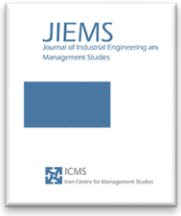
Vol. 11, No. 1, 2024, Pages 19-40

JIEMS
Journal of Industrial Engineering and Management Studies

journal homepage: www.jiems.icms.ac.ir



Human Error in Data Breaches of Electronic Health Records (EHR): A Systematic Literature Review

Wilmer Alvarado [1*], Konstantinos Triantis [1]

[1] Grado Department of Industrial and Systems Engineering, Virginia Polytechnic Institute and State University, Falls Church, VA, USA.

Received: Sep 2023-27/ Revised: Apr 2024-01/ Accepted: Apr 2024-10

Abstract

Human errors are a growing threat to EHR technology adoption and information sharing. Healthcare data breaches and criminal attacks continue to increase in volume and complexity. To achieve the full benefits of EHR technology, the industry must place the protection of health information as its highest priority. This paper presents the results of a systematic literature review of socio-technical system (STS) factors that influence human error in EHR data breaches. We present a conceptual framework of the STS factors that are hypothesized to reduce human error data breaches in the healthcare sector. The existing literature highlights a research gap in terms of understanding and modeling of human-computer interactions and the consideration of STS factors when developing solutions, signifying a need for further research in this domain. Hence, we recommend future research into the formulation and implementation of a STS approach to mitigate human error in information security, aiming to enhance the resilience of EHR and make them less attractive to cybercriminals.

Keywords: Healthcare Breaches, Cybersecurity Human Error, Information Security, Risk Methods, Socio-Technical Systems

Paper Type: Original Research

1. Introduction

This paper presents the results of a literature review of the STS factors that are believed to influence human errors in EHR data breaches, adoption and information sharing. EHR contain all or parts of patient's health information in a digital form. They are digital records that are intended to provide a complete picture of a patient's health record. A healthcare data breach occurs when an individual name plus a medical record is potentially put at risk because of exposure either through electronic or paper means (NIST, 2015; Rouached & Sallay, 2011; Hofmey, 1999). Human error is an unintended action that leads to unacceptable consequences. Although human error can lead to security breaches and present a barrier for EHR adoption and information sharing, the results of our literature review suggests that mitigation of human error should be considered in the system design and data security review efforts (Palabindala, Pamarthy, & Jonnalagadda, 2016).

1.1. Context: System Threat

The United States (U.S.) Healthcare Sector faces persistent and increasingly sophisticated malicious data breach attempts that threatens the EHR adoption and information sharing in the public and private sectors, and ultimately the patients' protected health information (PHI). The rise of cybersecurity incidents, EHR data breaches in particular, pose risks to the healthcare industry in general, and to hospitals especially (Callahan, 2013). The Health Insurance Portability and Accountability Act (HIPAA) Journal reported statistics showing that over the past 10 years there has been an increase in the data breaches reported in the healthcare sector. In 2021, HIPAA reported the highest number ever recorded with 715 data breaches where more than 500 records were compromised. The journal also published major changes in the determination of the root causes for the breaches reported (HIPAA, 2022).

*Corresponding Author: wilmera@dni.gov

1.2. System Improvements Needed: Research Hypothesis

The healthcare sector must improve its efforts to protect patients' information from cyber-attacks. The sector's cyber professionals must carefully examine what is currently occurring during major data breach incidents and apply lessons learned to make the infrastructure more resilient. However, this proposition is not as easy to implement as it sounds. The healthcare organizations are extraordinarily complex, with many typical extreme organizational characteristics that include a technology saturated environment, internal politics, regulatory pressures, and a patient-centered care (Smet, 1982). Given the complexity of healthcare organizations, protecting the information systems require more than robust technical design solutions, government policy, and action. It requires a deep change in the way the sector is approaching healthcare data security. As depicted in Figure 1, it is hypothesized in this paper, that STS factors are associated with the likelihood of human error in healthcare data breaches. Moreover, we argue that the implementation of STS principles to information security presents an opportunity to reduce human error and healthcare data breaches, increase EHR adoption and information sharing, and consequently improve the efficiency performance in the healthcare industry.

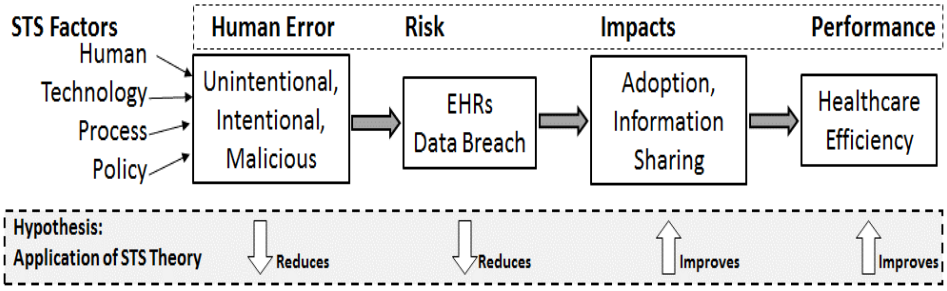


Figure 1. Process Flow of STS Factors Involved in Information Security of EHR

1.3. Literature Research Questions

The importance and impact of human error related data breaches to EHR adoption and information sharing, and the efficiency performance of healthcare units raise critical questions:

a) Are STS factors associated with the likelihood of human error in healthcare data breaches?

b) What are the sources of human error that cause data breach incidents?

c) Do human driven data breaches impact the EHR adoption and information sharing?

d) How does EHR adoption and information sharing impact the effectiveness and efficiency performance of the healthcare sector?

e) Is there a research data limitation in the literature?

f) Are there any gaps in literature that need further study to expand the knowledge in the field?

To answer these questions, we conducted a systematic literature review to get an in-depth understanding of these topics. We created a conceptual framework that highlights STS factors that cause human error in data breaches; developed a taxonomy of human errors causing data breaches incidents; proposed a research hypothesis model of STS factors hypothesized to reduce human error driven data breaches, increase EHR adoption and information sharing, and improve the effectiveness and efficiency performance of the healthcare sector; highlighted limitations of the literature reviewed; and, identified research that needs further study to expand the knowledge of the field.

1.4. Research Paper Findings and Contributions

In this paper, we conduct a systematic literature review associated with cyber risk and data breaches in the healthcare sector (Sardi, Rizzi, Sorano, & Guerrieri, 2020). The paper makes several contributions to the information security and STS literature. First, it illustrates that very few studies have been performed to address the implications of EHR human error on data breaches. Second, it identifies the lack of attention by the international research community about the subject and its implications to the EHR adoption and information sharing. Third, it recognizes that robust technical design solutions and government policy are not enough. Fourth, it identifies gaps in the literature, such as the application of a systems thinking approach in the cybersecurity domain. Fifth, the paper

presents a conceptual framework that illustrates the STS factors that drive human error in information security. Sixth and finally, the paper presents a qualitative causal loop model that illustrates the interrelationships of these STS factors. The work in this paper was motivated by the fact that an understanding of the human error causes in healthcare data breaches can lead to developing an actionable strategy and security governance to prevent the proliferation of breaches and barriers to EHR adoption and information sharing across the healthcare sector (Khan, Kim, Mathiassen, & Moore, 2019). Thus, one of the objectives of this paper is to leverage the Reason's Theoretical Model of Accident Causation (Perneger, 2005) to address the person approach and the system approach to human error as platforms to understand the role of human performance in information security of patient's health data.

1.5. Paper Organization

The paper is organized using a section format. Section 2 presents a summary of the healthcare sector and a background of the vulnerability of EHR to cybercriminals. Section 3.0 presents the literature review approach. Section 4.0 introduces the materials and methods used in the literature review and the process used to down select the relevant articles used in the paper. The scope of Section 5.0 is to provide the main outcomes and also outline findings from the literature review. In Section 6.0, we discuss the results, present a conceptual framework of causes of human error, and propose a conceptual model with factors hypothesized to reduce human driven data breaches that potentially increase efficiency performance in the healthcare sector. The final section of the paper provides the conclusions and references.

2. Background

The efficiency performance of the U.S. Healthcare System is a primary concern to government and industry leaders. The U.S. has probably the best healthcare infrastructure and most specialized healthcare providers than any other country (Schoen, Davis, How, & Schoenbaum, 2006). The Centers of Medicare and Medicaid Services estimated that the U.S. health spending in 2021 was estimated at 18 percent of its gross domestic product (GDP), double the median of industrialized countries. Even when the healthcare cost in the U.S. since 2000 has been growing more rapidly than before (Schoen, Davis, How, & Schoenbaum, 2006; Morgan, 2021). The U.S. healthcare sector is not the leader in information technology, and does not provide the best quality of care services to its patients (Schoen, Davis, How, & Schoenbaum, 2006). Government policy coupled with advances in information technology have helped the healthcare industry to digitize patient's records to provide more efficient and cost-effective services to the public. EHR enhance patient care. The convenience of having digital records accessible at all time can streamline healthcare process workflows, and increase productivity by improving healthcare providers to patients and providers to providers' interactions (HIPAA, 2021). EHR are seen by the government and many experts in the field as the transformation technology that the sector needs to improve its efficiency and lower the cost of healthcare services to patients.

2.1. Vulnerability of HER

The healthcare industry has become the main target for cybercriminals with four out five data breach incidents occurring in the sector. Data breaches are not just a concern for chief information officers and security experts; due to the sensitivity of patient's health records, they also affect the healthcare sector as a whole, the confidentiality of patients' PHI, and have become a barrier to a widespread EHR adoption and information sharing. Although there are different types of data breaches reported, their impact always results in financial losses and healthcare reputation implications (Seh, Zarour, Alenesi, Sarkar, Agrawal, Kuman, & Ahmad, (2020); Gesulgaa, Berjameb, Moquialac, & Galidod, 2018). Health information from EHR are more valuable than just credit cards information or financial data alone. Figure 2 and according to the Department of Health and Human Services (DHHS) health IT.gov (HIPAA, 2021), the data in the EHR contains: patient demographic, insurance and financial data, medical history, and information about the patients' healthcare providers. The loss of these data to unauthorized users can lead to a complete identity theft. EHR are an important tool to improve the efficiency performance and lower the cost of the healthcare sector (Yasnoff, 2016). So, better quality in healthcare service starts with healthcare providers' commitment to place the protection of health information as their highest priority (Ouksel & Lundquist, 2012).

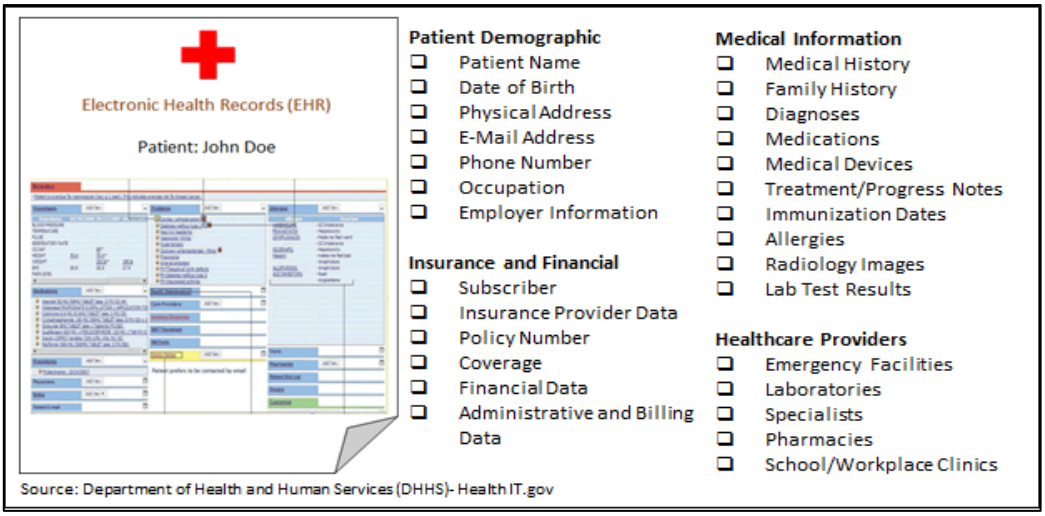


Figure 2. Patients' PHI Included in HER

The literature from the DHHS' Office of Civil Rights of 2022 (HIPAA, 2022) reports healthcare data breaches of 500 or more records (Figure 3) from 2009 to 2022. These breaches in the healthcare sector have led to the compromise, exposure, and loss of 381,761,286 patients' records, an amount roughly about 15% higher than the population of the U.S.

