Review

Assessing the Legal Aspects of Information Security Requirements for Health Care in 3 Countries: Scoping Review and Framework Development

Prosper Kandabongee Yeng*, MSc; Muhammad Ali Fauzi*, MSc; Luyi Sun*, MSc; Bian Yang*, PhD

Department of Information Security and Communication Technology, Norwegian University of Science and Technology, Gjovik, Norway

*all authors contributed equally

Corresponding Author:
Prosper Kandabongee Yeng, MSc
Department of Information Security and Communication Technology
Norwegian University of Science and Technology
Teknologivegen 22
Gjovik, 2815
Norway
Phone: 47 96992743
Email: prosper.yeng@ntnu.no

Abstract

Background: The loss of human lives from cyberattacks in health care is no longer a probabilistic quantification but a reality that has begun. In addition, the threat scope is also expanding to involve a threat of national security, among others, resulting in surging data breaches within the health care sector. For that matter, there have been provisions of various legislation, regulations, and information security governance tools such as policies, standards, and directives toward enhancing health care information security–conscious care behavior among users. Meanwhile, in a research scenario, there are no comprehensive required security practices to serve as a yardstick in assessing security practices in health care. Moreover, an analysis of the holistic view of the requirements that need more concentration of management, end users, or both has not been comprehensively developed. Thus, there is a possibility that security practice research will leave out vital requirements.

Objective: The objective of this study was to systematically identify, assess, and analyze the state-of-the-art information security requirements in health care. These requirements can be used to develop a framework to serve as a yardstick for measuring the future real security practices of health care staff.

Methods: A scoping review was, as a result, adopted to identify, assess, and analyze the information security requirement sources within health care in Norway, Indonesia, and Ghana.

Results: Of 188 security and privacy requirement sources that were initially identified, 130 (69.1%) were fully read by the authors. Subsequently, of these 188 requirement documents, 82 (43.6%) fully met the inclusion criteria and were accessed and analyzed. In total, 253 security and privacy requirements were identified in this work. The findings were then used to develop a framework to serve as a benchmark for modeling and analyzing health care security practices.

Conclusions: On the basis of these findings, a framework for modeling, analyzing, and developing effective security countermeasures, including incentivization measures, was developed. Following this framework, research results of health care security practices would be more reliable and effective than relying on incomprehensive security requirements.

(JMIR Hum Factors 2022;9(2):e30050) doi: 10.2196/30050

KEYWORDS

legal requirement; information security; healthcare; security practice

Introduction

Background

There have been enormous gains in the application of information technology (IT) in health care in various areas such as decision support, telemedicine, electronic health record (EHR) management, chronic disease management with medical devices, drugs, and vaccine production [1-3]. However, cyberattacks in health care and their related adverse impact are a significant problem, especially in the midst of the infamous COVID-19 pandemic [4]. For example, Brno University Hospital in the Czech Republic was recently attacked, and cyberattackers were believed to have used spear phishing to gain access and deployed ransomware, which encrypted the data in the entire hospital network [5]. The hospital was compelled to shut down and battle with the cyberattack to restore its data. Even though the hospital was one of the COVID-19 treatment centers, the incident apparently prevented them from providing health care services during the attack period. Following that, there were other cyberattacks on the World Health Organization, Hammersmith Medicines Research Group in the United Kingdom (a COVID-19 vaccine trial group), the US Health and Human Services Department, Paris Hospital Authority in France, Bam Construct and Interserve (a COVID-19 hospital construction company), and Babylon Health (a hospital appointment and teleconsultation videoconferencing system) in the United Kingdom [6].

In addition, cybersecurity and privacy issues in health care have become a global concern as data breaches in health care continue to surge. In 2017, approximately 5 million health care records were compromised globally [1-3]. This tripled in 2018 to approximately 15 million, and the number of compromised health care records continues to increase yearly [3]. In addition, the cost associated with data breaches (eg, cost of detection of breaches, cost of fines paid in data breaches, cost of recovery, and payment of ransoms) is the highest in health care among various industries [7].

Data breaches and security issues in health care have major consequences on confidentiality, integrity, and availability (CIA). This usually perturbs the data subjects, the health care organizations, and the laws of the countries involved [8,9]. The adverse impact on data subjects includes situations in which the stolen data can be used as a means of pressure to demand other goals by criminals. Recently, an instance occurred in Finland [10], where stolen medical records were used by cybercriminals to pressure the data owners for money. Unauthorized persons can also disrupt the proper functioning of health care operations, such that the net effect can result in the loss of a patient's life. A related instance occurred in Germany, where a hospital's IT systems were hit by ransomware, which resulted in the death of a patient due to the unavailability of the health care system at the time of need [11]. Mutual trust and confidentiality between health care providers and patients [12-15], economic losses [10,15,16], privacy issues [9,17], and unreliable medical records [11,18,19] or medical devices [3] are some of the effects often faced by data subjects during cyberattacks in health care. It could be much disheartening for patients to battle against their medical conditions, and at the same time, they have to battle with their privacy issues arriving from cyberattacks. Mutual trust with data between health care professionals and patients is very cardinal in terms of good-quality health provision. Health care professionals depend on the accuracy and comprehensiveness of the information provided by patients for therapeutic measures [13]. Therefore, health care providers are required to store large quantities of sensitive personal information of patients [14]. Similarly, patients trust that their personal information disclosed for medical reasons is to be kept confidential [15]. Sadly, this mutual trust in relation to patients' data is often broken in data breaches [15,16].

