Original Research Article

Health Informatics Journal

Health Informatics Journal
1–18
© The Author(s) 2024
Article reuse guidelines:
sagepub.com/journals-permissions
DOI: 10.1177/14604582241296398
journals.sagepub.com/home/jhi
Sage

A scoping review of the drivers and barriers influencing healthcare professionals' behavioral intentions to comply with electronic health record data privacy policy

Nabil D Alhassani
School of Health Science, University of Nottingham, Nottingham, UK

Department of Health Administration and Hospital, Faculty of Public Health and Health Informatics, Umm Al-Qura University, Makkah, Saudi Arabia

Richard Windle and Stathis Th Konstantinidis
School of Health Sciences, University of Nottingham, Nottingham, UK

Abstract

Objective: Electronic Health Records (EHRs) are now an integral part of health systems in middle and high-income countries despite recognized deficits in the digital competencies of Healthcare Professionals (HCPs). Therefore, we undertook a scoping review of factors influencing compliance with EHR data privacy policies. **Methods:** Seven databases revealed 27 relevant studies, covering a range of countries, professional groups, and research methods. The diverse nature of these factors meant that 18 separate theoretical frameworks representing technology-acceptance to behavioral psychology were used to interpret these. **Results:** The predominant factors influencing compliance with EHR data privacy policies included confidence and competence to comply, perceived ease of use, facilitatory environmental factors, perceived usefulness, fear that non-compliance would be detected and/or punished and the expectations of others. **Conclusion:** Human factors such as attitudes, social pressure, confidence, and perceived usefulness are as important as technical factors and must be addressed to improve compliance.

Corresponding author:
Nabil D Alhassani, School of Health Science, University of Nottingham, Queens Medical Centre, Nottingham NG7 2HA, UK.
Email: nabil.alhassani@nottingham.ac.uk

Keywords

data security and confidentiality, electronic health record, healthcare policy, human factors, privacy policy

Introduction

Electronic Health Records (EHRs) contain and enable the distribution medical information relevant to the delivery of care of an individual, along with relevant ancillary information, such as their demographic characteristics and insurance or financial data related to their care provision.[1,2] Following rapid developments in this area since 2000, the use of EHRs is now integral to healthcare provision in most developed healthcare systems in high or middle-income countries.[3]

Successful implementation of the EHRs can bring about substantial benefits for patients, HCPs, and the health organizations such as better care, more efficiency, improved data accuracy, and minimal errors. Indeed, successful implementation of EHR is often viewed as a key quality improvement indicator within these organizations.[2,4]

However, for the full benefits of EHRs to be realized, the information they contain must be as freely available as necessary to relevant healthcare professionals, but the widespread and easy access to EHRs within healthcare can also pose a potential threat to patients' data privacy. This can arise from unauthorized access of, or use of this information,[5–7] or through security breaches enabled through poor system security measures or practice.[8] The likelihood of the latter is raised exponentially in relation to the level of access permitted.[9] The potential for risk in this area is also exacerbated by the recognized deficit in digital skills and competencies found within the HCP workforce globally,[10] meaning that inadvertent misuse, or ill-considered uses of data or systems, such as password sharing is more likely.[11,12] Indeed, the most reported privacy violations do seem to be traceable to poor practice by HCPs who have valid access to the EHR system[5]; something that numerous healthcare facilities worldwide have struggled to deal with.[13] A recent study in the US reported 3912 verified healthcare data breach incidents between 2005 and 2019. This level of incident reporting is about 43% higher in the healthcare sector compared with other industries. As a result, the average cost incurred due to these issues is estimated to be approximately $15 million.[14]

Whilst there has been an increased awareness of the need to tackle data security issues within healthcare settings in recent years, rather than reducing, there is evidence that incidents of unauthorized access, where an individual HCP does not have a valid reason to access the data, or where they fail to secure the data they are accessing, are actually becoming more frequent. This increase does not appear to be confined to one healthcare context, but has been observed globally in countries including the UK[15] and Saudi Arabia.[16] Therefore, it is not surprising that concerns around EHR data privacy have escalated in recent years and are being voiced by many stakeholders, including patients and practitioners.[17]

Healthcare organizations themselves often face severe financial or reputational penalties when EHR data breaches occur,[14,18,19] perhaps partly underlying the increased concern they too are showing.[20,21] There is an increase realization that managing and storing patients' data is complex and open to multiple threats[22] and that many healthcare systems simply do not have the experience, expertise or processes to deal with this adequately.[23] At the same time, national and pan-national legislation, such as the EU's General Data Protection Regulations (GDPR), are requiring greater and greater stringency, governance, risk management and accountability.[24] Therefore, data privacy has become a fundamental element within health organizations' strategic plans,[25,26] with many implementing official data policies[27] that require HCPs to follow strict and comprehensive protocols for using digital technology and managing data security.[5]

Given that the behavior of HCPs concerning data privacy plays such a pivotal role in the effectiveness (or otherwise) of data security, it is vital to comprehend the factors that may influence behavior in this area. In particular, it is imperative to understand what drives or impedes compliance with data privacy policies. Moreover, while it is broadly accepted that attitudes to technology acceptance will play a big part in this, many other factors may likely act as barriers or drivers to compliance behavior.[28] Furthermore, some of these factors will be common, and others related to more specific sociocultural, national, or clinical contexts.[5] Therefore, a broad investigation is required to uncover these factors within the literature.[5,29]

Given the diverse nature of the likely influences on behavior, it is also expected that studies that have factors to investigate these will utilize a range of research methodologies. Therefore, a scoping review was adopted, as this approach is exploratory in nature. It does not exhibit bias towards or seek to assimilate similar types of studies or methodologies. Instead, this approach relies on more narrative synthesis and allows the inclusion of literature from a broad range of sources. In addition, it does not seek to exclude evidence based on an assessment of its quality. The present scoping review has been undertaken with the following question: "What does the literature reveal about the factors that influence HCPs' intention to comply with the local data privacy policies aimed at protecting information within the EHR?" It aims to comprehensively understand the existing evidence base in this area. By comprehending the factors that influence the HCPs' intention with the EHR privacy policy, we hope to understand current behavioral practices and develop better strategies to support compliance in the future.[30]