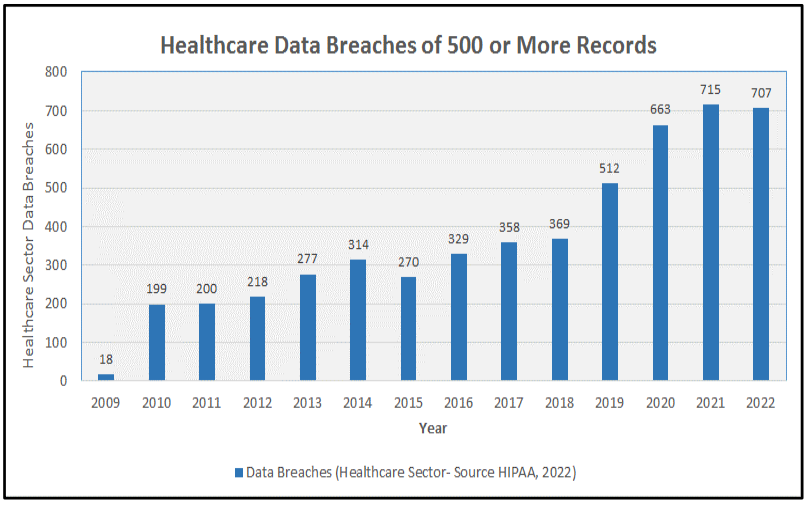


Figure 3. HIPAA Reported Data Breaches in the Healthcare Sector (HIPAA, 2022)

From 2018 to the end of 2022, the reported data breaches (500 or more records) jumped from an average of 1 to 1.92 per day (HIPAA, 2022) (Figure 3). Healthcare providers accounted for 73% of the breaches followed by Business Associates with 14% and Health Plans with 13% (HIPAA, 2022). The growth in data breaches in the sector seems to be driven by an increase in EHR adoption and their information sharing among healthcare organizations over the past several years, and the attractiveness of these data to cyber criminals. It is presumed that while healthcare systems have digitized to keep up, the healthcare sector has not dynamically implemented trusted digital identity access management (IAM) solutions at the same pace, leading to vulnerabilities in the EHR systems.According to an IBM study conducted in 2022, a data breach costs the healthcare sector an average of $10.1 million1 including fines, litigations, and damage of reputation (Ponemon Institute, 2022). It is calculated to be more than 70 percent higher than all other sectors. The report also indicates that it takes 327 days to detect and contain a data breach where credentials are compromised, such as in the healthcare sector. This is about 18% longer than the average of all industries (Ponemon Institute, 2022).

[1] IBM estimated cost of a data breach in 2022 increased from $7.13 in 2020 to $10.1M, a 42% increase in the past two years.

2.2. Human Error on Data Breaches

Spending in cybersecurity in the U.S. in the last decade exceeded $500 billion (Statista, 2021). Furthermore, it is expected to continue its ascending trend as cybersecurity has become the fastest growing crime in the U.S. The healthcare sector has been particularly vulnerable and targeted by cyberattacks because they possess so much information of high value in the black market. As reported by many Healthcare Practitioners, Business Associates and Health Plans, since 2005 in the U.S. alone, over 380 million individuals were affected by healthcare data breaches, with basic human error as the root of more than one-fourth of these breaches. Figure 4 presents a summary of the three major categories of root causes associated with healthcare data breaches reported in an IBM Security report published in 2020. Fifty percent of incidents involved a malicious attack, compared to 27% caused by human error, and 23% by system glitches. Only the entertainment, public, and consumer industries had higher percentages of data breaches caused by human error compared to the healthcare industry.

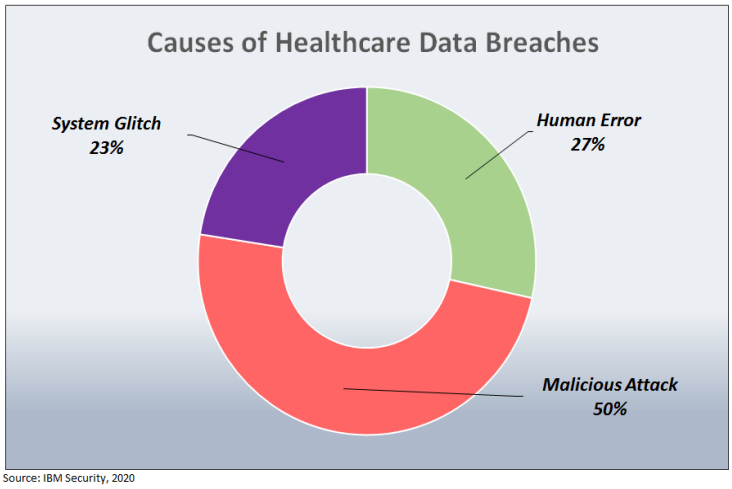


Figure 4. Causes of Data Breaches in the Healthcare Sector

It is recognized in the literature that technology alone cannot deliver a complete EHR system security solution. There is also a tangible need to address user awareness and insider threat aspects in the industry. One of the greatest challenges that the healthcare sector faces today is the lack of user awareness and the unintentional, intentional, and malicious actions of employees and healthcare stakeholders with daily access to EHR and the organization information resources (Warkentin, Millison, 2009; Warketin, & Millison, 2013; Pfleeger & Caputo, 2012).

2.3. Government Policy

In 2022, the HIPAA Journal reported statistics showing that over the past 10 years there has been an increase in the data breaches reported in the healthcare sector. HIPAA highlighted that in 2021 alone, 715 data breach events with more than 500 records per event were compromised, recording the highest ever event since breached records started being published. The HIPAA publication also reported notable changes in the determination of the main causes of the breaches (HIPAA, 2022). The loss/theft of healthcare records and electronic protected health information dominated the breach reports between 2009 and 2015. Better policies and procedures and the use of encryption has helped reduce these easily preventable breaches (HIPAA, 2022). In today's DNA, data breach events are common across numerous sectors of the economy. Cybersecurity concerns are not unique to the healthcare industry. However, coordinated efforts among healthcare providers to protect records and information systems have been slower and lacking in comparison with other sectors in the economy (Whitworth, 2009; Callahan, 2013).From the government regulation perspective, the 1996 HIPAA Policy and subsequent amendments (2004 Privacy Rule Provisions, 2005 Security Rule, 2009 Breach Notification Rule, and 2013 Omnibus Rule) have established protocols for prevention, protection, detection, remediation, and publication of patients' health information. Continuous enforcement of the policy and amendment rules should be a top priority for the healthcare sector since this is essential to improve industry efficiency. Compliance with HIPAA regulations and implementation of secure data protection solutions is an alternative to improve the organization's odds to make EHR less attractive to cybercriminals.

2.4. Information Sharing

Preventing errors in the management and maintenance of EHR is very difficult. All organizations that store, process, share, and manage data are a target for cybercriminals. To enable an effective EHR system, healthcare organizations have to exchange information within internal and external devices and platforms, among multiple healthcare units, and ideally between hospital systems nation-wide and with their international parent organizations (Beitollahi & Deconinck, 2012). This level of information sharing and interaction increases the information security risk by exposing system's vulnerabilities, thus broadening the information landscape for insiders and malicious cyber actors. To make things more challenging, the healthcare industry has traditionally been slower than other industries adopting safety measures for protecting its information technology platforms (Ponemon Institute, 2022). Many cybersecurity vulnerabilities in the health ecosystem are the results of the huge number of medical devices connected to healthcare networks. Information technology advances, such as EHR adoption, have enabled improvements in healthcare delivery that have translated in efficiencies in patient care (Palabindala, Pamarthy, & Jonnalagadda, 2016). An information sharing network includes components of health systems. For example, Health System A includes hospitals, family practices, primary care, research center, clinics/urgent care, cloud services, physical therapy centers, and health partners among others. When information is exchanged between the units of the Healthcare System A and across other healthcare systems within the sector, it creates an information sharing network ecosystem. This ecosystem that includes clinical and medical devices interconnected within each other, leaves these devices vulnerable and increases the landscape for potential cybercriminal attacks. This vulnerability is a cause of common concern in the healthcare sector, as an unauthorized access to these medical devices could have a direct and adverse impact on the clinical care and patient's safety, and could lead to compromising the security of health records (Williams & Woodward, 2020).

3. Literature Review Process

Literature reviews provide the basis for developing the foundational background in the specific area of research, and necessary to justify the research questions, hypothesis, and if well conducted, the literature has the capacity for landing new ideas and creative ideas in any particular field of research (Snyder, 2019; Torraco, 2005). It can also generate the "theoretical framework," to further advance the research in the field of study (Transfield, Denyer, & Smart, 2003). Selecting the literature review approach is critical to maximize the benefits of the publications review. Based on the literature information from Snyder 2019, we evaluated three types of review methodologies: systematic; semi-systematic; and, integrative approaches; for selecting the "best fit" approach to generate this research paper (Snyder, 2019). Systematic Review: In a systematic review the objective is to identify all empirical evidence that fits the criteria to develop answers to pre-established research questions and hypotheses (Moher, Liberati, Tetzlaff, & Altman, 2009). This type of review is effective for dissecting previous literature articles and to understand their content and what they're showing to respond to particular questions and to provide evidence that can be used to support policy development or practical approaches (Sardi, Rizzi, Sorano, & Guerrieri, 2020). Semi-Systematic Review: The type of subject suitable for a semi-systematic approach involve topics that have been previously studied by numerous researchers from various fields making a systematic literature review process too laborious or too long to complete and achieve its objective (Wong, Greenhalgh, Westhorp, Buckingham, & Pawson, 2013). A semi-systematic review often looks at progress achieved over time in a particular research area or how a topic has developed across research efforts (Snyder, 2019). Integrative Review: This type of review evaluates the literature and break down a specific topic to enable the development of new perspectives or theoretical frameworks (Torres-Tomas, Spolaora, Alvarez-Chermana, & Mona, 2014). It is more appropriate for new topics or to address well known or mature subjects.

