Sayer I Al-Azzam[2]
Karem H Alzoubi[2]
Sahar S Hawamdeh[2]
Suhaib M Muflih[2]

[1]Department of Basic Medical Sciences, Faculty of Medicine, Yarmouk University, Irbid, Jordan; [2]Department of Clinical Pharmacy, Faculty of Pharmacy, Jordan University of Science and Technology, Irbid, Jordan

Purpose: The main focus of this study is to assess the knowledge and practices of healthcare practitioners regarding data sharing, security, and confidentiality, with a focus on the use of health data retrieved from electronic health records (EHRs) for research purposes.

Methods: A descriptive, cross-sectional, questionnaire-based survey study was conducted across all academic institutions including all researchers in the medical field in Jordan. Personal and administrative practices in data sharing were assessed through collecting data from respondents.

Results: The response rate was 22% with an average of 10.25 years of experience in publications. Almost 60% had published at least 1 to 3 studies using EHRs. The prevalence of researchers who "Always" used antivirus software and preserved patient's information was 75.5% and 92.2%, respectively. However, other personal security and confidentiality measures were not satisfactory. Less than half of health data used in the research was "Always" anonymised or encrypted and only around 44.0% had "Always" used sensitive data with more specificity than normal data.

Conclusion: Confidentiality and data sharing practices of healthcare practitioners and researchers were generally less than optimal. Efforts from healthcare providers, health institutions, and lawmakers should be put in place to protect the security and confidentiality of electronic patient data.

Keywords: electronic, health records, EHRs, privacy, ethics

Introduction

The last decades have seen a rising incorporation of technology and informatics among healthcare sectors.[1] This has led to a shift from paper health records to electronically stored patient records, or electronic health records (EHRs). EHRs are defined as systems used to store patient data, including medical history, diagnosis, progress notes, and medication orders.[2] They present an advantage for patient data retrieval over paper records as they are more efficient, timesaving, less costly, and results in less medical errors.[3,4]

In addition to physicians and other healthcare providers, and beyond the scope of health organizations, EHRs are occasionally accessed by third parties such as insurance companies and researchers for purposes including clinical research.[5] Contrary to other methods, EHRs do not require the active participation of patients in clinical studies, and thus can facilitate biomedical, epidemiological, and public health research.[6,7] However, concerns have been raised towards the increasing risk of potential confidentiality breaches associated with EHRs particularly as data are shared among a larger group of people outside the medical team leading to

Correspondence: Reema A Karasneh
Department of Basic Medical Sciences, Faculty of Medicine, Yarmouk University, P.O. Box 566, Irbid 21163, Jordan
Tel +962 02 7211111, Ext: 7141
Fax +962 02 7211162
Email reema.karasneh@yu.edu.jo

submit your manuscript | www.dovepress.com
DovePress
http://doi.org/10.2147/RMHP.S227759

unintended release of data to unauthorized personnel.[8] This particular concern about the confidentiality of EHR systems was investigated by a recent survey of healthcare organizations, in which the majority of participants believed they are more subject to potential confidentiality breaches than other sectors and that such breaches are due to access from third parties.[9]

Failure to protect patient medical data may lead to diminished patient trust in their primary healthcare providers. This is especially a concern with data related to illness that are associated with perceived stigmatization such as sexually transmitted diseases (STDs), psychiatric illnesses, substance abuse, and reproductive health.[3] As a result, patients may become reluctant toward sharing sensitive information that are essential to the provision of high-quality care. Moreover, disclosure of patient data to unauthorized personnel may result in medical or financial identity theft, in addition to compromising patient autonomy.[9] This may pose a violation to the Data Protection Act, which only permits the use of patient data for medical purposes given that the security and privacy of such data is preserved.[10] Thus, protection of data privacy and confidentiality must be regarded as a key pillar to an optimal medical practice and must be weighed against the benefits of EHRs application. Therefore, various security safeguard measures were implemented by Health Insurance Portability and Accountability Act (HIPAA) which included physical, technical, and administrative techniques.[11] Physical techniques include those that prevent or limit physical access to only authorized parties (e.g. assigning security responsibilities), technical techniques are those that prevent or limit access to only authorized parties (e.g. using antivirus software), and administrative techniques take the form of policies, practices, and procedures in the facility.[11]