Materials and methods

Joanna Briggs Institute scoping review framework

This scoping review was conducted according to Joanna Briggs Institute's scoping review guidelines.[31] A scoping review allows researchers to explore the breadth of the literature and identify available materials in a particular field of investigation.[32] It is particularly suitable for an exploratory investigation of the literature into an area that is not highly focused, researched or clearly defined, and where several disparate elements may be expected to be contribute to the scope of the subject under investigation. Given its nature as an investigation into the boundaries of a field of study, the methodology does not rely on a systematized evaluation of the quality of the evidence-based discovered as part of the inclusion process, rather leaving it to the researcher to comment on and evaluate the significance of this. It is also suitable where the researcher expects to acquire information gained from a range of different study designs and research paradigms in order to cover the breadth of investigation required. It enables the researcher to call on both published and unpublished, peer reviewed and non-peer reviewed information.[32] A scoping review was, therefore, highly suitable for this investigation of the, as yet poorly defined and potentially disparate factors that influence HCPs' intentions to comply with data privacy.

Whilst scoping reviews do not rely on a published protocol or the rigid approach adopted for systematic reviews, the JBI-derived framework used in this study does apply standardized steps to the design, searching and presentation of results, in order to ensure the highest level of rigor and validity.[33] These steps are outlined in Table 1.

Table 1. The list of steps undertaken when conducting a scoping review in line with enhanced JBI Scoping Review Framework, as followed in this study.

Enhancements Framework 2015
Defining and aligning the objective/s and question/s
Developing and aligning the inclusion criteria with the objective/s and question/s
Describing the planned approach to evidence searching, selection, data extraction, and presentation of the evidence
Searching for the evidence
Selecting the evidence
Extracting the evidence
Analysis of the evidence
Presentation of the results
Summarizing the evidence in relation to the purpose of the review, making conclusions and noting any implications of the findings

Defining and aligning the objectives and question

Scoping review question. The following question was defined by the researchers, in consultation with other experts in the field:

"What does the literature reveal about the factors that influence HCPs' intention to comply with the local data privacy policies that are aimed at protecting information within the EHR?"

Scoping review objectives. In order to address the research question outlined above, the following review objectives were outlined:

i. To identify what is already known about the barriers and drivers that influence HCPs' compliance or intention to comply with their local data privacy policies, as these relate to the EHR.
ii. To identify the theoretical frameworks that have been applied to this area of study and how these relate to different fields of study.
iii. To synthesize the information gained regarding barriers and drivers that influence HCPs' compliance or intention to comply with their local data privacy policies into one holistic framework.

Developing and aligning the inclusion criteria with the objective/s and questions

Whilst the aim of this scoping study was to gain a holistic view of the barriers and drivers to HCPs compliance with data privacy policy, it was still necessary to define boundaries for the searches undertaken through the application of inclusion exclusion criteria. These are listed below in Table 2. This ensures that the review is manageable and the results are interpretable

Describing the planned approach to evidence searching, selection, data extraction, and presentation of the evidence

Participants. The search covered all HCPs using EHR systems as end-users, that is, inputting or accessing the data for clinical purposes.

Table 2. Inclusion and exclusion criteria applied to the search strategy for this scoping review of the factors influencing compliance of EHR data privacy by healthcare professionals.

Criteria	Inclusion	Exclusion	Reason/Alignment to research research question
Study language	English	Not English	The research team did not have the capacity to rigorously interpret studies published in other languages
Study design	All research designs aimed at collecting or collating empirical data	Narrative and opinion pieces	The research question requires a broad approach but is based on experimental evidence
Participants	HCPs working in healthcare settings with access to EHR	Non-HCPs, those accessing the system for technical or administration purposes, or HCPs not using EHR	The views of all HCPs accessing the multi-professional records are important in this study
Timeframe	2003 to February 2024	Before 2003	The year 2003 selected as the starting date, due to the implementation of relevant legislation. For example, the national health Service (NHS) in the UK started the adoption of EHRs 3 3 in 2002, while in 2004, the EHR adoption plan for the USA was announced[34]
System	EHR, as defined in the introduction	Non-EHR	The study focuses on EHR, and factors influencing compliance with data privacy in other formats are likely to be extensively different, and indeed, fewer breaches have been reported from purely paper-based systems[35]
Subject area	Studies that investigate compliance or intentions to comply with data privacy policies regarding EHR	Studies that focus only on EHR usage or usability or acceptance without reference to impact on data privacy compliance Studies that look at behavior intentions in other fields of activity unrelated to data privacy and security	To remain within the focus of the research question
Setting	Any health organizations using an EHR system in conjunction with patient care, as defined within the introduction	Organizations using EHR for training or simulation purposes only	This is a global scoping study and is not seeking to categorize by the nature or location of the organization

Concept. The review focused on the HCPs' compliance or intentions to comply with EHR data privacy, as presented in Table 2.

Context. This review includes any health organization with an EHR implemented for clinical purposes, as shown in Table 2. As the investigation is global, the review was not limited to a specific country, region, or demographic group.

Outcome. The outcomes considered within this review were wide in nature and included any measures or records of compliance or stated intentions in relation to compliance, and the factors that were recorded or articulated as impacting on this compliance or intention to comply. HCPs' perceptions, attitudes, beliefs, social influences, perceived control, and behavioral intentions regarding compliance were the main concern of this review.

Searching, selecting, and extracting evidence. Following exploratory searches using the OVID (MEDLINE) database and consultation with expert search librarians regarding the search approach and search objectives, the main search for this study was carried out using seven scientific publications' databases, as between them, these were known to cover the key literature in this area. These were; Cochrane library, OVID (MEDLINE, AMED, PsycINFO, and EMBASE), SCOPUS, and Web of Science.

The Medical Subject Headings (MeSH), EHR, Data privacy and security, Behavior, and HCPs were used to generate key words for the full search strategy (see Table 3).

"Hand searching", that is searching outside of the recognized scientific databases of published work, was also carried out using the Google Scholar search engine to identify any additional information fitting within the inclusion criteria. The reference lists of relevant articles found through the search process were also hand searched for relevant article that could be included.

Table 3. The search terms used, and the relationships between them, as employed to interrogate the databases used to identify articles relating to the barriers and drivers influencing behavioral intentions to comply with data privacy policies in relation to EHR use.