3.1. Systematic Literature Review- Methodology Selection

After evaluating the different literature review approaches, we concluded that a systematic literature review was the most appropriate approach to review the searched publications. Systematic reviews have been broadly used in medical and healthcare related research, and have been referred to as the "gold standard" among reviews (Davis, Kurti, Skelly, Redner, White, & Higgins, 2014). This approach was selected because the goal of this study was to identify all empirical evidence, while minimizing bias or speculations based on expert knowledge in the field or common beliefs about what is generally accepted, and to identify the most impactful findings from which results and recommendations about the STS factors influencing human error in data breaches and EHR adoption and information sharing can be reached (Armitage, & Keeble-Ramsay, 2009), Snyder, 2019). Although there are many approaches to carry out a systematic review, we adopted the Transfield approach (Transfield, Denyer, & Smart, 2003) because it is one of the most recognized in the management literature, with more than 8,000 citations on Google Scholar and Web of Science, and has been tested and validated by the research community (Sardi, Rizzi, Sorano, & Guerrieri, 2020). The approach (adapted from Transfield) suggests the following steps for conducting a rigorous review:

Step 1: Planning the Review
- Planning the systematic literature review and identifying keywords

Step 2: Conducting a Review
- Defining the criteria of document selection
- Classifying the information
- Extracting the relevant documents

Step 3: Reporting and Dissemination
- Discussion and validity of results

These three steps are further developed and the findings are presented in the Materials and Methods, Results, and Discussion sections of this paper.

3.2. Literature Sources

This paper intends to provide the key research themes about human error in data breaches and data privacy and the application of STS principles to expand the knowledge in the healthcare information technology field. To ensure consistency in the publications search, the paper leveraged information from electronic web search engines including Google Scholar, and the electronic libraries from the National Institute of Health (NIH), Virginia Polytechnic Institute and State University, the University of Southern California, and the George Mason University. Other sources included industry's company websites and reports, Federal Government literature from the Department of Commerce's National Institute Standards and Technology, DHSS, and statistics about healthcare data breaches from the HIPAA Journal. Articles from various medical science magazines were also used to explore the different aspects of the literature and the viewpoints from healthcare experts in the field. The literature sources for all these publications included peer reviewed journals and university research papers from the following databases: Academic Press, American Medical Association, Cross-Mark, De Gruyter, Scopus Elsevier, Institute of Electrical and Electronic Engineers (IEEE), NIH, Journal Storage (JSTOR), Oxford University Press, Research Gate, Springer, and the Taylor & Francis Group among others.

4. Materials and Methods

The systematic literature review and the final selection of articles is aimed to identify STS factors influencing human error in data breaches of EHR. The review was based on literature identified from multiple datasets and web-based resources. Following Sardi and Rizzi et al. (Sardi, Rizzi, Sorano, & Guerrieri, 2020), Snyder (Snyder, 2019), and Katharakisa et al. (Katharakisa, Katharakib, & Katostaras, 2013) previous works and by adopting the Transfield's systematic review guidelines summarized in Steps 1 thru 3 below, 40 articles out of 1,071 initial searches were included in the review.

4.1. Step 1: Planning the Review

Planning the systematic literature review and identifying search and keywords. To plan this review, we leveraged 11 previous systematic literature review journal papers performed in the field of healthcare. Three of the journal papers came from information security experts in the field that address cyber risks and human factors in healthcare systems (Sardi, Rizzi, Sorano, & Guerrieri, 2020; Nifakos, Chandramouli, Nikolaou, Papachristou, Koch, Panaousis, & Bonacina, 2021; Franke & Brynielson, 2014). The other five journal papers were related to measuring efficiency and addressing managerial challenges in healthcare systems (Moher, Liberati, Tetzlaff, & Altman, 2009; Davis, Kurti, Skelly, Redner, White, & Higgins, 2014; Katharakisa, Katharakib, & Katostaras, 2013; Crema & Verbano, 2013; Menear, Dore, Clouthier, Perrier, Roberge, Duhoux, Houle, & Fournier, 2014). From the process standpoint, the planning stage was supplemented by three journal papers on the methods to conduct a systematic literature review (Armitage, & Keeble-Ramsay, 2009; Transfield, Denyer, & Smart, 2003; Keathly-Herring, Van Aken, Gonzalez-Aleu, Deschamps, Letens, & Cardenas, 2016). The planning stage was also informed by consulting a healthcare professional responsible for developing tools for mining information from EHR, and multiple interviews with cyber-security professionals developing IAM systems to protect national defense networks and systems data from cyber-intrusions. Informed by the literature, EHR professionals, and cybersecurity experts, we identified the search and keywords needed for exploiting publications for the literature review. The keywords identified for the review are listed in Table 1.

	Keywords				
Linked Keywords	***Computer Security***	***Cybersecurity***	***Data Breaches***	***Data Envelopment Analysis***	***Electronic Health Records***
	Cyber Security	Cyber Risks	Data Breaches	Hospital Efficiency	Electronic Health Records
	Ethics	Cyber Attacks	Redundancy	E-Health	Patients Health Information
	Network Security	Zero Trust Architecture	Healthcare	Efficiency	HIPAA Policy
	Computer Science	Identity Access Management	Information Security Policy	Health IT	Electronic Medical Records
Linked Keywords	***Healthcare***	***Human Errors***	***Methods***	***Risk***	***Social Technical Systems***
	Health	Human Errors	Literature Review	Risk Management	System Thinking
	Healthcare Sector	Internal Threat	Resiliency	Risk Assessment	Socio Technical Theory
	Healthcare Facilities	User Awareness	Framework	Risk Evaluation	Accident Analysis
	Medical IT	Human Mistakes	Reliability Theory		System Dynamics
	Security of Health Data		Control Theory		Human Relations
			Economic Production		Organizational Change
					Safety Incidents

Table 1. Keywords Used to Search Publications for the Literature Review.

4.2. Step 2: Conducting a Review

Defining the criteria of document selection. We chose a combination of peer-reviewed journal articles, university research papers, and articles from government and private industry from multiple databases including Scopus Elsevier, IEEE, NIH, JSTOR, Research Gate, and Pergamon Press. The criteria for the document selection are listed in Table 2.

	Research Criteria		
Dataset Source	Academic Press	Scopus-Elsevier	HeinOnline
	IEEE	JSTOR	National Institute of Health
	Pergamon Press	Research Gate	University Research
Timeframe		From 1926 to 2022	
Document Type Reviewed	Journal	University Research	Government Articles
	Handbooks	News/Magazine Articles	Private Industry Research
Search Words	Computer Security and Cybersecurity	Electronic Health Records	Methods
	Data Breaches	Healthcare	Risks
	Data Envelopment Analysis	Human Errors	Social Technical Systems
Subject Areas	Communications	Information Systems	Safety and Risk Analysis
	Economics	Management Science	Science
	History	Modeling	Technology and Engineering
	Human and Social Factors	Operations	Theory and Policy
Analysis Criteria		Qualitative vs. Quantitative	
Selection Criteria	Title and Language	Abstract Review	Full Text Review

Table 2. Topics Used for Defining the Research Criteria of the Document Selection.

Classifying the Information. To conduct the assessment and synthesis of the documents extracted from the literature, we created a Microsoft excel spreadsheet and logged all the 1,071 documents from the initial search. The excel sheet facilitated management and analysis for informing the down select of the relevant publications for the research. Given the high volume of documents, we also added excel pivot tables that enabled the characterization and accurate quantification of the documents by the multiple categories and publications' trends (e.g., year of publications, countries of origin, etc.). In the next section, the information obtained in the literature was classified by publications' trend. Table 3 presents all the publications obtained from the literature classified by subject areas and keywords. Table 4 presents the document type such as journals and research papers obtained by keywords. The description used to classify the documents by type is provided for reference. The publications' trend presented in Figure 5 shows that the documents reviewed in the literature spanned from 1926 to 2022.

	Keywords										
Subject Area	**Computer Security**	**Cybersecurity**	**Data Breaches**	**DEA**	**EHRs**	**Healthcare**	**Human Errors**	**Methods**	**Risk**	**STS**	**Total**
Communications	37	0	3	0	6	0	10	0	1	6	63
Economics	0	0	2	0	0	2	0	1	0	0	5
History	0	0	0	0	0	4	0	0	0	0	4
Human and Social Factors	6	11	12	9	75	96	23	7	21	33	293
Information Systems	37	99	43	0	50	26	22	7	1	10	295
Management Science	6	4	22	0	8	10	6	10	3	8	77
Modeling	3	5	5	0	9	9	6	2	0	9	48
Operations	6	3	6	0	2	2	12	0	1	9	41
Safety and Risk Analysis	1	12	5	0	8	2	12	4	18	8	70
Science	38	0	0	0	0	5	1	0	3	0	47
Technology & Engineering	5	2	0	0	0	1	13	1	3	11	36
Theory and Policy	8	17	26	0	3	3	1	22	2	10	92
Total	**147**	**153**	**124**	**9**	**161**	**160**	**106**	**54**	**53**	**104**	**1071**

Table 3. Publications' Trend- By Keywords and Subject Area

	Keywords									
Document Type	Computer Security	Cybersecurity	Data Breaches	DEA	EHRs	Healthcare	Human Errors	Methods	Risk	STS	Total
Articles	5	13	5		7	66	2	5	18	1	122
Books / Handbooks	6	14	3			18	3	6	1	9	60
Doctoral Theses	2	4	1	1	1			1		2	12
Journals	104	34	71	6	110	37	90	15	11	84	562
Notes and Links	1	1				1					3
Research Papers	29	87	44	2	43	38	11	27	23	8	312
Total	147	153	124	9	161	160	106	54	53	104	1071

Table 4. Publications' Trend- By Keywords and Document Type

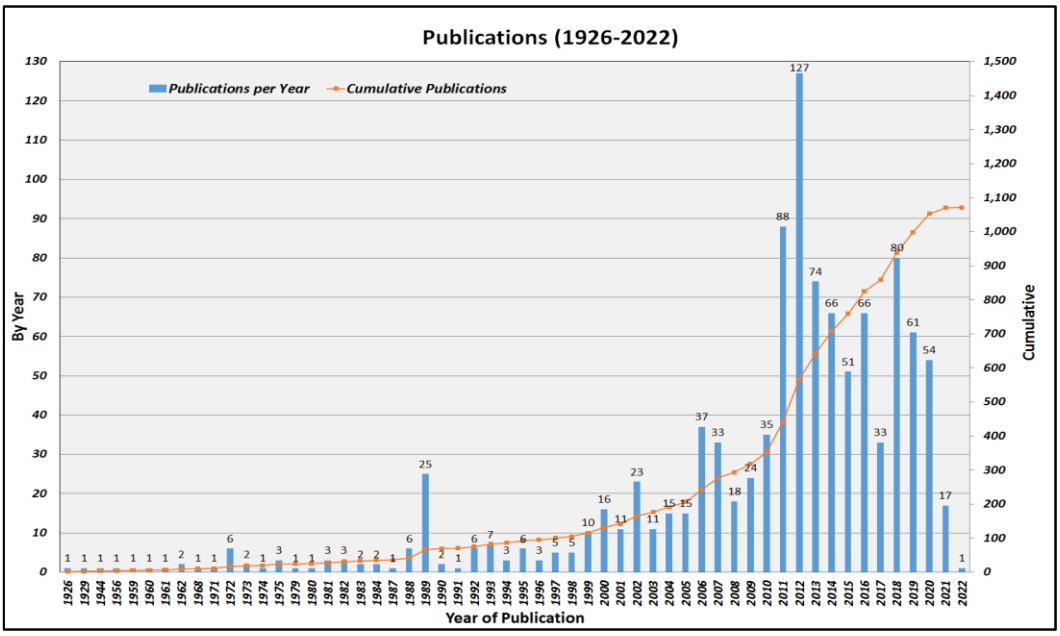


Figure 5. Publications' Trend- Documents by Year of Publication. Initial Search Included Documents from 1926-2022.

The descriptions used to categorize each publication from Table 4, among articles, books/handbooks, doctoral theses, journals, notes and links are presented in the bullets below.