Furthermore, health care systems are targeted for various computer crimes with the intention of stealing, altering, hindering, and disrupting data or other functions [5,11]. The consequences of cyberattack on health care organizations include loss of trust, credibility, and confidence from stakeholders; in addition, the financial impact on their organization and the hospital may face regulatory sanctions [9,20,21] if due care and due process were not followed. Health care issues emanating from cyberattacks can also undermine a nation's health care policy as a whole, as the unavailability of health care systems could undermine the rights of citizens to health care [14,22].

In addition, laws have been enacted in various jurisdictions to protect the privacy of people in their countries [18,20,23]. However, data breaches in health care disrupt all these measures. According to the forecast of the International Organization for Standardization (ISO), the estimated annual losses from cybercrime could soon reach USD2 trillion [14] with countless daily breaches [19]. This forecast is in resonance with the current trend of the cost of data breaches of which health care is in the lead [7].

In this light, the European Union (EU) classified health care as an essential service having foreseen cyberattack on health care as a threat to national security [22]. This requires member states and the European Economic Area–affiliated member states to develop a culture of security across services that are vital for the economy and society and rely heavily on information and communication technology (ICT).

To maintain security in health care, various laws exist, including regulations, directives, statutory and constitutional laws, and various information security governance measures such as policies, standards, guidelines, and best practices, called "information security requirement" in this study. These were developed to prevent information security issues in health care. Owing to various cybersecurity issues, various efforts have been made to measure the security practices of health care staff [3,16,24-29], as they are the weakest link in the security chain [30,31]. However, these activities require a benchmark in the context of legal requirements in information security in health care that can be used as the measuring standard in such studies. For example, to create a questionnaire to measure health care staff's cybersecurity practices, the content of the questionnaire could be derived from the legal requirements. Therefore, the question is, what is the benchmark that is to be used as a yardstick for measuring the security compliance level of health

care staff and to what extent have these security requirements been incorporated at the organizational level where these security requirements are to be followed?

Security violations in health care facilities are not due to a lack of rule-based requirements but due to a lack of compliance with rules and in some cases due to technical vulnerabilities that could not be addressed by law, requiring an investigation as to why the challenges exist in complying with these rules. In measuring the cybersecurity practices of the health care staff, a comprehensive security requirement is required. However, a noncomprehensive security requirement is sometimes relied on, which does not serve as an effective baseline. For instance, in a recent assessment of the security practice of health care in Norway [32], the study relied on the Health Register Act, the Health Personnel Act, the Patient Records Act, and the General Data Protection Regulation (GDPR). The study relied on some legal sources; however, other vital legal sources such as the Personal Data Act of Norway, the Network and Information Security Directive of EU, and the Medical Device Directive of EU, were not considered. Other related studies [33,34] have considered a legal requirement in their work, but no study has comprehensively and systematically conducted a study on legal requirements that can serve as a benchmark for assessing health care staff security practices.

The general objective of this study is therefore to address this gap by comprehensively identifying the required security requirements in health care through state-of-the-art studies to provide input for the development of a framework for analyzing health care security practice in the context of legal requirements. The remaining sections include background studies and a specification of the scope, contribution, and research questions. This is followed by the research methods, findings, and discussion of results. A framework for analyzing health care security practice in the context of legal requirements is then presented for real studies in the future.

The health care information of persons is one of the most sensitive personal information and therefore has special protection from various laws [14,23,35,36]. Laws are rules elected to be followed by members of a society to meet the needs of society while balancing individual rights to their self-determination [37]. Laws frown against certain behaviors and are enforced by a state or the governing body. Therefore, all categories of health care information system users are legally bound to comply with legal requirements of which a contrary act will attract the application of punitive measures [20,36,38]. Therefore, it is extremely important to consider legal requirements as the baseline in measuring the security practices of health care staff.

Owing to the numerous threats of attack in health care [1-6], there have been initiatives to measure the security practices of health care staff [16]. This is to help identify the security requirements that are not being complied with and further determine the challenges or reasons why these security measures are not being complied with. The results of this study will help in finding effective solutions to enhance the conscious care behavior of users. Security practice in this study refers to how users respond to or comply with security measures that have been established to meet the CIA requirement of systems and resources [16,24,26].