Concept1 AND	Concept2 AND	Concept3 AND	Participants
Electronic medical record* OR electronic health record* OR computerized medical record* OR computerized health record* OR hospital information system* OR medical records systems OR computerized OR electronic health records OR EHR	Privacy, computer security OR data privacy OR data security OR data breach OR security breach OR information breach OR privacy concerns* OR confidentiality	Perception* OR attitude OR belief* OR issues* OR ethics* OR behavior* OR behavior	Health personnel* OR nurse* OR doctor* OR hospital employee* OR health information management staff

The asterisk (*) is usually employed when searching databases to magnify results by netting all words that begin with the same letter. It aids in discovering variations of a term with fewer words typing.

Selecting the evidence

Based on the approach outlined above, the search was performed in February 2024 on the seven databases noted. This resulted in 2964 articles. An additional five articles were found by hand-searching.

In order to find the articles that were relevant to the research question posed, the articles identified from the search process were then screened using the Preferred Reporting Items for Systematic reviews and Meta-Analyses (PRISMA) process.[36] This is illustrated in Figure 1. Initially, 387 duplicate articles were removed using bibliographic software. Following this process, an initial screening of the titles of the papers resulted in a further 2577 being rejected. Therefore, 164 articles were then retrieved for further screening. Screening of the abstracts and then full text of these articles led to the exclusion of a further 142, leaving 22 articles that satisfied the inclusion criteria for the study. The five hand-sought articles were added to these to make a total of 27 articles that were accepted into the analysis phase of the review. The detailed reasons for excluding the articles from the study are outlined in Figure 1. Moreover, the Scoping Reviews (PRISMA-ScR) Checklist was used to help in checking and identifying the content of the review[37] (see Table 10 in the supplementary file).

Extracting the evidence

The 27 articles identified as being relevant to the review were read in detail several times and all information contained within them that was relevant to the search question was extracted. The information was coded and stored for thematic analysis, using EndNote Version 20.

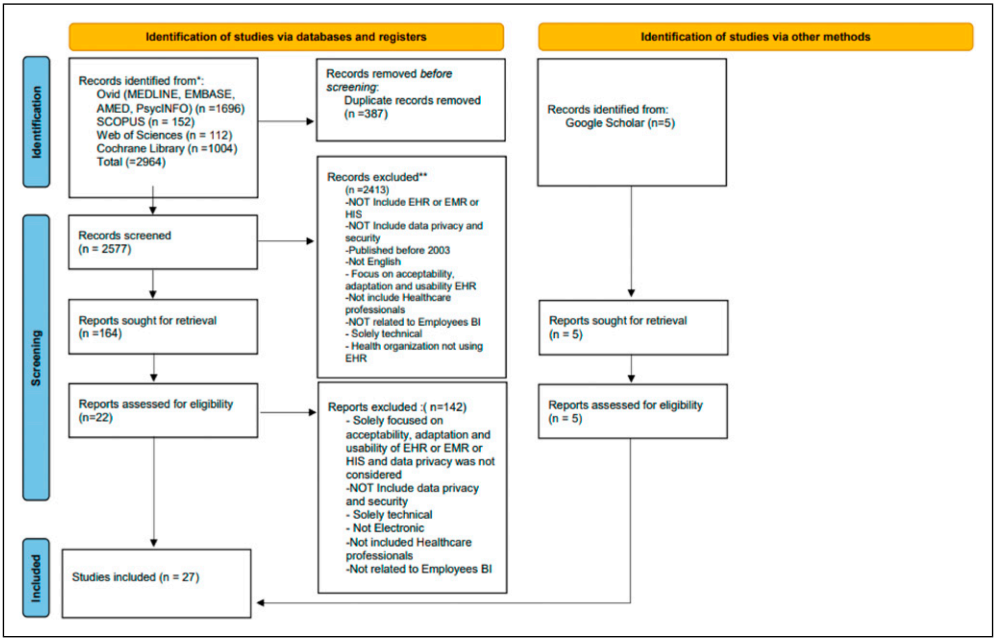
Identification of studies via databases and registers
Identification of studies via other methods
Identification
Screening
Included
Records identified from*:
Ovid (MEDLINE, EMBASE, AMED, PsycINFO) (n =1696)
SCOPUS (n = 152)
Web of Sciences (n = 112)
Cochrane Library (n =1004)
Total (=2964)
Records removed *before screening*:
Duplicate records removed (n =387)
Records identified from:
Google Scholar (n=5)
Records screened (n = 2577)
Records excluded**
(n =2413)
-NOT Include EHR or EMR or HIS
-NOT Include data privacy and security
-Published before 2003
-Not English
- Focus on acceptability, adaptation and usability EHR
-Not include Healthcare professionals
-NOT related to Employees BI
- Solely technical
- Health organization not using EHR
Reports sought for retrieval (n =164)
Reports sought for retrieval (n = 5)
Reports assessed for eligibility (n=22)
Reports excluded :(n=142)
- Solely focused on acceptability, adaptation and usability of EHR or EMR or HIS and data privacy was not considered
-NOT Include data privacy and security
- Solely technical
- Not Electronic
-Not included Healthcare professionals
-Not related to Employees BI
Reports assessed for eligibility (n = 5)
Studies included (n = 27)

Figure 1. The PRISMA flow diagram outlining the steps taken to collect and review articles for inclusion in the scoping review.[36]

Analysis of the evidence

As outlined above, each article included in the review was subjected to thematic analysis. A narrative synthesis was used to combine the findings from the different papers together. This included an iterative combining of the more granular themes identified from individual papers into more robust, general categories. This process of coalescing the themes continued until these could not be justifiably combined further.

Presentation and summarization of the data

The data will be presented and discussed in the remainder of this article in textual form. Conclusions and implications of the findings will be presented in a similar manner.

Results

Summary of the studies

All of the 27 studies included in this review focused on the factors that influence HCPs' intention to comply with data privacy in relation to EHR use and were conducted in healthcare organizations that have electronic systems. The majority of the studies used descriptive, quantitative approaches with questionnaires being the most commonly used data collection tool. Two studies did employ qualitative methods[28,38] and one study was a systematic review[58] (see Table 6 in the supplementary information).