- Articles: Writings from a particular topic included in newspapers, magazines, websites, blogs, and/or journal publications.
- Books / Handbooks: This category includes books or sections of a book. It also includes publications that are organized as guidelines and/or policy for a certain field of knowledge.
- Doctoral Theses: Published work by a student focused on original research performed to obtain a PhD.
- Journals: Includes scholarly papers about a subject in a specific field of study that have been researched or reviewed and written by an expert in the field. Papers in this category were published in a major journal.
- Notes and Links: This category includes discussion notes and internet articles about a specific research area. They are not full academic papers.
- Research Papers: Publications in this category come from university research, and/or research from an independent organization or business unit. These publications analyze a perspective or argue a point.

Extracting the relevant documents. After all documents were retrieved from the multiple data sources and categorized by year of publication and by publication type, the following inclusion criteria were used to identify the papers included in the literature review:

- Publications relevant to cyber security threats to the healthcare sector.
- Articles that report on STS factors associated with cyber security management.
- Articles that report on data breaches occurring in hospitals and other healthcare organizations.
- Publications that report human, technical, and organizational factors that drive human error in the healthcare sector.
- Publications that address barriers and solutions for EHR adoption and information sharing.
- Articles that identify vulnerabilities of the healthcare information technology infrastructure.
- Publications relevant to policy and system capabilities aimed at protecting patients' PHI.

The following exclusion criteria were used to filter out irrelevant publications from the study:

- Duplicates and repeated publications.
- Articles that by their titles were found irrelevant to the research questions or hypothesis.
- Documents that were not written in English.
- Publications that were not related nor had any implications for the healthcare sector environment.
- Articles that were focused primarily on technical developments (e.g., algorithms, software) and failed to address their implications to data breaches, EHR, or involvement of human in the loop-healthcare professionals.

How were the relevant documents extracted? After all documents were collected, we conducted an evaluation of them to decide which documents were relevant to inform the aim of the literature review. First, we removed 157 publications because they were not written in English or because the title of the document was found irrelevant to the questions and hypothesis of this study. Second, we rejected 16 documents that were duplicates or repeated. After studying the abstract of the remaining 898 documents and based on the inclusion and exclusion criteria, we rejected 626 articles that were not related to data breaches, or did not have any implications for the healthcare sector environment, or were incomplete. The review of the document abstracts enabled us to eliminate documents that were published prior to the introduction of the 1996 HIPAA Privacy Protection Act as they were found to be out of date and irrelevant to the aim of the paper. Consequently, we selected 272 publications for studying the full text. In the next step, we read the full text of these 272 publications and selected 70 documents useful to inform the aim of the study. Finally, after conducting an in-depth evaluation of the 70 documents, we only selected 40 publications. This final selection was limited to articles that specifically addressed the three main aspects of this study: STS factors influencing human error in data breaches and EHR adoption.

4.3. Step 3: Reporting and dissemination

Discussion and validity of results. We analyzed the findings and developed a conceptual framework of the STS factors that drive human error in data breaches. The inclusion criteria provided the basis for the literature search where the 'human error on data breaches' within the title, abstract, and body of the publications were used to select the relevant documents for the study. This gave a better foundation to filter out unrelated articles to our study's main objective. The information systems, human and social factors, safety and risk analysis, and management science were key focus subject areas to relate the publications to data breaches and data privacy in healthcare from a management perspective. The document exclusion criteria ensured current reality of what is happening in the dynamic information security environment and the implications that protection of data privacy is having in the adoption and information sharing of EHR. For example, after reviewing the abstracts, publications before 1996 were deemed out of date due to the introduction of new policy such as the 1996 HIPAA privacy protection act, new technologies and digital modernization introduced in the healthcare sector in the new millennium, and the different developments within data privacy and data breaches. In addition, blogs, magazines, unreliable websites and newspaper sources were all disregarded. The disciplined approach employed for evaluating and down selecting the relevant documents provides high confidence in the validity of the research process and the results. This process was based on a clear keyword selection criterion and the collection of a broad list of reference publications. The Transfield literature approach reinforced the credibility of the research process and the results. This approach is one of the most recognized in the management literature because it has been tested and validated by the research community. Thus, the attributes of this systematic literature review approach are summarized as follows: (a) transparent, clearly describes the selection criteria; (b) reproducible, based on methodical user friendly and easy to follow process; (c) quantitative, leveraged statistics collected on multiple criteria used to characterize the content of the literature; (d) unbiased, followed a discipline process for selecting relevant documentation to inform the study; and (e) international, included documents from international databases with papers from more than 70 countries to make available a wide perspective of the topic area to reviewers (Sardi, Rizzi, Sorano, & Guerrieri, 2020).

5. Results

5.1. Main Findings- Quantitative Analysis of Publications' Trend

The total number of documents identified by the keywords searched from multiple publishing sources was 1,071. Figure 6 presents the step-by-step process used for evaluating the publications and to arrive to the papers that were found to be relevant for providing responses to the research questions. The document search spanned from publications made as early as 1926, for method papers related to the economic production theory, and the latest from 2022 with the HIPAA Journal' statistics about number of data breaches per year and number of records that were compromised. The down select literature approach selected 40 relevant documents. The selection of the papers was made starting with all the publications gathered through the database searches. The country with the major contribution of published papers was the U.S. with 68% of the documents followed by England with about 10%. The majority of the publications were journals and university research with over 25% of all documents from Scopus Elsevier.

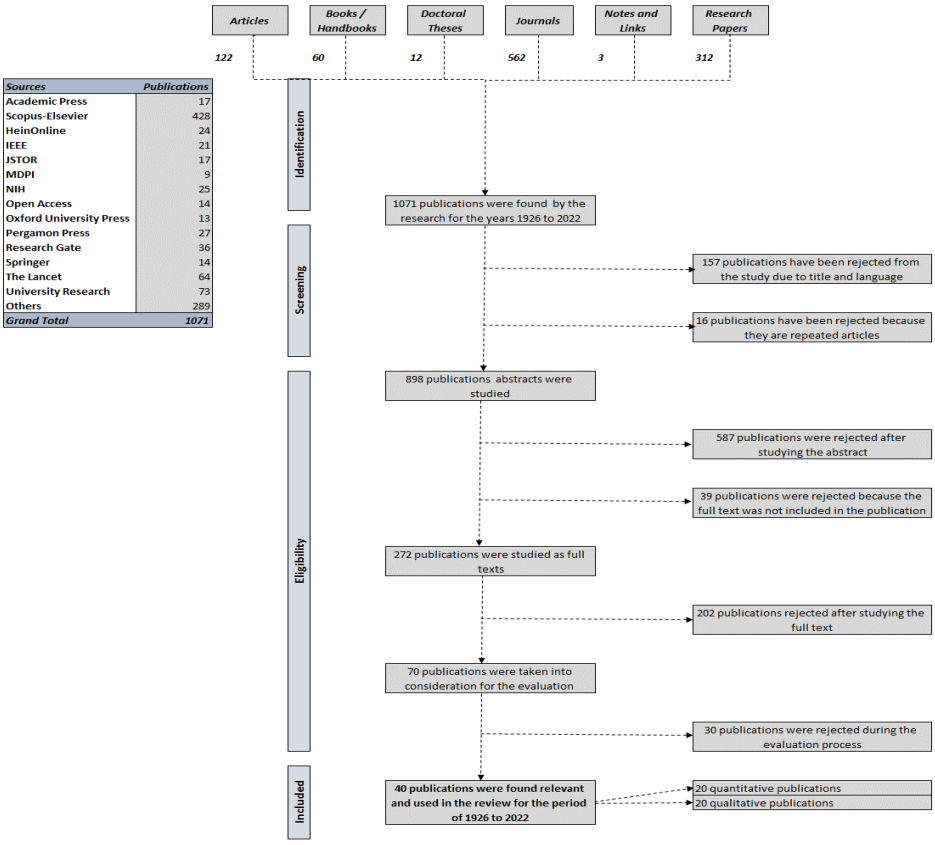


Figure 6. Flow Chart of the Process Selection of Relevant Documents[2]

The first group of results describes the publications' trend on human error in EHR data breaches. The assessment performed of the publications' trend is a quantitative analysis. It illustrates multi-criteria set of metrics gathered to assess the content of the selected relevant documents. Figures 7 through 10 present the distribution of the relevant documents and a brief analysis of the results broken down by keywords, subject areas, publications by year, publications by country, and a literature methodological information. Consistent with the aim of this study, the most keywords on the final selection of relevant documents as illustrated in Figure 7 come from healthcare (9, 23%); cybersecurity (8, 20%); electronic health records (7, 18%); human error (7, 18%); and last but not least, data breaches (3, 7%). Given the specific selection criteria and the lesser number of documents addressing the healthcare sector, data envelopment analysis (0), risk (1, 3%), computer security (1, 3%), and methods (1, 3%) received a lower consideration in the final selection. Another significant publications' trend reviewed in the literature was "subject area." In Figure 7, results from the literature show that the information systems (22, 55% of documents), human and social factors (10, 25%), safety and risk analysis (5, 13%), and management science (3, 7%) received the most consideration in the final document selection.

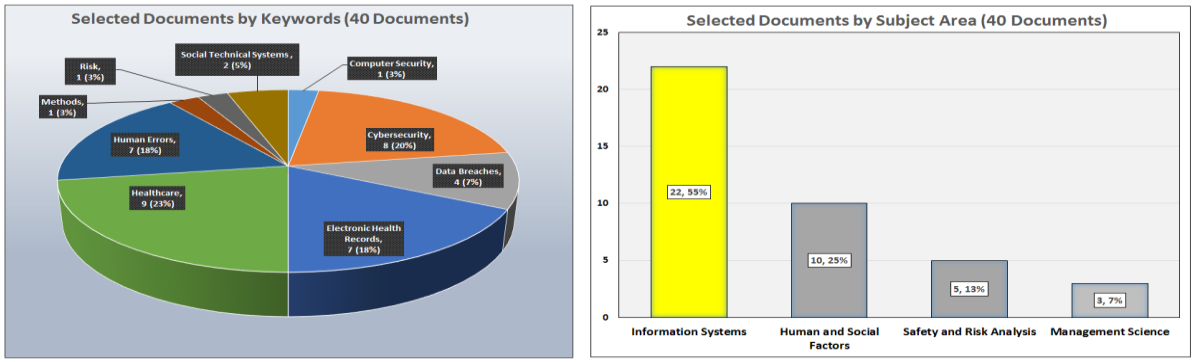


Figure 7. Publications' Trend Taxonomy – Selected Documents by Publication Keywords and Subject Area

[2] Quantitative publications are based on empirical observations where analytical quantitative evaluations, including statistical analysis of historical data and testing of hypotheses, were presented. Meanwhile, Qualitative publications were based on methods where the authors conducted surveys and developed conceptual models to influence future research and policy development.

Figure 8 presents another analysis conducted on the publications' trend. This trend indicates that 2020 was the year with the greatest number of relevant documents (6 articles). The 2011-2021 decade witnessed a significant growth in publications related to healthcare data breaches. This result is consistent with recent reports from the HIPAA Journal where the healthcare sector is reporting a continuing increase in the number of data breaches with most events compromising the privacy of more than 500 patient records per data breach incident. This metric is also consistent with the total number of published reports in the last two decades where the number of publications has doubled since 2010.