The risks regarding the use of EHRs have been previously studied.[12–14] Until now, data regarding malpractices of EHRs use in clinical research are still scarce. In fact, it is essential for researcher to understand and take responsibility for the protection of patient health data.[4] In this study, we explored knowledge and practices of researchers utilizing EHRs from different healthcare sectors in Jordan in terms of sharing and confidentiality of patient data, with particular reference to data sharing practices for research. The importance of this study is that it addresses the widely emerging trend of HER and their use in research studies in developing countries taking Jordan as an example. Moreover, this is the first study assessing the confidentiality issue from the perspective of researchers.

Methods

A cross-sectional, descriptive study of data sharing practices in clinical research that utilizes EHRs in Jordan was conducted. Ethical approval was obtained from the authors' Institutional Review Board (IRB).

A web-based questionnaire containing variables of interest was utilized and distributed to all academic researchers from a wide range of health disciplines at private and public universities in Jordan. A letter was emailed with the survey to potential participants with a brief description of the study. Participants were informed prior to starting the survey that it is completely anonymous and that all data would be treated as confidential and notified that their participation is entirely voluntary and their withdrawal from the study could be possible at any time. Participants were also notified that their information will be used for research purposes only and no one other than members of the research team will have access to them. Inclusion criteria were being a faculty member working in a healthcare discipline at private or public universities, ever involved in research activities, willing to sign the participation letter, and willing to complete the survey online. Participants were excluded if they have not used electronic health records in their research during the past 5 years. The average completion time of the survey was 10 mins.

The study instrument was developed and face, content, and construct validity were examined by the authors of the current research. Before starting the actual study, the questionnaire was piloted. At first, face validity was checked – the questionnaire draft was passed through several colleagues. These colleagues were asked for their opinions about the clarity and correctness of the questions. Then the questionnaire was modified taking into consideration their collective suggestions. Thereafter, to ensure that the respondents would understand what was required from the questions, the questionnaire was further validated using the verbal protocols, where 10 participants were recruited individually and asked to fill in the questionnaire. At the same time, they were asked and encouraged to think loudly, and to speak out about what they meant by each answer, and how they understood each question. The investigator was noting down all their responses, and the questionnaire was adjusted accordingly. Besides, the internal validity was established and Cronbach's alpha of 0.77 was obtained.

The content of the questionnaire was divided into three parts: personal information, knowledge, and practices.

Personal information collected included demographics, participant's years of experience in research, and affiliations. Knowledge was addressed through three items: previous participation in research ethics program reflecting the presence of basic knowledge, the recommendation of an introductory course into research ethics reflecting the recognition of such program importance, and knowledge regarding electronic data encryption reflecting knowledge of security techniques. Each of these items was given one point, summed, and then, participants were classified based on the total score into needing improvement (≤1 point), Moderate (2 points), and Good (3 points). Researchers' and Institutional practices included those related to for data access, storage, and delivery (shown in detail in Table 5). Practices were measured by the 5-point Likert scale options "Always", "Often", "Usually", "Rarely", and "Never". Scoring of practice statements ranged from 0 to 4 for positive items and the reverse for negative items. The average scores for Researchers' (7 items) and Institutions (9 items) were calculated and classified into two subgroups representing researchers and institutions with "proper practice" at an acceptable level (mean score ≤1) and "needs improvement" practices (mean score >1).

No identifiable personal details were collected from the respondents. Privacy and confidentiality were taken into consideration throughout the research period by not sharing any information collected from the survey with anyone else except researchers who conducted the study.

Statistical analysis was performed using SPSS v.20.0 (SPSS, Inc., Chicago, IL). Descriptive data analyses were carried out to determine means and percentages of responses.