There has been a surge of research interest on the factors that influence HCPs' compliance with EHRs data privacy globally in recent years with the results indicating that 88% of the studies captured in this scoping review were published between 2015 and 2023, (see Table 7, supplementary information). Studies were published in a range of different countries from America, Europe, Asia and the Middle East, representing high or middle-income countries, as might be expected in relation to the prevalence of EHR implementation. Whilst six studies focused on nurses, most studies included participants from a range of healthcare professions.

Study categorization

The majority of the studies included in this review were aimed at measuring HCPs' behavioral intentions towards EHR data privacy (see Table 6, supplementary information). However, a closer examinations showed that four clear subgroups emerged based on the objectives of the investigations undertaken (see Table 4). 12 of the studies were focused on uncovering the HCPs' intentions

Table 4. Study categories based on behavioral intention categorization of studies included in the scoping review, based on the objectives of the original investigation and the aspects of behavioral intention that they sought to investigate in relation to EHR data privacy policy.

Behavioral intention	Included studies	No.	%
Compliance intention	6,17,42,45,47,46,48,52,54,56,58,60	12	46.15
Attitude, perception, and awareness	28,38,40,41,44,49,51,53,55,59	10	34.6
Protection intention	39,50,57	3	11.5
Violation intention	5,43	2	7.6

towards compliance. 10 studies focused on their attitudes, perceptions, and awareness toward the EHR privacy policy itself. Three studies sought to understand the HCPs' reasons to protect EHR data, whilst two studies looked at the opposite; their willingness to violate the EHR policy.

Factors identified as impacting HCP's intentions to comply with data privacy in relation in EHR

Overall, 82 different factors were identified as influencing the intentions of HCPs to comply with data privacy policies. Many of these factors were unique to one publication, although some were common to many. Thematic analysis of the factors enabled them to be grouped as overarching themes emerged. A detailed breakdown of the factors can be observed in Table 8, supplementary information, and Table 5, which lists the 17 key thematic areas that arose. These can cover the individual, the work environment, and broader organizational factors.

Extracted theories and theoretical framework

In total, 18 different theoretical frameworks were adopted by 21 out of 27 studies to help interpret HCPs' compliance with the EHR policy, with eight adopting multiple frameworks[5,6,40–42,45,53,54] (see Table 9 in supplementary file). These theories range from pure behavioral theories, the most commonly used being the Theory of Planned Behavior (TPB),,[5,42,45,52,59,60] which argues that action is determined by beliefs or the perceived beliefs of others, about a behavioral course of action. Others, such as Deterrence Theory (DT),[5,17,47,56] and Protection Motivation Theory (PMT),[6,57] are concerned with responses to threats. Moreover, some studies adopted theories that related more specifically to technology adoption behaviors, including the Technology Acceptance Model (TAM),[42,45] or the Unified Theory of the Acceptance and Use of Technology (UTAUT),.[38,42]

Discussion

Scope and focus of observations

The data from the papers included in the scoping review show there were many different factors that arose as influencing HCPs intentions to comply with data privacy policy and procedure in relation the EHR. Many of these were internal factors, such as attitude, confidence or concern about the implications for non-compliance (see Table 5). This is perhaps not surprising as the vast majority of the studies started with a purpose to explore person-centered behavioral objectives, such as intentions to comply, or inherent attitudes, as outlined in Table 4. However, between them the studies also uncovered a whole range of structural factors such as organizational culture that also influenced behavior.

The broad scope that must be considered when looking at factors influencing intentions to comply with data privacy policy, as outlined in the results of the review is also evident from the range of theoretical positions and perspectives that were applied in attempts to understand the observations made. It is pleasing to see that nearly all of the studies relied on at least one theoretical framework in order to interpret their results. In total, 18 different theoretical frameworks have been employed in this way. These theories and theoretical framework were adopted from different fields, such as psychology, criminology and technology disciplines. Several of the theoretical frameworks were used to determine the actual behavior or behavioral intentions of HCPs.[58]The diversity of theoretical frameworks in the reviewed studies indicate that there is no single theory or theoretical

Table 5. The key thematic areas that arose from data extraction and synthesis from the papers contained within the scoping review show the number of articles that noted this theme at least once and gave a subjective description.

No	Themes	No of papers	Description
1	Confidence and competence	10	The ability and confidence of individuals to undertake data privacy activities, including self-efficacy, perceived knowledge, skills, and experience
2	Punishment severity	6	The perceived severity of any breach in policy
3	Detection certainty	5	How likely participants felt it was that breaches in policy would be detected, including monitoring and audit
4	Punishment certainty	4	How likely participants felt that punishments for non-compliance would be applied
5	Social influences	7	The extent to which other's perceptions influenced compliance, including peer and superior influence and religion
6	Attitude	10	The general attitude of the subject to the importance of data privacy and its negligence
7	Personal benefit and recognition	3	The extent to which compliance benefitted the individual participant
8	Personality	2	The personality traits of participants that made it more or less likely that they would comply, including self-control, stress, coping, and commitment
9	Perceived usefulness	8	How useful participants felt maintaining data privacy was
10	Privacy, confidentiality, and security concerns	7	The extent to which concerns about issues relating to patient data, including ethical issues, regulatory concerns, and safeguards, influenced intentions
11	Perceived ease of use	8	How easy it was to undertake data privacy activities, including system and process factors
12	Perceived behavior control	7	The level of control, involvement, or perceptions of trust that participants felt they have over the process
13	Perceived level of direction	5	The extent to which participants felt they gained clarity about what was required and why, either from legal or institutional policies
14	Facilitating conditions	8	Organizational and environmental factors that supported data privacy compliance or emphasized its importance
15	Training and awareness programs	8	The availability and impact of training and awareness programs
16	Perceived organizational support	4	How much support was available during the process
17	Clinical needs	3	The particular clinical characteristics underpinning the data being accessed or stored

framework that alone can adequately explain HCPs' compliance or behavioral intention concerning EHR privacy and security policies. Nevertheless, it is notable that the most frequently used theoretical frameworks were the TPB, the DT, and the PMT.[58]The TPB argues that our externalized behaviors are driven largely by our beliefs and attitudes towards the behavior and its outcome, as well as our own beliefs about how others perceive our potential behavior in this area. Therefore, internal, person-centered factors become the overarching barriers and drivers to behavior despite the facilitatory or inhibitory conditions that surround the action, suggesting the primacy of these internal factors. The DT and PMT theoretical frameworks are concerned with perceptions about avoidance of negative consequences as a result of decisions taken in relation to behavioral actions, and so again, deal very largely with internalized factors.