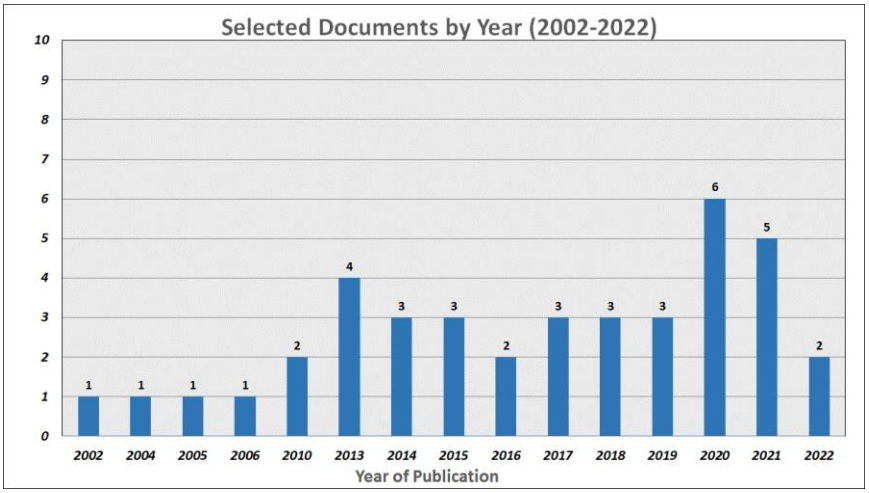


Figure 8. Publications' Trend---Highest Number of Selected Documents Were Published in 2020.

In Figure 9, the publications' trend by country illustrates that the most prolific country performing research in the field is the U.S. (27, 68% of documents). The U.S. is considered by far the top country in research development and most notably research related to the associated risks of information security. It is also worth to note that the U.S. also accounted for about 45% or 538 publications of the total 1,071 searched in this study. After the U.S. the following country with the most relevant publications was England (4, 10%). The remaining nine countries with relevant publications only contributed one document per country.

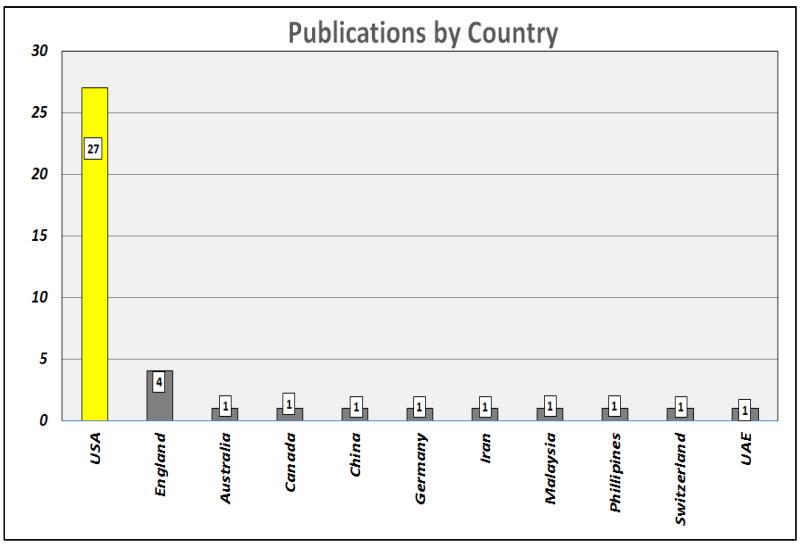


Figure 9. Publications' Trend--- Most Publications Selected Were Published by the U.S.

Finally, the last analysis performed about the publications' trend, Figure 10, presents an assessment of the literature methodological information. In this trend analysis, the metrics illustrate that of the 40 documents selected, 20 publications were based on empirical observations where analytical quantitative evaluations, including statistical analysis of historical data and testing of hypotheses, were presented. This trend also includes 20 publications that used qualitative methods where the authors conducted surveys and developed conceptual models to influence future research and policy development.

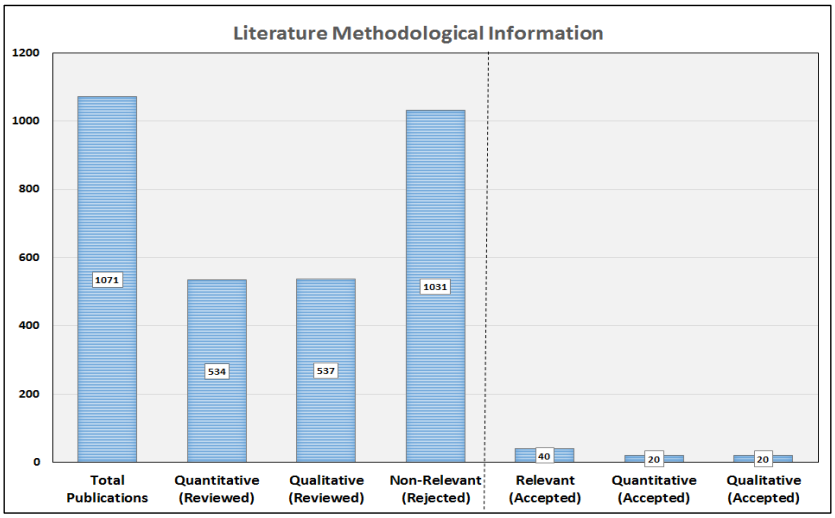


Figure 10. Document Down Select by Qualitative and Quantification Categories

5.2. Main Findings- Qualitative Analysis

The second group of analyses performed were more qualitative in nature. This group includes two separate analyses. The first analysis is summarized in the taxonomy illustrated in Table 5. The second part of the qualitative analysis is discussed in the section about the barriers for the adoption and information sharing of EHR.

Taxonomy of Human Error Causing Data Breaches.

In Table 5 we present a taxonomy of human driven privacy data breach incidents. To provide the context for this taxonomy, sources of human error are organized by either unintentional, intentional, or malicious incidents. The types of human error are categorized by their consequences or intent.

Human Error Cause	*Source of Human Error Causing Data Breaches*
Unintentional -- ***Lack of knowledge or skill, distraction***	Data entry error
	Lack of/or incorrectlyrecording privacy policy agreement
	Leaving sensitive information accessible to others
	Inappropriate skill in IT SW
	SW vulnerabilities
	Improper disposal of information
	Lost/misplaced mobile devices
	Lost paperworks
	Work pressure (pressure to work too fast)
	Employee attitude and behavior
	Insufficiently protecting stored information (e.g. encryption)
	Lack or improperly documented procedures
	Stress
	Not following security best practices
	System design flaws
	Lost of confidential security and credential
	Email misdelivery- releasing information to the wrong person
	Lack of awareness and training
	Lack of supervision
	Down loading internet files from unknown sources
	Victim of phishing
	Password hygiene
Intentional-- ***Know of potential risk but reckless***	Collecting information beyond requirement or unrelated to the purpose
	Restricting owners' access to information
	Storing or handling information in unsecured manner for the sake of simplicity or efficiency
	Secondary use of information during processing
	Inserting removable unauthorized media
	Sending unencrypted data
	Releasing information to an unauthorized party
	Mishandling passwords
	Poor access control
	Insufficient monitoring
	Inadequate, incomplete, or delayed patching SW security vulnerability
Malicious-- ***Intentional and damaging consequences***	Unauthorized access
	Service disruption
	Malware infection
	Employee manipulation and malfeasance
	Posting PHI on social media
	Discussing PHI with third parties

Table 5. Taxonomy of Human Driven Privacy Data Breach Incidents

Of these types of human error, unintentional errors are due to the lack of awareness or skills, or just a distraction from the employee performing the tasks. This type of error can be the result from simply surfing an internet site looking for an important account without understanding the associated risk of accessing such site. Or, while working, an employee inadvertently gets to an unsafe website linked from his/her social media account (Maalem, Caulkins, Mohapatra, & Kuman, 2020). Under an intentional human error, the employee understands the risk of his/her actions but still moves on, or misuses available resources. This behavior may not necessarily bring an immediate harmful action to the organization, but it may lead to an incident where private health information is compromised or results in a violation of existing laws or privacy. For example, an intentional error could be the result of an employee's reckless behavior transmitting unencrypted data for the sake of saving time. Or, just simply mishandling passwords such as writing a password to an important account on a sticky note and leaving it next to his/her computer terminal (Parsons, Calic, Pattinson, Butavicius, McCormac, & Zwaans, 2017; Ahola, 2020). In contrast, in a malicious error, the behavior of the employee is intentional and can have major damaging consequences. This is the worst type of error. Malicious error can occur when an employee deliberatively uses an unauthorized account, and or steals equipment from a hospital that stores patients' PHI (Liginlal, Sim, & Khansa, 2008). Overview of Barriers for the Adoption and Information Sharing of EHR. The reference section includes articles selected to inform the aim of this study. The main findings of the selected documents: (1) describe STS factors driving human error; (2) discuss the cost impacts of data breaches; (3) provide a framework to establishing a strong culture of cybersecurity; and, (4) discuss the potential benefits of EHR and the barriers that the healthcare sector is facing for their adoption and information sharing (Miller & Sim, 2004). In summary, multiple publications from the final list present evidence that computer-human interface factors represent a barrier to the widespread adoption and information sharing of EHR in the healthcare sector. These factors are not unique to the adoption of the EHR technology. Rather for the most part, they are no different to the type of challenges faced by organizations when new technologies are introduced. Gesulgaa, Berjameb, Moquialac, and Galidod (Gesulgaa, Berjameb, Moquialac, & Galidod, 2018); Ajami and Arab-Chadegani (Ajami & Arab-Chadegani, 2013); and Miller and Sim (Miller & Sim, 2004) evaluated barriers and solutions for widespread adoption and information sharing of EHR. Their research share the same perspective: people behavior and available resources are the primary EHR adoption and information sharing barriers to overcome. Personnel attitudinal constraints-behavior of individuals such as physicians' attitudes, users' lack of skills, and lack of administrative and policy support are the most relevant barriers to the adoption and information sharing. They conclude that public and private policy interventions can effectively counter these barriers and drive quality improvement. Palabindala, Pamarthy, and Jonnalagadda (Palabindala, Pamarthy, & Jonnalagadda, 2016) concluded that the acquisition cost of EHR systems for healthcare providers is a major contributing factor impeding the widespread adoption and information sharing of patients' records. Their publication suggests that healthcare providers must commit to upgrading their systems and establish regular training for their users to prevent human error and adverse information security incidents. Bowman (Bowman, 2013) addresses the importance of understanding how a poorly designed and improperly used EHR system can lead to human error that risks patient safety and the quality of services provided by the healthcare system. She concludes that failure to recognize and address EHR security issues, rather than improving the healthcare efficiency performance and reduce cost, could lead to spiraling cost, medical errors, and irreparable reputation. Bowman suggests that a combination of government policy and industry technology improvements are necessary to prevent such an unintended consequence from EHR adoption and use.

6. Discussion

The selected publications included in the paper expand the scope of this research. The findings not only inform the research topic but also contribute to the information security theory and in a limited way to the STS principles. The findings also advance the understanding of combining these two bodies of knowledge and suggest changing the way the sector is approaching healthcare data security to reduce the impact of human error in data breaches. These findings can be summarized as follows: (1) a taxonomy that identifies typical human error contributing to privacy data breach incidents (Table 5); (2) a STS model for EHR systems (Figure 11); (3) a conceptual framework of STS factors that drive human error (Figure 12); (4) a proposed conceptual model of STS factors hypothesized to reduce human driven data breaches in EHR (Figure 13); and a (5) a qualitative model represented by a causal loop diagram with the interrelationships between these STS factors (Figure 14). Further, these findings will help government and healthcare leaders implement policy to improve the design of IAM solutions to reduce human error and protect EHR.