Results

Study Subject Characteristics

The study response rate was around 22% (n= 243). Males represented 62.7% of study subjects, while the percentage of females was 37.3%. Of those who responded, 42% (n= 102) had conducted research via electronic health systems in the past 5 years and were therefore included in the study (Table 1). Researchers who did not conduct any studies using electronic patient records were excluded (58%, n=141). The mean age among the sample was 40.9 years. 14.7% (n=15) of respondents held the position of professor, while 47.1% (n=48), 31.4% (n=32), and 6.9% (n=7) were assistant professors, associate professors, and lecturers, respectively. Among these researchers, the majority were affiliated with a medicine faculty (43.1%), followed by pharmacy (29.4%), nursing (16.7%), dentistry (7.8%), and applied medical science (2.9%) faculties. The degree held by most respondents was a PhD (84.3%), followed by master's degree (7.8%) and board specialty (7.8%). Overall, researchers had an average of 10.25 (±7.02) years of experience, during which the mean number of publications reached 22.5 papers. For most participants (58.8%), the number of studies conducted using EHS in the past 5 years ranged from 1 to 3 studies.

Table 1 Baseline Characteristics of Study Participants

Variable	Participants (n= 102) (N (%)
Age (mean ± SD), years	40.9 ± 7.9
Years of experience (mean ± SD)	10.25 ± 7.0
Number of publications (mean± SD)	22.5 ± 47.2
Gender	
Male	64 (62.7%)
Female	38 (37.3%)
Faculty	
Nursing	17 (16.7%)
Dentistry	8 (7.8%)
Pharmacy	30 (29.4%)
Medicine	44 (43.1%)
Applied health sciences	3 (2.9%)
Degree	
MSc	8 (7.8%)
PhD	86 (84.3%)
Board Specialty	8 (7.8%)
Studies where EHS was used	
1–3	60 (58.8%)
4–6	23 (22.5%)
7–10	10 (9.8%)
>10	9 (8.8%)

Knowledge Regarding EHRs Data Security and Confidentiality

The vast majority of respondents (81.4%, n=83) stated that they had previously joined a research ethics program. In addition, nearly all respondents (93.1%) agreed that an introductory course into research ethics should be mandatory prior to conducting research. Among these researchers, only 50% had knowledge regarding electronic data encryption. As per calculated knowledge scores, knowledge was considered to be needing improvement in 15.7% (n=16), Moderate in 43.1% (n=44), and Good in 41.2% (n=42) of respondents.

Practices for Protection of EHRs-Extracted Data

The documents required for granting access to EHRs varied between an Institutional Review Board (IRB) approval, a data collection form, a research proposal, or a combination of these (Table 2). The provision of both the IRB approval and data collection form was required in 55.4% of cases, while only 2% were also asked to provide the research proposal in addition to the IRB approval and data collection form. Overall, in around 8% of cases, IRB approval was not necessary to grant access to EHRs neither the research proposal in around 8% of cases. However, around 65% of cases were required to submit the data collection form.

As shown in Table 3, data access and storage were granted mainly for researchers listed in the research proposal (90.2% and 83. 2%, respectively), while research assistants were able to access and store data in 33.7% and 38.6% of conducted research, respectively. However, even not listed in the research proposal, research assistants alone were able to access and store data (6.9%, 15.7%, respectively). Furthermore, around 4% and 2% of respondents reported access and storage of data, respectively, by other researchers not listed in the research proposal form.

Methods used for delivering and storing data (Table 4) included mainly an institution's computer with a fixed password (54.9% and 51.5%, respectively), an e-mail (22.8% and 11.9%, respectively), and a USB flash memory (20.8% and 31.4%, respectively). Other methods used for data delivery included printouts or mobile phones in 6.8% of conducted research. Nevertheless, personal laptops were used for data storage in 70.3% of conducted research. Other used devices for storage included compact disc (CD) and researchers' own drop box account (4%).

Other practices in conducting research were assessed (Table 5). Regarding researchers' practices; around two-thirds of respondents reported always installing antivirus into their computers. Furthermore, patient's confidentiality was maintained in 92.2% of researchers who claimed to have always ensured patient data confidentiality and non-disclosure of health data to unauthorized personnel and around 40% have treated sensitive data with more specificity. Moreover, in most cases data were only used for the approved research proposal, however; only quarter of researchers sent to IRB their results after research completion. Interestingly, patient data were always removed after publication in only 30.5% of the cases.