Of course, it does not follow that the most used theories are the best fit to study the HCPs' compliance behavior, and we also have to be careful of an ""echo chamber effect" where application of the theoretical model can lead to observations to support that positioning. However, it is notable that theoretical models that dealt more with the technological aspects of the EHR and data privacy did not feature highly in the investigations, suggesting that this was not seen as a primarily a technological issue. In the longer term, other frameworks such as Decomposed Theory Planned Behavior (DTPB), which is an extended theory from the TPB,[61]should be also considered, as they offer a broader number of constructs and may be able to holistically capture and categorize many of the factors more fully.

The broad scope of the observations does also illustrate and confirm the decision to undertake this review as a scoping review, which enables a much more exploratory investigation of the literature without the constraints of a systematic review and enables a wider range of literature to be considered in order to probe the parameters of the field under investigation.[31,32]

Confidence and competence

Whilst this review is primarily a qualitative synthesis, confidence and competence were the elements most commonly reported as having an influence on compliance, despite the focus of the investigation undertaken.

A lack of computer skills, such as logging in and off from the system, and changing passwords, can hinder HCPs from running the electronic health system properly.[6,39] There is a well-recorded deficit in digital competencies across HCPs internationally,[6,39,42,46] and it is vital that this is addressed, if higher levels of compliance with data privacy procedures are to be effectively implemented. Some studies have suggested that hospitals should equip HIM staff with suitable and sufficient skills to operate software and hardware in a way that ensures data privacy is protected.[6] Nurses' self-efficacy, that is their personal belief that they are capable to execute the course of action required, is important with regard to their technical abilities to maintain EHR data privacy.[39] Indeed, when hospital staff are made aware that the management trust and rely upon their skills to protect data, their intentions to comply with data regulations has been seen to increase commensurately.[50]

Negative consequences from non-compliance

Concerns over detection of non-compliance, the level of any ensuing punishment or negative personal consequences as well as the certainty with which HCPs perceived such a punishment would be applied were clearly factors that influenced HCPs intentions to comply with EHR data privacy policy. Monitoring was considered to be a driver for the HCPs' compliance.[17,58,56] It has been reported that HCPs are deterred from violating EHR privacy policy if the policy itself states and communicates to them that the system is actively monitored, and that any unethical or illegal activities and non-compliance will be detectable.[17] Nurses' intentions to violate privacy policy can be deterred if their organizations audit and inspect employee use of the EHR, as this makes employees feel more accountable for their actions.[47] Moreover, the severity and certainty of sanctions have been reported to be effective in reducing non-compliance behavior towards data privacy policy among HCPs and others who work within healthcare organizations.[6,17,58,47] Thus, the more HCPs and other professionals are worried about the consequences of violating EHR and other data policy, the more likely they are to follow it.

In contrast, some studies argued that sanction and punishments cannot solely prevent the HCPs from violating data privacy policy.[43] Furthermore, if health organizations monitor HCPs' activities via the computerized system, this can reduce inappropriate system usage behavior, but might also impact their performance negatively, due to feelings of suspicion, which are known to have detrimental impacts on moral and productivity.[17]

Social influence

Social influence is the change in behavior that one person causes in another, intentionally or unintentionally. It happens as a result of the way the influencee person perceives themselves in relationship to the influencer, other people and society in general.[62]

Peer social influence is an important factor that influences HCPs' intentions towards data privacy policy and regulations.[5,6,39,45,47] Previous studies have reported that nurses are more likely to influence other nurses to desist from non-compliance if they themselves are skilled and familiar with the EHR data privacy process,[39,47] and peer influence between IT staff in hospitals has been found to be effective to the management and valuing the privacy environment in the hospital.[6] However, the actual strength of this influence is disputed. Foth[5] for example argues that from their observations, peer influence between HCPs is low regarding adherence to data protection rules. Therefore, we need to understand more about the nature and effectiveness of positive peer influences.

Many scholars agree that a positive influence of supervisors and managers has an important driving effect on the intention of HCPs to accept the data privacy policy and regulation.[6,39,45,47] However, this can also have negative influence if the culture inside the hospital prioritizes HCPs' task-based productivity over their compliance with EHR privacy and security measures.[53,58]

Attitudes, personality and personal gain

Attitudes towards compliance[5,41,45,48,39,55,58,60] and conceptions of negligence[51,53,58] were seen to play a mediating role in the intentions of individual HCPs to comply with data privacy. Likewise, personality traits, including self-control,[58] stress and coping strategies[58] were also seen to mediate compliance. However, it must be recognized that these are intermediary, potentially dynamic constructs, as much influenced by other personal and organizational factors as they in turn influence them.

The prospect of personal benefit and recognition was one of the drivers seen have a positive impact on compliance intention towards data protection regulations.[5,46,52,50] HCPs were more likely to comply where they felt it led to intrinsic personal benefit,[57] or if they felt their efforts were noticed and appreciated.[48] This suggests that healthcare organizations need to create a reward environment, to encourage the system's end users to follow the rules. Moreover, there is evidence that suitable rewards systems can have a positive impact on reinforcing compliance into more habitual behavior[46] with a potentially greater and more sustained impact on data protection.