6.1. STS Principles and Application to Information Security in the Healthcare Sector.

One objective in this literature review was to investigate the application of STS principles to information security in the healthcare sector. Thus, the final selection of articles was focused on identifying cases where a systems engineering approach was applied to develop a conceptual model of STS factors hypothesized to reduce the likelihood of human error leading to breaches in the healthcare industry. Highly technological systems such as telecommunications, defense, and healthcare with the objective of improving patients' safety are becoming more complex (Qureshi, 2008). A primary characteristic of these systems is the high degree of human-technology interaction and

collaboration required to deliver outcomes that otherwise would be impossible. These systems with components such as innovative technology artifacts, people in the loop, and governance, are often part of a larger ecosystem comprised of complex social structures such as internal/external stakeholders, economic and financial aspects, and government regulation realities. Within the STS principles, human factors and organizational processes interact with technology in the workplace, and achieving the organizational objectives can only be met by the joint optimization of the technical and social aspects (Trist & Bamforth, 1951). Figure 11 illustrates the application of the STS principles to an EHR system. The diagram implies that a complex STS, such as EHR, must consider the interactions between technologies, people and processes, and governance as critical factors for understanding the system optimizing its output. In the figure, the EHR system is represented by the inverted inner triangle with an inner loop where technology innovation, human risk, and policy compliance interact. The interaction of the EHR system within the healthcare organization is represented by the external triangle, and their relations with the external environment by the outer circle.

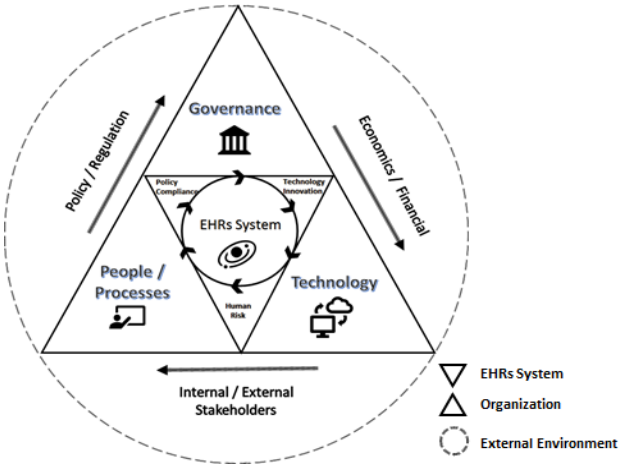


Figure 11. STS Model Application to the EHR System

It is hypothesized in this paper that STS factors are associated with the likelihood of human error in healthcare data breaches. Simply relying on technical alternatives might not be the solution to improve the security of healthcare records. Instead, the application of STS principles to information security introduces an approach that incorporates government policy, human in the loop, organizational processes, economic aspects, and technical factors, as well as the interrelationship among them, to reduce the impact of human error in data breaches. This interaction of STS factors is hypothesized to reduce data breaches--- by improving the reliability and consistency of the identity access management (IAM) process that identify and accurately confirm the credentials of the users getting access to the system--- increase the EHR adoption and information sharing, and consequently improve the efficiency performance in the healthcare industry (Vargheese, Prabhudesai, 2014).

6.2. Conceptual Framework of Human Error Drivers of Healthcare Data Breaches

Many STS factors that contribute to human error causing data breaches in healtcare systems are closely related. Our analysis of the literature review began by listing all of the factors and attributes identified by authors that probably contribute, at varying degrees, to increasing the likelihood of data breaches not only in hospitals but in healthcare organizations such as private practices, health insurance organizations, and treatment and medical test facilities. This list from our conceptual framework of human error drivers presented in Figure 12, specifically excludes technical risk-drivers such as encryption protocols, software cyber detection applications, and firewalls, which are typically captured by the inherit design of hardware infrastructures and most commercial EHR software applications found in industry. The following paragraphs describe the factors included in the framework and present viewpoints expressed by authors from the literature where these factors were addressed.

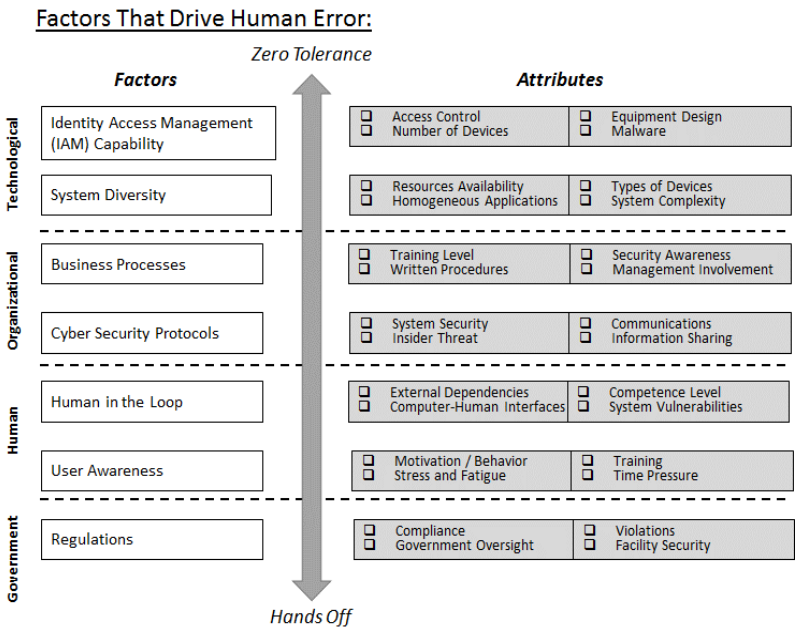


Figure 12. Organizations' Conceptual Framework of Human Error Drivers

IAM Capability. Despite significant investments in IAM systems, data breaches continue to grow affecting healthcare organizations and compromising patients' data, with basic human error as the root of a significant proportion of these breaches (Ponemon Institute, 2022). While healthcare systems have digitized to keep up with the adoption and information sharing of EHR, the sector has not dynamically implemented trusted digital IAM solutions at the same pace, leading to vulnerabilities in the records system. Strong IAM solutions are a necessary component of an information security system. Organizations that keep a close audit and monitoring of their devices authorized for conducting official business, are better positioned to avoid malware and can respond to incidents faster than organizations that don't follow this practice (Megas, Lam, & Nadeau, 2015). System Diversity. The EHR vulnerability of the U.S. Healthcare Sector is affected by the vulnerabilities of all individual healthcare units. In this large system, reducing variability of IAM capabilities of individual healthcare units will make the whole system less vulnerable (Jalali & Kaiser, 2018). Most healthcare units operate within a constraint budget. Despite over 80% of hospitals reporting data breaches, on average healthcare units allocate about 5% of their IT budgets to the development of IAM capabilities and other cyber-security activities (Garrity, 2009). Low IT investment increases the likelihood of successful data breaches. In other words, healthcare units that do not have sufficient IT budgets will struggle to develop IAM capabilities and will continue to be the victim of data breaches (Jalali & Kaiser, 2018). Networked or connected medical devices have become a popular practice in healthcare to remotely monitor patients, deliver care, and transfer patient data. A coordinated approach within the healthcare sector that leverages common standard practices and access controls to systems is necessary to protect these devices in todays' highly interconnected system (Meeks, Smith, Taylor, Sittig, Scott, & Singh, 2014; Williams & Woodard, 2020). A common IAM capability framework focused on reducing human technology interface errors will make the healthcare industry less attractive to cybercriminals (Jalali & Kaiser, 2018). Business Processes. Cybersecurity threats and data breaches in the healthcare sector are far from over. There is no sign that the trend of record breaches will slow down. The healthcare sector needs to be prepared and proactive to respond to data breaches, protect their reputation, and lessen the financial burden associated with identifying and responding to a data breach (Basset, Hylender, LangloisPinto, & Widup, 2021). Given the sensitivity of patient' information, healthcare management efforts should strive to create an organizational security culture environment, where employees feel the responsibility of immediately reporting mistakes or unintentional disclosures of patient's data without fear of repercussion (Hung, 2010). Even when the mistakes or disclosures might not be reversed, their impact might be mitigated and the end damage to the organization and patient's data be diminished (HIPAA, 2021). Employee awareness training and emphasis on the importance of following written security procedures for protecting patients' PHI will create a security culture environment where the healthcare staff will be more conscious about the detrimental impact of a data breach and will reduce the likelihood of occurrence of human errors. (Miller & Sim, 2004; Palabindala, Pamarthy, & Jonnalagadda, 2016). Cyber Security Protocols. People make mistakes. Most errors are unintentional actions, typically taken by an internal or insider threat actor, but partner actor errors also occur. The trend of basic human error in the healthcare industry is not diminishing. Errors such as email mis-delivery where employees release information to the wrong person is among the most common errors. Lack of following cybersecurity protocols such as neglecting two-factor authentication is making it easier for cyber criminals to get unauthorized access to

secure systems. Simultaneously, criminal groups continue to target the market looking for financial opportunities (Health Informatics & Health Information Management, 2021). Adoption of "zero trust architecture" principles to security will provide a defensible architecture to protect from human error that are creating vulnerabilities in healthcare systems. Under a "zero trust" model, the identity and credentials of all users requesting access to a network are authenticated, authorized, and validated for security before access is granted to systems applications and the data within (Rose, Borchert, Mitchell, & Connelly, 2020; The White House, 2021). Adoption of a "zero trust architecture" offers management the information security principles to focus attention in their people actions, working environments, and business processes with the goal of reducing information security incidents through a reduction in human error (Evans, He, Luo, Yevseyeva, Janicke, & Maglaras, 2019). Human in the Loop. In terms of economic impact to the firms, "human error is the largest single cause of economic and productivity loss in the information systems security arena" (Zimmermann & Renaud, 2019). Healthcare information technologist have raised concerns that although human behavior and their errors often lead to data breaches and present a barrier for EHR adoption and information sharing (Gesulgaa, Berjameb, Moquialac, & Galidod, 2018), despite repeated calls for human factors to be addressed in the design of IT systems the issue has not adequately been addressed by many current security models (Isaac & Zeadally, 2011; Carayon, 2006; Chena, Lia, & Zhang, 2011). In the information security theory, humans are seen as the weakest link in the security chain (Yan, Robertson, Park, Bordoff, Chen, & Sprissler, 2018). The variability on the probability of human error has a significant importance in reducing the healthcare unit vulnerability to data breaches. People are a vital part of protecting the privacy of patients' EHR. An organizational culture shift, focused on human-computer interaction, which integrates medical professional staff in the design of IAM capabilities rather than treating them as their weakest point, could be associated with the reduction of cyber incidents leading to data breaches (Zimmermann & Renaud, 2019). User Awareness. Experts in the field recognize that technology alone cannot deliver a complete EHR system security solution (Safa, Sookhak, Von Solms, Furnell, Ghani, & Herawan, 2015). There is also a tangible need to address the user aspects. The greatest threat to EHR lies with the unintentional and sometimes malicious actions of unmotivated users with open access to information resources (Warkentin & Williamson, 2009; Warketin & Williamson, 2013; Khan, Brohi, & Zaman, 2020). However, simply blaming users will not lead to more effective security systems (Vargheese & Prabhudesai, 2014; Khan, Brohi, & Zaman, 2020). Rather, it is recommended to cybersecurity system designers to address the causes of undesirable user behavior and incorporate mitigations for designing effective security systems (Safa, Sookhak, Von Solms, Furnell, Ghani, & Herawan, 2015; Workgroup for Electronic Data Interchange, 2017). Awareness about the damaging consequences of cybersecurity incidents is key for employees to be cognizant about security while executing their daily tasks (Di Nella, Mansourian, 2021). Regulations. The 1996 HIPAA act and subsequent amendments such as the Privacy Rule of 2003 regulates the use and disclosure of PHI and sets national standards that an entity working with health data must follow to protect patient private medical information. Those who must comply with the HIPAA requirements includes healthcare providers that performs transactions in electronic forms, and health plans, business associates, and healthcare clearing houses. To date, continuous enforcement of this provision has been a driving force behind healthcare organizations' creation of protocols for prevention, detection, and remediation of reported incidents. Implementation of HIPAA policy is expected to reduce the likelihood of human error in data breaches of the healthcare sector (HIPAA, 2021). HIPAA and the 2009 Health Information Technology for Economic and Clinical Health Act (HITECH) laws not only require hospitals and other healthcare organizations to keep access to their facilities and their patients' secured PHI, but also include data breach notification requirements, which mandate breaches be reported to the DHHS (HIPAA, 2021; Sector Coordinating Councils, 2017). Government regulation have made an impact on the operation of healthcare providers and providing safeguards to protect the information integrity contained in EHR. Government oversight, in the form of policy regulation, is necessary to ensure healthcare enforcement and compliance of PHI security standards to avoid information security issues resulting from unintentional consequences from EHR use (Bowman, 2013).