The role of health institutions that provide access to EHRs for researchers in data protection was also assessed through researchers' response. Around quarter of patients' data were neither encrypted nor de-identified with only 57.9% of researchers were supervised during data extraction. Two-thirds of researchers claimed that an IRB approval was requested before data release, however; around 15% of researchers reported usually being required to submit such documentation for data release. Regarding protection of sensitive patient data (e.g. psychotic and sexually transmitted diseases), more limitations were always put by the responsible institution than with regular data in 44.1% of cases. Interestingly, 40% of researchers reported that they had received more patient data than required from the health institution. The role of the Human Research Committee (HRC) in data protection

Table 2 Documents Required for Granting Access to EHRs

Document	Frequency (%)
IRB approval alone	15 (14.9)
IRB and DCF	56 (55.4)
IRB and RP	17 (16.8)
IRB, DCF, and RP	2 (2)
Other documents but not IRB	8 (7.9)

Abbreviations: IRB, Institutional Review Board approval; DCF, Data Collection Form; RP, Research proposal.

Table 3 Data Access and Storage Granted Personnel

Personnel	Data Access	Data Storage
	N (%)	N (%)
Researchers listed in the research proposal	92 (90.2)	84 (83.2)
Researchers not listed in the research proposal	4 (4)	2 (2)
Research assistants	34 (33.7)	39 (38.6)

Table 4 Patient's Data Storage and Delivery Methods of the Conducted Research Utilizing EHR

Data Storage		Data Delivery	
Method	N (%)	Method	N (%)
Institutions computer	52 (51.5)	Institutions computer	56 (54.9)
USB flash memory	32 (31.4)	USB flash memory	21 (20.8)
Email	12 (11.9)	Email	23 (22.8)
Personal laptop	71 (70.3)	Printouts or mobile phones	7 (6.8)

Table 5 Researcher's and Institutional Data Sharing Practices

Practice	Always N (%)	Often N (%)	Usually N (%)	Rarely N (%)	Never N (%)
Researcher					
Uses antivirus software	77 (75.5)	4 (3.9)	15 (14.7)	4 (3.9)	2 (1.9)
Data sent using web-based applications	16 (15.7)	18 (17.7)	22 (21.6)	12 (11.8)	33 (32.4)
Data destruction after completion of the study	31 (30.5)	23 (22.5)	14 (13.7)	14 (13.7)	33 (32.4)
Non-disclosure of patient information	94 (92.2)	1 (1)	7 (6.9)	0 (0.0)	0 (0.0)
More controlling measures for sensitive data (by researcher)	41 (40.2)	13 (12.7)	20 (19.6)	13 (12.7)	11 (10.8)
Data used only for the approved research	89 (87.3)	2 (1.9)	10 (9.8)	0 (0.0)	0 (0.0)
Results sent to the IRB after conducting the research	26 (23.5)	16 (13.7)	21 (18.6)	8 (5.9)	29 (26.5)
Institution					
Encryption of patients' data	42 (41.2)	17 (16.6)	14 (13.7)	7 (6.9)	22 (21.6)
Patients de-identification	42 (41.2)	14 (13.7)	12 (11.8)	8 (7.9)	25 (24.5)
Monitoring of data extraction	59 (57.9)	12 (11.8)	16 (15.7)	12 (11.8)	5 (4.9)
Request an approval from the IRB for data release	77 (75.5)	7 (6.9)	15 (14.7)	1 (1)	2 (1.9)
More controlling measures for sensitive data (by IT department)	45 (44.1)	20 (19.6)	10 (9.8)	8 (7.9)	9 (8.8)
Provide only required data	32 (31.4)	12 (11.8)	19 (18.6)	22 (21.6)	13 (12.7)
Training of users to prevent unauthorized disclosure of patient data	48 (47)	10 (9.8)	18 (17.6)	9 (8.8)	17 (16.7)
Request signing a document to grant privacy and confidentiality of patient information before data release	52 (50.9)	6 (5.9)	20 (19.6)	4 (3.9)	20 (19.6)
Set a specific timeframe for data usage	40 (39.3)	13 (12.7)	25 (24.5)	5 (4.9)	18 (17.7)

was also assessed through which 47% of respondents reported always receiving recommendations and instructions on handling patient data from the HRC. However, 25.5% stated they rarely or never did so. In addition, around half of the researchers were required to sign a document to grant patient's information privacy and confidentiality. A specific timeframe for data usage was always set for 39.3% of respondents. However, 22.6% reported never or rarely being limited by a timeframe.