Perceived usefulness and perceived ease of use

Perceived Usefulness is the extent to which the employee believes that using a specific application will increase their job performance,[63] and Perceived Ease of Use, is the extent to which task-effort is minimized.[63] These are both key constructs in many technology acceptance models, and they did indeed feature in the review here. There was generally a sense that compliance with data privacy policy was useful for HCPs as individuals[49,59,54] and also for patient care.[49]

Many factors were listed as negatively impacting on ease of use of the systems or processes. Impact on workload was an important example of this. Workload is a key barrier to HPCs' compliance with EHR policy,[58] and compliance itself can sometimes exert an invisible additional pressure on clinical staff.[46] HCPs can find themselves facing dilemmas between the impetus to comply with privacy and security regulations and the expectations placed upon them to provide clinical care in practice.[38] Other studies have indicated major concerns about HCPs' compliance with data protection within health organizations due to the added a workload and changed clinical workflow.[5,45] Some researchers asserted that HCPs can be preoccupied with privacy issues to the extent that this obstructs their work routine, which can ultimately cripple the system usage itself in addition to potentially reducing quality of care and undermining patient satisfaction and safety.[40] Some studies reported that suboptimal workflows caused HCPs to adopt negative behaviors such as failing to log out at the end of session or copying patient information, even though they were aware of the pertinent privacy regulations and understood the legal consequences.[28,58,54,53] Some adopted beliefs that stringent information privacy protection regulations were negatively impacting on patient care.[28,38,51]

Perceived behavior control

A sense of ownership, involvement and control in the process of data privacy also appeared to be an important factor in some of the studies identified in this review, and it is known that these factors can play an important role in behavioral intention and technology acceptance.[5,39,58,40,41] However, this appears to be a fine balance as HCPs were also concerned about receiving an appropriate and helpful level of direction for the use of the process from both organizational[58,38] and legislative frameworks.[40]

Facilitating conditions and training

Although person-centered factors were clearly important in relation to intentions to comply with EHR data privacy, a number of structural components were identified that could influence this intention. Many of these related to the organizations in which the HCPs worked and related to issues such as their organizational management,[58] the culture within the organization,[58] the size and status of the organizations concerned,[40] their maturity in terms of information security,[44] the clarity of the communication[39] and the integration of the processes into already established everyday working practices.[58] It is clear then that organizations wanted to undertake successful implementation or improve the compliance with data privacy must address institutional culture and may need to invest specifically into change management processes.

Resource availability is another factor that facilitates a higher level of compliance with data protection regulations.[5,46,54] The availability of compatible software and hardware affiliated with the hospital EHR system was found to enable privacy protection behavior among nurses in Taiwan.[39] Moreover, training and availability of information have been shown to be essential for a high level of adherence to data protection regulations among HCPs.[56,5,51,52,58] Training can empower and equip the HCPs with the knowledge and skills they need when they notice privacy or security threats, empowering them to adhere with best practices.[50–52,58] It can positively impact the HCPs' awareness and their compliance with the EHR privacy policy.[52] Conversely, a lack of training and insufficient knowledge can lead to inadvertent data breaches.[43,51]

Limitations

Whilst scoping reviews do not require critical appraisal of the materials accessed, some limitations need to be noted regarding studies that were included in. Firstly, this method may lead to the inclusion of low-quality data. The reviewed studies primarily relied on one source of information, and most often on self-reporting, rather than observation or more objective measures. This could lead to bias in the results analyzed. Moreover, several studies analyzed multiple HCP groups and so it was not possible to draw conclusions between them.[5,38,42]

With regard to the conduct of the scoping review itself, again, some limitations need to be acknowledged. Even though this review was performed on seven major databases, inclusion of other databases may have uncovered other, more specialized articles and hence other factors to be considered.[64]

Conclusions

This review set out to explore the factors that influence HCPs intentions to comply with EHR privacy policy and showed that in recent years a range of studies had sought to capture this information in a range of countries. The review identified many individual and organizational factors that have the potential to either encourage or hinder associated behavior. These observations were under pinned by a series of diverse theoretical frameworks, highlighting the multifactorial nature of these influential factors.

The review shows that in order for an organization to develop approaches that improve compliance, they must take a multifaceted approach working to improve training, capability and training of their workforce and also ensuring that the organizational culture is one that is mature in its management of change, has sufficient structural resources and clearly values individuals for their work in this area. Clearly articulating the potential consequences of lack of compliance is also important.

As the current research is primarily quantitative in nature, there may be scope to conduct qualitative or mixed methods research in order to gain deeper an in-depth insight into the behavioral intentions of HCPs toward data privacy compliance.

Declaration of conflicting interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article.

Ethical statement

Ethical approval

The full name of the ethical board: FMHS resaerch ethics committte review and favourable opinin at Faculty of Medicine & Health Sciences, University of Nottingham. Ethics refernce No : FMHS 316-0723.

ORCID iDs

Nabil D Alhassani https://orcid.org/0000-0003-1900-4581
Stathis Th Konstantinidis https://orcid.org/0000-0002-3680-4559

Supplemental Material

Supplemental material for this article is available online.

References

1. Uslu A and Stausberg J. Value of the electronic medical record for hospital care: update from the literature. *J Med Internet Res* 2021; 23: e26323. DOI: 10.2196/26323.
2. Lorkowski J and Pokorski M. Medical records: a historical narrative. *Biomedicines* 2022; 10: 2594. DOI: 10.3390/biomedicines10102594.
3. Currie WL and Finnegan DJ. The policy-practice nexus of electronic health records adoption in the UK NHS: an institutional analysis. *J Enterprise Inf Manag* 2011; 24: 146–170. DOI: 10.1108/17410391111106284.
4. Tapuria A, Porat T, Kalra D, et al. Impact of patient access to their electronic health record: systematic review. *Inform Health Soc Care* 2021; 46: 192–204. DOI: 10.1080/17538157.2021.1879810.
5. Foth M. Factors influencing the intention to comply with data protection regulations in hospitals: based on gender differences in behaviour and deterrence. *Eur J Inf Syst* 2017; 25: 91–109. DOI: 10.1057/ejis.2015.9.
6. Sher ML, Talley PC, Yang CW, et al. Compliance with electronic medical records privacy policy: an empirical investigation of hospital information technology staff. *Inquiry: The Journal of Health Care Organization, Provision, and Financing* 2017; 54: 004695801771175. DOI: 10.1177/0046958017711759.
7. Rothstein MA. Health privacy in the electronic age. *J Leg Med* 2007; 28: 487–501. DOI: 10.1080/01947640701732148.
8. Kumar R, Marchang N and Tripathi R. Distributed off-chain storage of patient diagnostic reports in healthcare system using IPFS and blockchain. In: *2020 International conference on communication systems and networks (COMSNETS)*. Piscataway: IEEE, 2020, pp. 1–5.
9. Kuo KM, Ma CC and Alexander JW. How do patients respond to violation of their information privacy? *Health Inf Manag* 2014; 43: 23–33. DOI: 10.1177/183335831404300204.
10. Navarro-Martínez O, Igual-García J and Traver-Salcedo V. Bridging the educational gap in terms of digital competences between healthcare institutions' demands and professionals' needs. *BMC Nurs* 2023; 22: 144.
11. Safa NS, Sookhak M, Von Solms R, et al. Information security conscious care behaviour formation in organizations. *Comput Secur* 2015; 53: 65–78. DOI: 10.1016/j.cose.2015.05.012.
12. Stanton JM, Stam KR, Mastrangelo P, et al. Analysis of end-user security behaviors. *Comput Secur* 2005; 24: 124–133. DOI: 10.1016/j.cose.2004.07.001.
13. Anwar RW, Abdullah T and Pastore F. Firewall best practices for securing smart healthcare environment: a review. *Appl Sci* 2021; 11: 9183. DOI: 10.3390/app11199183.
14. Seh AH, Zarour M, Alenezi M, et al. Healthcare data breaches: insights and implications. In: *Healthcare*. Basel: MDPI, 2020, p. 133.
15. Saxena N, Bhadoria RS, Dickerson S, et al. Security and privacy issues in UK healthcare. In: *Security and privacy of electronic healthcare records: concepts, paradigms and solutions*. London: Institution of Engineering and Technology, 2019, p. 283.
16. Almaghrabi NS and Bugis BA. Patient confidentiality of electronic health records: a recent review of the Saudi literature. *Dr Sulaiman Al Habib Med J* 2022; 4: 126–135. DOI: 10.1007/s44229-022-00016-9.