6.3. Literature Limitations

Going into the literature review, we acknowledged that one challenge in this research study was going to be the lack of a robust literature with a focus specifically on the human aspect of data breaches and cybersecurity in healthcare in general. Therefore, with the assistance of a healthcare professional and multiple cybersecurity professionals, we formulated the search queries using well-established STS factors related to healthcare information security to maximize the value of the literature searches. Further, in literature, the application of STS principles associated with human error in information technology and the cybersecurity domain has not received much attention (Charitoudi & Blyth, 2013). Most research emphasis to solve healthcare information security incidents has been placed on technical solutions with marginal attention to solving the challenges presented by the human-technology interactions in the organization (Malatji, Von Solms, & Marnewick, 2019). Due to the limitations of the literature reviewed, further investigation is recommended to validate the hypothesis and expand the knowledge of the field.

6.4. Proposed Research Hypothesis Model

Several publications from literature recognize that robust technical design solutions and government policy are not enough to contain data breaches of EHR. Rather, they suggest a deep change on the way the sector is approaching healthcare data security. Leading deep change requires showing healthcare organizations why the change will work and why the new paradigm is different from past experiences and their normal assumptions. Deep change depends on individuals' emotional state and emotions (Quinn, 2012). Based on this consideration, to effectively influence a change in culture, the sector's cyber professionals should be put through their security incident experiences to cause them to challenge their own assumptions. They should carefully examine what is currently occurring during major data breach incidents caused by human error and apply lessons learned to make the infrastructure more resilient. Based on the results from literature, it is also hypothesized that reducing the impact of human error in healthcare data breaches will improve hospitals and healthcare organizations' EHR adoption and information sharing. Consequently, a reduction in human error driven data breaches would result in an increase in the efficiency performance of the industry. Drawing from the human error factors described in Figure 12 of the previous section and to address the gaps and limitations from the literature, we propose a research hypothesis model that applies STS principles to the data breaches challenge in the healthcare sector. This model depicted in Figure 13 represents a culture shift from the way that the sector is approaching data security, from purely technical design solutions to a STS dynamic environment. The model proposes factors that are hypothesized to reduce human error driven data breaches in EHR, and increase adoption and sharing of EHR to improve the healthcare efficiency performance. Ideally, these are STS factors that designers of IAM systems should consider when thinking about reducing human error in data breaches and cybersecurity incidents in EHR.

Based on Figure 13, it can be hypothesized that:

H1: Implementation of trusted digital IAM solutions will reduce the likelihood of human error driven data breaches in EHR.

H2: Implementing a common IAM capability framework focused on limiting human technology interface errors will lower human error driven data breaches in EHR.

H3: The STS factors related to organizational security culture will be associated with the reduction of human error driven data breaches in the healthcare sector.

H4: Adoption of a "zero trust" architecture will reduce the likelihood of human error causing data breaches in EHR.

H5: Integration of healthcare professionals in the design of IAM capabilities will reduce the likelihood of occurrence of human error driven data breaches in EHR.

H6: The greatest threat to EHR's security lies by the careless or malicious actions of internal users. The factors related to user behavior are associated with the likelihood of reducing human error driven data breaches.

H7: Government policy and the security rules related to the implementation of HIPAA and HITECH policies will be associated with reducing the human error that are causing data breaches.

H8: The application of an STS approach that considers the combination of all H1-H7 hypotheses will result in a reduction of human error driven data breaches in the healthcare sector.

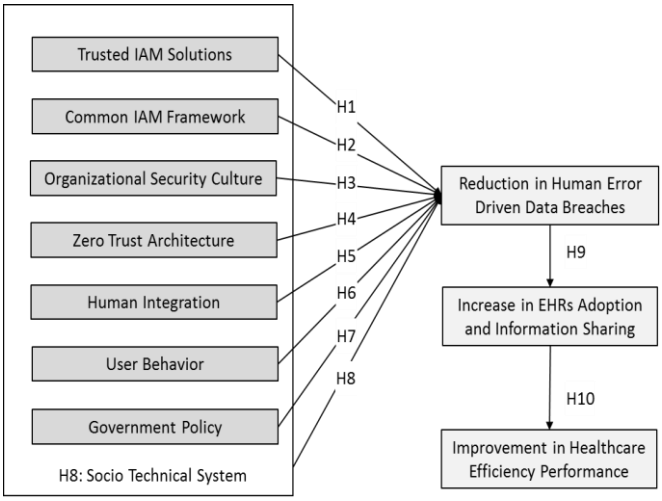


Figure 13. Proposed Research Hypothesis Model of STS Factors Hypothesized to Reduce Human Error Driven Data Breaches and Increase Adoption and Information Sharing in EHR, and Improve the Efficiency Performance of the Healthcare Sector

H9: A reduction of human error driven data breaches will increase the EHR adoption and information sharing in the healthcare sector.
H10: A reduction of human error driven data breaches will improve the efficiency performance of the healthcare industry.
The interrelationships between these factors are depicted in Figure 14 representing the qualitative model by a causal loop diagram (CLD). The CLD illustrates how these factors interact in a STS environment to reduce data breaches caused by human error in the healthcare sector. Six balancing feedback loops and two reinforcement loops are introduced in the CLD. The balancing loops leverage STS factors to achieve a desired state of reducing human error driven data breaches in the healthcare sector. For example, balancing feedback loop 1 (B1) addresses the need for stronger capabilities. B2 and B4 illustrate the effects of government policy and the organizational culture driving the organization to adopt zero trust architecture principles that consequently enables the organization to reduce human error driven data breaches in the sector. The B3 balancing loop relates user behavior and human integration as critical factors that drive data breach events in the healthcare organization. B5 and B6 represent the balancing feedback loops that interface all others factors and integrate them as a STS. Reinforcement feedback loop 1 (R1) captures the growth in EHR Users resulting from increases in the adoption rate and information sharing between healthcare units. The R2 reinforcement loop shows the growth in the system from the adoption of information security safeguards such as zero trust principles that results in an increase in the adoption rate.

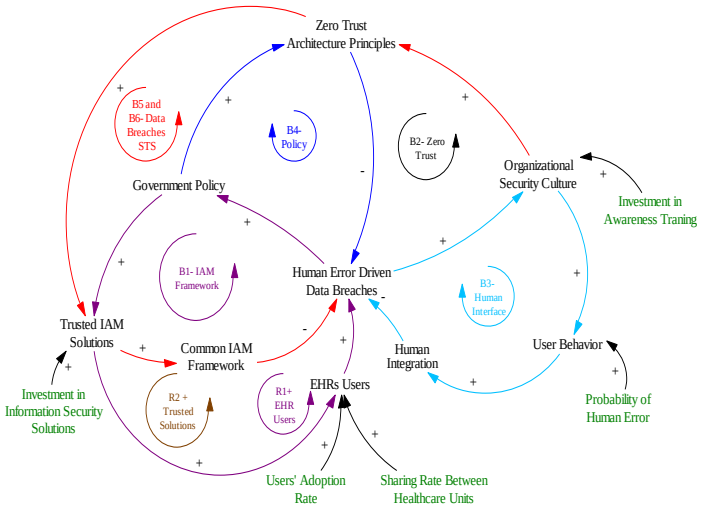


Figure 14. Causal Loop Diagram Illustrating the Inter-Relationship of the STS Factors Hypothesized to Reduce Human Error Driven Data Breaches in EHR

7. Conclusions

The U.S. Healthcare Sector faces persistent and increasingly sophisticated malicious data breach attempts that threaten the adoption and widespread information sharing of EHR and risk patients' information privacy. This paper presents the results of a systematic literature review of factors that influence human errors in healthcare data breaches and the EHR technology adoption. The objective was to apply Socio-Technical Systems (STS) principles to address the issue of human error in data breaches, which is posing challenges to the adoption of EHR technology and information sharing. It is hypothesized that mitigating these challenges will contribute to improving the overall effectiveness and efficiency performance in the industry. The paper introduces a taxonomy of human errors that cause data breach incidents. This taxonomy offers information security practitioners a solid base to categorize the sources of human error within the IT systems to enable the design of more resilient systems. The paper proposes a conceptual framework of STS factors that cause human errors in data breaches. We argue that the study of complex systems such as EHR should consider the interactions and relationships between technology, organization processes, people, and government policy. The framework highlights the following STS factors: Identity Access Management (IAM) Capabilities; System Diversity; Business Processes; Cyber Security Protocols; Human in the Loop; User Awareness; and, Government Regulations. Findings from multiple sources in the literature converge to the same conclusion: people behaviors leading to errors are the primary information privacy concern and a barrier to EHR adoption and information sharing. Personnel attitudinal constraints and behaviors such as physicians' attitudes, users' lack of skills, and lack of administrative and policy support are sources of human mistakes that are creating vulnerabilities and opening opportunities for cyber attackers to compromise the confidentiality of the digital information infrastructure. While the adoption of EHR systems have resulted in substantial benefits to patient care, patients' information privacy resulting from human error data breaches have emerged during their

implementation. These data breaches have put in danger patient safety, information privacy, and have decreased the quality of patients' care services. This paper makes several contributions to the information security theory by identifying STS principles that have not been explored in previously published work. First, it highlights a research gap in terms of understanding and modeling human-computer interactions and the consideration of STS factors when developing solutions. Second, it identifies the lack of attention by the international research community about the subject and its implications for the adoption and information sharing of EHR. Third, it recognizes that robust technical design solutions and government policy are not enough, rather, what is required is a deep change on the way the sector is approaching healthcare data security. Fourth, the paper presents a conceptual framework of STS factors that drive human error in information security. The results of the systematic literature review led us to recommend further research opportunities to investigate the formulation and implementation of a STS approach with the goal of mitigating human error in information security and make EHR less attractive to cybercriminals. The landscape in human privacy is changing and becoming more challenging as we move more and more of our lives into the digital space. Although most of our lives are now stored somewhere online, the healthcare sector must realize the risks involved in the ways in which protected health data is being used once records are stored digitally. Hopefully greater attention to STS factors in the design of information security solutions will lead to a change, and better protection of patients' privacy.

References

Ahola, M., (2020). The Role of Human Error in Successful Cyber Security Breaches. Newspaper-Usecure Blog.