Regarding researcher's practices, the average scores of their rating on 7-items, researchers were classified into two subgroups: 60 (58.8%) had proper practice and 42 (41.2%) need improvement in their current practices. Institutional practices assessed through researcher's ratings on 9-items and found that 44.1% (n=45) of institutions have proper practice; however, around 56% (n=57) needs improvement.

Discussion

To our best of knowledge, this is the first cross-sectional population-based study to explore the nature of key issues regarding data sharing practices in clinical research. The results of this study show suboptimal practices regarding data security and confidentiality among researchers from various health sectors. Similar results were previously reported where practices within healthcare environments fell short to expectations.[15–17] In one incident, security failure lead to information exposure of 2 million patients in Central America including their full names, dates of birth, insurance information, disability status, and home addresses.[18,19]

Controlling access and the use of EHRs by identifying who has access to the data, authentication, and access methods in addition to data governance by identifying who maintains confidentiality of the data are important safeguards for security and protecting confidentiality.[20] It is also recommended that access to patient data should be limited to persons who absolutely need it.[7] However, results of the current study showed that data collected for clinical research were shared among a wide range of personnel within the research team with data received more than that required for completion of the study most of the time. This is consistent with results from the Caldicott report, where 86 information flows from the UK health systems were mapped to assess the transfer of patient-identifiable data. It was found that the complete set of patient information was shared even when only certain data are required.[21] These practices present a violation to the Data Protection Act, which allows the use of information under the condition that data are "not excessive in relation to the purpose".[4,10]

Furthermore, assigning institution's fixed passwords, determining the level of information to be shared, monitoring data extraction, and training researchers to prevent unauthorized data disclosure are key technical and administrative safeguard techniques for the security of EHRs.[3,11] Unfortunately, in the current study, more than a third of the researchers claimed that administrators have never or rarely adhere to such techniques. Setting a password to patient records and patient data encryption have been proposed as useful technical safeguard methods for security protection.[22] Passwords are particularly important when data are stored on personal devices such as laptops. Current study results showed that personal laptops are the preferred location for data storage among researchers. This make health data more susceptible to breaches resulting from stealth or loss of devices. A recent study has shown that 95% of health staff have previously reported breaches resulting from loss or stealth of stored data.[9] Additionally, an incident has been reported were data of 34,000 patients were compromised due to stealth of a personal laptop on which they were stored.[3] As per the current study results, universal Serial Bus (USB) flash memories were also used in a considerable percent of the cases to deliver and store data. According to the Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data, breaches due to the loss or stealth of a USB drive compromised 14% and 9% of data breaches reported by healthcare organizations in 2015 and 2016, respectively. The type of data compromised mainly included medical files, insurance records, and payment details.[23] This does not suggest that the use of personal devices must be completely avoided, but rather that efficient methods of security protection should be put in place, such as encryption coupled with password-access.[4]

Encryption of data serves as a valuable technical safeguard for patient health records.[16] It is one of the 10 security domains recommended by the American Health Information Management Association (AHIMA) and is defined as ciphering text so it can only be comprehended by authorized personnel.[22] Despite claiming to have knowledge regarding encryption, the overwhelming majority of current study respondents claimed that patient data were not encrypted. However, an additional technical safeguard was used by the majority of current study participants by installing antivirus into their personal devices which is also in the top ten listed methods for avoiding security breaches.[11] In one incident, health records of almost 100 million patients worldwide were put at risk by security bugs found in one of the world's most widely used patient and practice management systems.[23]