17. Kuo KM, Talley PC and Cheng TJ. Deterrence approach on the compliance with electronic medical records privacy policy: the moderating role of computer monitoring. *BMC Med Inform Decis Mak* 2019; 19: 254. DOI: 10.1186/s12911-019-0957-y.
18. Rowland SP, Fitzgerald JE, Lungren M, et al. Digital health technology-specific risks for medical malpractice liability. *NPJ Digit Med* 2022; 5: 157. DOI: 10.1038/s41746-022-00698-3.
19. Kwon J and Johnson ME. Healthcare security strategies for data protection and regulatory compliance. *J Manag Inf Syst* 2013; 30: 41–66. DOI: 10.2753/MIS0742-1222300202.
20. Andriole KP. Security of electronic medical information and patient privacy: what you need to know. *J Am Coll Radiol* 2014; 11: 1212–1216. DOI: 10.1016/j.jacr.2014.09.011.
21. Ghazvini A and Shukur Z. Security challenges and success factors of electronic healthcare system. *Procedia Technology* 2013; 11: 212–219. DOI: 10.1016/j.protcy.2013.12.183.
22. Choi SJ and Johnson ME. Do hospital data breaches reduce patient care quality? arXiv preprint arXiv: 190402058 2019. https://arxiv.org/pdf/1904.02058
23. Sipanoun P, Oulton K, Gibson F, et al. The experiences and perceptions of users of an electronic patient record system in a pediatric hospital setting: a systematic review. *Int J Med Inform* 2022; 160: 104691. DOI: 10.1016/j.ijmedinf.2022.104691.
24. Georgiou D and Lambrinoudakis C. Data protection impact assessment (DPIA) for cloud-based health organizations. *Future Internet* 2021; 13: 66.
25. Casadesus-Masanell R and Hervas-Drane A. Competing with privacy. *Manag Sci* 2015; 61: 229–246. DOI: 10.1287/mnsc.2014.2023.
26. Chuma KG and Ngoepe M. Security of electronic personal health information in a public hospital in South Africa. *A Global Perspective* 2022; 31: 179–195. DOI: 10.1080/19393555.2021.1893410.
27. Alzamil ZA. Information security practice in Saudi Arabia: case study on Saudi organizations. *Informa Compu Sec* 2018; 26: 568–583. DOI: 10.1108/ICS-01-2018-0006.
28. Eikey EV, Murphy AR, Reddy MC, et al. Designing for privacy management in hospitals: understanding the gap between user activities and IT staff's understandings. *Int J Med Inform* 2015; 84: 1065–1075. DOI: 10.1016/j.ijmedinf.2015.09.006.
29. D'Arcy J and Greene G. Security culture and the employment relationship as drivers of employees' security compliance. *Inf Manag Comput Secur* 2014; 22: 474–489. DOI: 10.1108/IMCS-08-2013-0057.
30. Desveaux L, Agarwal P, Shaw J, et al. A randomized wait-list control trial to evaluate the impact of a mobile application to improve self-management of individuals with type 2 diabetes: a study protocol. *BMC Med Inform Decis Mak* 2016; 16: 144, Journal Article; Randomized Controlled Trial; Research Support, Non-U.S. Gov't. DOI: 10.1186/s12911-016-0381-5.
31. Joanna Briggs Institute reviewers' manual: 2015 edition / Supplement.
32. Tricco AC, Lillie E, Zarin W, et al. A scoping review on the conduct and reporting of scoping reviews. *BMC Med Res Methodol* 2016; 16: 15. DOI: 10.1186/s12874-016-0116-4.
33. Peters MD, Godfrey CM, Khalil H, et al. Guidance for conducting systematic scoping reviews. *Int J Evid Based Healthc* 2015; 13: 141–146. DOI: 10.1097/XEB.0000000000000050.
34. Simborg DW. Promoting electronic health record adoption. Is it the correct focus? *J Am Med Inform Assoc* 2008; 15: 127–129. DOI: 10.1197/jamia.M2573.
35. Ronquillo JG, Erik Winterholler J, Cwikla K, et al. Health IT, hacking, and cybersecurity: national trends in data breaches of protected health information. *JAMIA Open* 2018; 1: 15–19. DOI: 10.1093/jamiaopen/ooy019.
36. Page MJ, McKenzie JE, Bossuyt PM, et al. The PRISMA 2020 statement: an updated guideline for reporting systematic reviews. *Bmj* 2021; 372: n71. DOI: 10.1136/bmj.n71.
37. Tricco AC, Lillie E, Zarin W, et al. PRISMA extension for scoping reviews (PRISMA-ScR): checklist and explanation. *Ann Intern Med* 2018; 169: 467–473. DOI: 10.7326/M18-0850.