Ajami, S., Arab-Chadegani, R., (2013). Barriers to Implement Electronic Health Records (EHR). Avicena Publisher.

Armitage, A., Keeble-Ramsay, D., (2009). The Rapid Structured Literature Review as a Research Strategy. US-China Education Review.

Basset, G., Hylender, C.D., Langlois, P., Pinto, A., Widup, S., (2021). Data breach Investigation Report. Verizon Corporation.

Beitollahi, H., Deconinck, G., (2012). A Four-Step Technique for Tackling Distributed Denial of Service Attacks. Scopus Elsevier.

Bowman, S., (2013). Impact of Electronic Health Record Systems on Information Integrity: Quality and Safety Implications. AHIMA.

Bump, J.B., Fan, V.Y., Lanthron, H.E., Yavuz, E.N., (2012). In The Global Fund's Court: Experimentation, Evaluation, and The Affordable Medicine Family. The Lancet.

Callahan, M.E., (2013). Cybersecurity and Hospitals. American Hospital Association.

Carayon, P., (2006). Human Factors of Complex Socio-Technical Systems. Scopus Elsevier.

Charitoudi, K., Blyth, A., (2013). A Socio-Technical Approach to Cyber Risk Management and Impact Assessment. Scientific Research.

Chena, W., Lia, J., Zhang, J., (2011). An Approach to Service Adaptation for Exploratory Application Construction. Scopus Elsevier.

Crema, M., Verbano, C., (2013). Guidelines for Overcoming Hospital Managerial Challenges: A Systematic Literature Review. Dove Press.

Davis, D.R., Kurti, A.N., Skelly, J.M., Redner, R., White, T.J., Higgins, S.T., (2014). A Review of the Literature on Contingency Management in the Treatment of Substance Use Disorders, 2009-2014. Europe PubMed Central (PMC).

Di Nella, A., Mansourian, A., (2021). The Human Error in Cybersecurity. NMS Consulting.

Evans, M., He, Y., Luo, C., Yevseyeva, I., Janicke, H., Maglaras, L., (2019). Employee Perspective on Information Security Related Human Error In Healthcare: Proactive Use Of IS-CHEC In Questionnaire Form. Research Gate.

Franke, U., Brynielsson, J., (2014). Cyber Situational Awareness: A Systematic Review of the Literature. Scopus Elsevier.

Garrity, M., (2019). 5% of Hospital IT Budgets Go to Cybersecurity Despite 82% of Hospitals Reporting Breaches. Global Research.

Gesulgaa, J.M., Berjameb, A., Moquialac, K.S., Galidod, A., (2018). Barriers to Electronic Health Record System Implementation and Information Systems Resources: A Structured Review. Scopus Elsevier.

Health Informatics & Health Information Management, (2020). Cybersecurity: How Can It Be Improved in Health Care? University of Illinois, Chicago.

Health Insurance Portability and Accountability Act (HIPAA), (2021). Guide to Privacy and Security of Health Information. Department of Health and Human Services- Health IT.Gov.

Health Insurance Portability and Accountability Act (HIPAA), (2022). Healthcare Data Breach Statistics. Department of Health and Human Services.

Hofmey, S.A., (1999). An Immunological Model of Distributed Detection and Its Application to Computer Security. University Research- University of the Witwatersrand.

Hung, P.C.K., (2010). Towards a Privacy Access Control Model for e-Healthcare Services. University of Ontario Institute of Technology (UOIT).

Information Technology Laboratory, NIST, (2015). Measuring Strength of Identity Proofing. National Institute of Standandards and Technology (NIST).

Isaac, J.T., Zeadally, S., (2011). An Anonymous Secure Payment Protocol in a Payment Gateway Centric Model. Scopus Elsevier.

Jalali, M.S., Kaiser, J.P., (2018). Cybersecurity in Hospitals: A Systematic, Organizational Perspective. Render Internet Publishing.

Katharakisa, G., Katharakib, M., Katostaras, T., (2013). SFA vs. DEA for Measuring Healthcare Efficiency: A Systematic Review. University Research-International Journal of Statistics and Medical Research.

Keathley-Herring, H., Van Aken, E., Gonzalez-Aleu, F., Deschamps, F., Letens, G., Cardenas Orlandini, P., (2016). Assessing the Maturity of a Research Area: Bibliometric Review and Proposed Framework. Springer.

Khan, F., Kim, J.H., Mathiassen, L., Moore, R., (2019). Data Breach Management: An Integrated Risk Model. Scopus Elsevier.

Khan, N.A., Brohi, S.N., Zaman, N., (2020). Ten Deadly Cyber Security Threats Amid COVID-19 Pandemic. IEEE Computer Society.

Liginlal, D., Sim, I., Khansa, L., (2008). How Significant is Human Error as a Cause of Privacy Breaches? An Empirical Study and a Framework for Error Management. Scopus Elsevier.

Maalem Lahcen, R.A., Caulkins, B., Mohapatra, R., Kumar, M., (2020). Review and Insight on the Behavioral Aspects of Cybersecurity. Open Access.

Malatji, M., Von Solms, S., Marnewick, A., (2019). Socio-Technical Systems Cybersecurity Framework. Emerald Publishing Limited.

Meeks, D.W., Smith, M.W., Taylor, L., Sittig, D.F., Scott, J.M., Singh, H., (2014). An Analysis Of Electronic Health Records Related Patient Safety Concerns. Open Access Publishing.

Megas, K., Lam, P., Nadeau, E., (2015). NSTIC Pilots: Catalyzing the Identity Ecosystem. National Institute of Standards Technology (NIST).

Menear, M., Doré, I., Cloutier, A.M., Perrier, L., Roberge, P., Duhoux, A., Houle, J., Fournier, L., (2014). The Influence of Comorbid Chronic Physical Conditions on Depression Recognition in Primary Care: A Systematic Review. Scopus Elsevier.

Miller, R.H., Sim, I., (2004). Physicians' Use of Electronic Medical Records: Barriers and Solutions. Scopus Elsevier. Project Hope.

Moher, D., Liberati, A., Tetzlaff, J., Altman, D.G., (2009). Preferred Reporting Items for Systematic Reviews and Meta-Analyses: The PRISMA Statement. Annals of Internal Medicine.

Morgan, S., (2021). The 2020-2021 Healthcare Cybersecurity Report. HERJAVEC Group.

Nifakos, S., Chandramouli, K., Nikolaou, C.K., Papachristou, P., Koch, S., Panaousis, E., Bonacina, S., (2021). Influence of Human Factors on Cyber Security within Healthcare Organisations: A Systematic Review. Multidisciplinary Digital Publishing Institute (MDPI).

Ouksel, A., Lundquist, D., (2012). A Context-Aware Cross-Layer Broadcast Model for Ad-Hoc Networks. Scopus Elsevier.

Palabindala, V., Pamarthy, A., Jonnalagadda, N.R., (2016). Adoption Of Electronic Health Records And Barriers. Taylor & Francis Group.

Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., Zwaans, T., (2017). The Human Aspects of Information Security Questionnaire (HAIS-Q): Two Further Validation Studies. Scopus Elsevier.

Perneger, T.V., (2005). The Swiss Cheese Model of Safety Incidents: Are There Holes in The Metaphor?. BMC Health Research.

Pfleeger, S.L., Caputo, D., (2012). Leveraging Behavioral Science to Mitigate Cyber Security Risk. Research Gate.

Ponemon Institute, (2022). Cost of a Data Breach Report. International Business Machines (IBM).

Quinn, R.E., (2012). Deep Change Field Guide. Jossey-Bass, John Wiley & Sons, Inc.

Qureshi, Z.H., (2008). A Review of Accident Modelling Approaches for Complex Critical Socio-Technical Systems. Defense Science and Technology Organization.

Rose, S., Borchert, O., Mitchell, S., Connelly, S., (2020). Zero Trust Architecture. National Institute of Standards Technology (NIST).

Rouached, M., Sallay, H., (2011). An Efficient Formal Framework for Intrusion Detection Systems. Scopus Elsevier.

Safa, N.S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N.A., Herawan, T., (2015). Information Security Conscious Care Behaviour Formation in Organizations. Scopus Elsevier.

Sardi, A., Rizzi, A., Sorano, E., Guerrieri, A., (2020). Cyber Risk in Health Facilities: A Systematic Literature Review. Multidisciplinary Digital Publishing Institute (MDPI).

Schoen, C., Davis, K., How, S.K.H., Schoenbaum, S.C., (2006). USA Health System Performance: A National Scorecard. Project HOPE–The People-to-People Health Foundation.

Sector Coordinating Councils, (2017). Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients. Department of Health and Human Services.

Seh, H.A., Zarour, M., Alenesi, M., Sarkar, A.K., Agrawal, A., Kumar, R., Ahmad Khan, R., (2020). Healthcare Data Breaches: Insights and Implications. Multidisciplinary Digital Publishing Institute (MDPI).

Smet, M., (1982). Cost Characteristics of Hospitals. Social Science & Medicine. Europe PubMed Central (PMC).

Snyder, H., (2019). Literature Review as a Research Methodology: An Overview and Guidelines. Scopus Elsevier.

The White House, (2021). Improving the Nation's Cybersecurity. Executive Order 14028.

Torraco, R.J., (2005). Writing Integrative Literature Reviews: Guidelines and Examples. SAGE Journals.

Torres-Tomas, J., Spolaˆora, N., Alvares-Chermana, E., Mona, M.C., (2014). A Framework to Generate Synthetic Multi-Label Datasets. Scopus Elsevier.

Tranfield, D., Denyer, D., Smart, P., (2003). Towards a Methodology for Developing Evidence-Informed Management Knowledge by Means of Systematic Review. University Research-British Journal of Management.

Trist, E., Bamforth, K., (1951). Some Social and Psychological Consequences of the Longwall Method of Coal Getting. Human Relations.

Vargheese, R., Prabhudesai, P., (2014). Securing B2B Pervasive Information Sharing Between Healthcare Providers: Enabling the Foundation for Evidence Based Medicine. Scopus Elsevier.

Warkentin, M., Willison, R., (2009). Behavioral and Policy Issues in Information Systems Security: The Insider Threat. European Journal of Information Systems.

Warkentin, M., Willison, R., (2013). Beyond Deterrence: An Expanded View of Employee Computer Abuse. Journal Storage (JSTOR).

Whitworth, B., (2009). The Social Requirements of Technical Systems. University Research- IGI Global.

Williams, P.A.H., Woodward, A.J., (2020). Cybersecurity Vulnerabilities In Medical Devices: A Complex Environment And Multifaceted Problem. Publication Medication Central (PMC).

Wong, G., Greenhalgh, T., Westhorp, G., Buckingham, J., Pawson, R., (2013). RAMESES Publication Standards: Meta-Narrative Reviews. Open Access.

Workgroup for Electronic Data Interchange, (2017). The Rampant Growth of Cybercrime in Healthcare. FORTINET.

Yan, Z., Robertson, T., Yan, R., Park, S.Y., Bordoff, S., Chen, Q., Sprissler, E., (2018). Finding the Weakest Links in the Weakest Link: How Well Do Undergraduate Students Make Cybersecurity Judgment? Scopus Elsevier.

Yasnoff, W.A., (2016). A Secure and Efficiently Searchable Health Information Architecture. Scopus Elsevier. Scopus Elsevier.

Zimmermann, V., Renaud, K., (2019). Moving from a 'Human-as-Problem" to a 'Human-as-Solution" Cybersecurity Mindsetj. Scopus Elsevier.