Classifying data into sensitivity levels was previously recommended to limit access to data and limit the type of data shared.[4] Sensitive personal data as defined in data protection legislation should include specific protections for highly stigmatized diseases, such as sexually transmitted and psychiatric illnesses.[24] Current results show that in less than half of the cases, more limitations were put on sensitive data than with regular data. A descriptive cross-sectional study that was conducted in Vietnam assessed practices regarding security and confidentiality of human immunodeficiency virus (HIV)-related information among staff (which is sensitive to stigmatization). The staff practices for securing and protecting patient information were found to be at acceptable levels. However, the protection of patient confidentiality, particularly for data access, sharing, and transfer, still required improvement.[15] Furthermore, it was previously shown that staff from different disciplines had access to data of HIV patient, regardless of their involvement in their care.[16,25] Consequently, certain levels of data must be shared and stored according to the needs of each researcher within a team, rather than being shared in whole. As a matter of fact, this method was preferred by patients in a study by Caine et al, where patients reported their desire for their information to be shared selectively according to the type and recipient of information.[26] Most patients were reluctant that their complete set of data being shared with all recipients. However, another study showed that patients did not mind their complete data being shared for research purposes as long as their consent was obtained.[27] It is argued, however, that patient consent must not be used as the sole method for privacy protection. It is, in fact, debatable whether patients really understand what their consent entails.[28]

One more proposed administrative safeguard method for securing data is de-identification of patient information, which waives the need for consent under the Data Protection Act and eliminates the need for an IRB approval.[10,29,30] In the current study, an IRB approval was claimed to be the most requested document for data release; however, around quarter of data was released without such documentation. Moreover, more than half of the current study participants have received identifiable data for their research. This is against the common law duty of confidentiality in conducting such research whereas obtaining patient's consent is unfeasible.[31,32] Anonymization has been suggested to de-identify patient's

identity; however, the quality of health data collected may be affected leading to loss or mix-up of patient data. Some information may also be relevant to the research query and therefore impossible to omit.[4,25] Alternatively, pseudonymization may be used to ensure confidentiality while maximizing benefit from health records.[33–35]

Imposing laws and regulations that control data sharing, while vital, is not enough. It is essential that the staff at health organizations are made aware about, and active in enacting these laws. The majority of researchers in this study agreed that ethics training must be mandatory prior to conducting clinical studies. This is similar to results reported by Ponemon, where health organizations agreed that most data breaches can be prevented by training employees.[9] Furthermore, training was found to improve practices for confidentiality and security.[15] However, low rates of technical security measures such as encryption in addition to complementary administrative practices including security awareness and training programs were also reported.[3] Therefore, the adherence of health staff to HIPAA or similar organizations' policies must be routinely assessed by health organizations by running audits. Consequently, any breaches or disclosure of confidential data must be recognized and prosecuted.[22,28]

This cross-sectional study and was based on self-reported information provided by researchers at the national level. Furthermore, questions were administered in Arabic language (first language in Jordan) to enhance interpretation. Although all responses are susceptible to recall bias, rates of security and confidentiality practices may have been less prone to this bias, since questions used to assess respondents and administrative practices were more subjective. Furthermore, there may be a source for social desirability bias; however, an anonymous model survey was implemented in an attempt to remedy potential effect. Significance testing (cross-tabulation of knowledge and practices about data sharing as per baseline characteristics of study participants) were not carried out due to relatively low number of responses in each subgroup. Such work is a recommended future study. Future research should consider the inclusion of qualitative studies to explore in depth individual and administrative practices in EHRs data sharing. However, potential barriers towards assessing administrative practices may make it underestimated.

Conclusion

Confidentiality and data sharing practices of healthcare institutions and researchers were generally less than optimal. Such practices might risk the security of electronic patient data, putting them at risk for data loss and medical identity theft. Loss of patient trust in healthcare providers could also occur and could in result affect the quality of care provided. A balance must be found between benefiting from electronic health records for better healthcare and research, and minimizing breaches in data confidentiality. An interwoven effort from health providers, health institutions, and law makers must be put in place in order to protect electronic patient data. In addition to developing regulations on a national level that control data sharing, access, and transfer, healthcare providers must be continuously trained and made aware of such regulations. Institutions are also recommended to run routine audits to assess their performance in this sense. Results of these audits must be translated into continuous revision and development of policies and taking proper measures where misconduct occurs.