38. Holen RE, Thygesen E, Eikebrokk TR, et al. Barriers to exchanging healthcare information in inter-municipal healthcare services: a qualitative case study. *BMC Med Inf Decis Making* 2018; 18: 92. DOI: 10.1186/s12911-018-0701-z.
39. Ma CC, Kuo KM and Alexander JW. A survey-based study of factors that motivate nurses to protect the privacy of electronic medical records. *BMC Med Inform Decis Mak* 2016; 16: 13. DOI: 10.1186/s12911-016-0254-y.
40. Angst CM and Agarwal R. Digital health records and privacy concerns: overcoming key barriers to adoption. In: *ICIS 2006 Proceedings - Twenty Seventh International Conference on Information Systems*, 2006, pp. 1331–1340.
41. Angst CM and Agarwal R. Adoption of electronic health records in the presence of privacy concerns: the elaboration likelihood modeland individual persuasion. *MIS Q: Manag Inf Syst* 2009; 33: 339–370. DOI: 10.2307/20650295.
42. Johnston AC and Warkentin M. Information privacy compliance in the healthcare industry. *Inf Manag Comput Secur* 2008; 16: 5–19. DOI: 10.1108/09685220810862715.
43. Altamimi S, Storer T and Alzahrani A. The role of neutralisation techniques in violating hospitals privacy policies in Saudi Arabia. In: *2018 4TH Internnational Conference on Information Management (ICIM2018)*. Piscataway: IEEE, 2018, pp. 133–140.
44. Entzeridou E, Markopoulou E and Mollaki V. Public and physician's expectations and ethical concerns about electronic health record: benefits outweigh risks except for information security. *Int J Med Inform* 2018; 110: 98–107. DOI: 10.1016/j.ijmedinf.2017.12.004.
45. Foth M, Schusterschitz C and Flatscher-Thöni M. Technology acceptance as an influencing factor of hospital employees' compliance with data-protection standards in Germany. *J Public Health* 2012; 20: 253–268. DOI: 10.1007/s10389-011-0456-9.
46. Kuo KM, Chen YC, Talley PC, et al. Continuance compliance of privacy policy of electronic medical records: the roles of both motivation and habit. *BMC Med Inform Decis Mak* 2018; 18: 135. DOI: 10.1186/s12911-018-0722-7.
47. Kuo KM, Talley PC, Hung MC, et al. A deterrence approach to regulate nurses' compliance with electronic medical records privacy policy. *J Med Syst* 2017; 41: 198. DOI: 10.1007/s10916-017-0833-1.
48. Lapke M, Garcia C and Henderson D. The disconnect between healthcare provider tasks and privacy requirements. *Health Policy and Technology* 2017; 6: 12–19. DOI: 10.1016/j.hlpt.2016.08.004.
49. Saito K, Shofer FS, Saberi P, et al. Health care personnel perception of the privacy of electronic health records. *J Occup Environ Med* 2017; 59: 535–538. DOI: 10.1097/JOM.0000000000001016.
50. Sher ML, Talley PC, Cheng TJ, et al. How can hospitals better protect the privacy of electronic medical records? Perspectives from staff members of health information management departments. *Health Inf Manag* 2017; 46: 87–95. DOI: 10.1177/1833358316671264.
51. Fernández-Alemán JL, Sánchez-Henarejos A, Toval A, et al. Analysis of health professional security behaviors in a real clinical setting: an empirical study. *Int J Med Inform* 2015; 84: 454–467. DOI: 10.1016/j.ijmedinf.2015.01.010.
52. Humaidi N and Balakrishnan V. Indirect effect of management support on users' compliance behaviour towards information security policies. *Health Inf Manag* 2018; 47: 17–27. DOI: 10.1177/1833358317700255.
53. Kessler SR, Pindek S, Kleinman G, et al. Information security climate and the assessment of information security risk among healthcare employees. *Health Informatics J* 2020; 26: 461–473. DOI: 10.1177/1460458219832048.
54. T Alanazi S, Anbar MA, A Ebad S, et al. Theory-based model and prediction analysis of information security compliance behavior in the Saudi healthcare sector. *Symmetry* 2020; 12: 1544. DOI: 10.3390/sym12091544.

55. Ozer O, Ozkan O and Budak F. The relationship between the nurses' perception of electronic health records and patient privacy. *Hosp Top* 2020; 98: 155–162. DOI: 10.1080/00185868.2020.1799729.
56. Kuo KM, Talley PC and Lin DYM. Hospital staff's adherence to information security policy: a quest for the antecedents of deterrence variables. *Inquiry* 2021; 58: 469580211029599. DOI: 10.1177/00469580211029599.
57. Lee E and Seomun G. Structural model of the healthcare information security behavior of nurses applying protection motivation theory. *Int J Environ Res Public Health* 2021; 18: 2084. DOI: 10.3390/ijerph18042084.
58. Sari PK, Handayani PW, Hidayanto AN, et al. Information security behavior in health information systems: a review of research trends and antecedent factors. In: *Healthcare*. Basel: MDPI, 2022, p. 2531.
59. Kim J, Park EH, Park YS, et al. Prosocial rule-breaking on health information security at healthcare organisations in South Korea. *Inf Syst J* 2022; 32: 164–191, Health & Mental Health Personnel Issues 3400. DOI: 10.1111/isj.12338.
60. Kang P, Kang J and Monsen KA. Nurse information security policy compliance, information competence, and information security attitudes predict information security behavior. CIN: computers, informatics. *Nursing* 2023; 41: 595–602. DOI: 10.1097/CIN.0000000000000981.
61. Taylor S and Todd PA. Understanding information technology usage: a test of competing models. *Inf Syst Res* 1995; 6: 144–176.
62. Ajzen I. The theory of planned behavior. *Organ Behav Hum Decis Process* 1991; 50: 179–211. DOI: 10.1016/0749-5978(91)90020-T.
63. Davis FD. Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Q* 1989; 13: 319–340. DOI: 10.2307/249008.
64. Munn Z, Peters MD, Stern C, et al. Systematic review or scoping review? Guidance for authors when choosing between a systematic or scoping review approach. *BMC Med Res Methodol* 2018; 18: 143.