Abbreviations

EHR, Electronic Health Records; STDs, sexually transmitted diseases; HIPPA, Health Insurance Portability and Accountability Act; IRB, Institutional Review Board; HRC, Human Research Committee; USB, Universal Serial Bus; AHIMA, American Health Information Management Association; HIV, human immunodeficiency virus.

Ethics Approval

Approval of the study protocol (15/2019) was granted by the institutional review boards of King Abdullah University Hospital and Jordan University of Science and Technology (JUST) on February 28, 2019.

Author Contributions

All authors contributed to data analysis, drafting or revising the article, gave final approval of the version to be published, and agree to be accountable for all aspects of the work.

Funding

Work on this project was supported by grant number 5R25TW010026-02 from the Fogarty International Center of the US National Institutes of Health. The funders had no role in the study design; collection, analysis, and interpretation of data; writing of the report; or the decision to submit for publication.

Disclosure

The authors report no conflicts of interest in this work.

References

1. Win KT. A review of security of electronic health records. *Heal Inf Manag*. 2005;34(1):13–18. doi:10.1177/183335830503400105
2. Layman EJ. Ethical issues and the electronic health record. *Health Care Manag (Frederick)*. 2008;27(2):165–176. doi:10.1097/01.HCM.0000285044.19666.a8
3. Ozair FF, Jamshed N, Sharma A, et al. Ethical issues in electronic health records: a general overview. *Perspect Clin Res*. 2015;6(2):73–76. doi:10.4103/2229-3485.153997
4. Kalra D, Gertz R, Singleton P, Inskip HM. Confidentiality of personal health information used for research. *BMJ*. 2006;333(7560):196–198. doi:10.1136/bmj.333.7560.196
5. Safety I of M (US) C on DS for P. *Key Capabilities of an Electronic Health Record System*. National Academies Press (US); 2003.
6. Safran C, Bloomrosen M, Hammond WE, et al. Toward a national framework for the secondary use of health data: an American Medical Informatics Association white paper. *J Am Med*. 2007;14(1):1–9. doi:10.1197/jamia.M2273
7. Kukafka R, Ancker JS, Chan C, et al. Redesigning electronic health record systems to support public health. *J Biomed Inform*. 2007;40(4):398–409. doi:10.1016/j.jbi.2007.07.001
8. Miller AR, Tucker CE. Encryption and the loss of patient data. *J Policy Anal Manage*. 2011;30(3):534-56. doi:10.1002/pam.20590
9. Ponemon Institute LLC. *Fifth Annual Benchmark Study on Privacy & Security of Healthcare Data.* Ponemon Institute LLC; 2015. Available from: https://media.scmagazine.com/documents/121/healthcare_privacy_security_be_30019.pdf. Accessed 26 November 2019.
10. Data protection - GOV.UK. Gov.uk. Avaliable from: https://www.gov.uk/data-protection/the-data-protection-act. Published 1998. Accessed July 9, 2019.
11. Kruse CS, Smith B, Vanderlinden H, Nealand A. Security techniques for the electronic health records. *J Med Syst*. 2017;41(8):127. doi:10.1007/s10916-017-0778-4
12. Thakkar M, Davis DC. Risks, barriers, and benefits of EHR systems: a comparative study based on size of hospital. *Perspect Heal Inf Manag*. 2006;3(5):5.
13. Menachemi N, Collum TH. Benefits and drawbacks of electronic health record systems. *Risk Manag Healthc Policy*. 2011;4:47–55. doi:10.2147/RMHP.S12985
14. Raposo VL. Electronic health records: is it a risk worth taking in healthcare delivery? *GMS Health Technol Assess*. 2015;11:Doc02. doi:10.3205/hta000123
15. Khac Hai N, Lawpoolsri S, Jittamala P, Thi Thu Huong P, Kaewkungwal J. Practices in security and confidentiality of HIV/AIDS patients' information: a national survey among staff at HIV outpatient clinics in Vietnam. *PLoS One*. 2017;12(11):e0188160. doi:10.1371/journal.pone.0188160
16. Cross S, Sim J. Confidentiality within physiotherapy: perceptions and attitudes of clinical practitioners. *J Med Ethics*. 2000;26(6):447–453. doi:10.1136/jme.26.6.447
17. Cushman R. Serious technology assessment for health care information technology. *J Am Med Inform Assoc*. 1997;4(4):259–265. doi:10.1136/jamia.1997.0040259
18. EI Global Security. *Is cybersecurity about more than protection? EY Global Information Security Survey 2018–19*. Available from: https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/advisory/ey-global-information-security-survey-2018-19.pdf. Accessed 26 November 2019.
19. Abrams L. Health care data of 2 million people in mexico exposed online. Avaliable from: https://www.bleepingcomputer.com/news/security/health-care-data-of-2-million-people-in-mexico-exposed-online/. Accessed July 15, 2019.
20. Filkins BL, Kim JY, Roberts B, et al. Privacy and security in the era of digital health: what should translational researchers know and do about it? *Am J Transl Res*. 2016;8(3):1560–1580.
21. The Caldicott Committee. *Report on the Review of Patient-Identifiable Information*. Department of Health, UK; 1997. Available from: http://static.ukcgc.uk/docs/caldicott1.pdf. Accessed 26 November 2019.
22. Dougherty M. The 10 security domains (AHIMA practice brief). *J AHIMA*. 2004;75(2):56A–D.
23. Ponemon Institute LLC. *Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data*. Ponemon Institute; 2016. Available from: https://www.ponemon.org/local/upload/file/Sixth%20Annual%20Patient%20Privacy%20%26%20Data%20Security%20Report%20FINAL%206.pdf. Accessed November 26 2019.
24. Rumbold J, Pierscionek B. Contextual anonymization for secondary use of big data in biomedical research: proposal for an anonymization matrix. *JMIR Med Informatics*. 2018;6(4):e47. doi:10.2196/medinform.7096
25. Allen A. Confidentiality: an expectation in health care. *Fac Scholarsh Penn Law*. 2008.
26. Caine K, Hanania R. Patients want granular privacy control over health information in electronic medical records. *J Am Med Inform Assoc*. 2013;20(1):7–15. doi:10.1136/amiajnl-2012-001023
27. Spencer K, Sanders C, Whitley EA, Lund D, Kaye J, Dixon WG. Patient perspectives on sharing anonymized personal health data using a digital system for dynamic consent and research feedback: a qualitative study. *J Med Internet Res*. 2016;18(4):e66. doi:10.2196/jmir.5011
28. Fairweather NB, Rogerson S. A moral approach to electronic patient records. *Med Inform Internet Med*. 2001;26(3):219–234. doi:10.1080/14639230110076412
29. Huser V, Cimino JJ. Don't take your EHR to heaven, donate it to science: legal and research policies for EHR post mortem. *J Am Med Inform Assoc*. 2014;21(1):8–12. doi:10.1136/amiajnl-2013-002061
30. Brothers KB, Clayton EW. "Human non-subjects research": privacy and compliance. *Am J Bioeth*. 2010;10(9):15–17. doi:10.1080/15265161.2010.492891
31. Humphreys S. Healthcare datasets: ethical concerns. *Br J Gen Pract*. 2013;63(611):310–311. doi:10.3399/bjgp13X668230
32. *The Health Service (Control of Patient Information) Regulations 2002*. National Health Service, UK. Available from: http://www.legislation.gov.uk/uksi/2002/1438/contents/made. Accessed 26 November 2019.
33. Neubauer T, Heurix J. A methodology for the pseudonymization of medical data. *Int J Med Inform*. 2011;80(3):190–204. doi:10.1016/j.ijmedinf.2010.10.016
34. Noumeir R, Lemay A, Lina J-M. Pseudonymization of radiology data for research purposes. *J Digit Imaging*. 2007;20(3):284–295. doi:10.1007/s10278-006-1051-4
35. Pommerening K, Reng M. Secondary use of the EHR via pseudonymisation. *Stud Health Technol Inform*. 2004;103:441–446.