In assessing the security practices in health care, it is important to establish the scope of the hospital's legal and ethical obligations in relation to information security and privacy management [16,24,37]. This requires a catalog of comprehensive security requirements to understand the state-of-the-art legal requirements, including regulations, directives, policies, and guidelines for the fortification of users in health care IT systems against cyberattacks.

A comprehensive state-of-the-art security requirement is needed [39,40]; otherwise, what will be the benchmark in assessing the security practice level of hospital users? Moreover, if there is a security breach in health care by a user based on a lack of knowledge of a security requirement, the organization can still be liable or legally responsible [41]. This means that the health care organization will continue to make restitution for related harm caused in the breach [41]. This calls for due care and due diligence [42,43] on the part of health care organizations. Due care is measures taken by an organization to ensure that all employees are aware of acceptable and nonacceptable security practices, whereas due diligence is reasonable measures that are taken by the organizations or people to meet the established security requirements imposed by law [37]. Health care organizations increase their risk of being liable if they fail to adopt due care and due diligence measures. This is necessary because health care tends to rely more on IT and the internet for efficiency; a larger number of people can be adversely affected in a security breach situation as internet-based solutions are globally reached, which therefore require security due diligence and due care [37,42,43].

Type of Laws

Laws can be categorized based on their origins, such as constitutional law, statutory law, regulatory or administrative law, and common law, which is otherwise known as case law or precedents [37,44,45]. Constitutional law originates from the constitution of a state, bylaws, or a charter, but laws that originate from the legislative arm of governance with the mandate to make and publish laws of the country are known as statutory laws [37,44]. Furthermore, regulatory or administrative laws are created from the executive arm of the government or an authorized regulatory agency backed with executive orders and regulations [37,44]. Laws made from the judicial branch and boards based on the interpretation of law through the previous ruling of a higher court or boards are referred to as common law, case law, or precedents.

Statutory law can be further categorized into civil law and criminal law based on their association with individuals, groups, and the state [46]. Civil law has to do with issues between and among individuals and organizations [37,44] and includes contract law, employment law, and tort law. Tort law enables individuals to settle their issues in court on personal, physical, or financial matters. In such matters, restitution is settled in civil courts without the state's involvement. At the same time, criminal law is enforced and prosecuted by the state and deals with violations that are harmful to society. In criminal law, the state acts on behalf of the plaintiff to obtain retribution for the

plaintiff. For instance, in some jurisdictions, health care professionals are punished for criminal behavior if they disclose their clients' information without good causes [47].

Security Policies, Standards, Guidelines, Procedures, and Practices

In controlling information security in a health care organization, information security governance is usually adopted by organizations that use policies, standards, guidelines, procedures, and practices [37]. In various health care units, organizational policies function as the laws. Therefore, information security policies are required to be made and implemented to ensure that they are complete and appropriate and should be able to fairly apply to everyone in the workplace [37]. As laws, organizational policies must be completed with retributions, judicial practices, and sanctions to require compliance.

However, the variance between law and policy is that although ignorance of state law is not an excuse, ignorance of an organizational policy is an acceptable defense [37]. Therefore, to have an enforceable policy in an organization, the policy must be disseminated, reviewed, comprehended, complied with, and uniformly enforceable to all staff in the organization.

Information security policy directs how issues should be addressed and how IT resources should be used, but it does not define the proper operation or functioning of the system. How a software program should function is specified in the standard procedures and practices of the users' manuals and systems documentation.

Policies specify acceptable and unacceptable information security practices at the organizational level and outline rules with the aim of protecting the organization's information assets [48,49]. There are 3 types of information security policies [37,48,49]: the enterprise or organizational information security policy (EISP), issue-specific security policy (ISSP), and system-specific policy.

EISP is a general information security policy that contains the overall strategic direction, scope, and goal of the organizational information needs at a high level. In addition, EISP defines the legal requirements, outlines the responsibilities of the system administration of information security policy maintenance and practices, and outlines the responsibilities of the users.

While EISP is aimed toward addressing a broad scope of the entire organization's security issues, ISSP provides detailed guidelines pertaining to the use of specific resources, such as processor or technology, for all members or users to comply with [37,48,49]. Some of these instances include email use, internet use, security measures against viruses, bringing your own devices, use of cloud computing, home use of company-owned devices, data retention policy, and media disposal policy.

EISP and ISSP still provide information security rules at a more general level when focusing on specific systems in the organization, and they do not address security issues concerning specific systems. This gap has been filled by system-specific policy, which provides adequate information or direction in complying with the security of specific systems in the organization [37,48-50]. System-specific policy focuses on one system such as EHR systems. In this context, system-specific policy, for instance, can be used to define the access control policy of the EHR system. Therefore, system-specific policy varies from system to system and is defined by management.

All these types of policies are effectively implemented using tools such as standards, guidelines, procedures, and practices [37,48-50]. Specifics that enable employees to comply with a security policy are known as information security standards, whereas guidelines are recommendations or examples provided to help users comply with a security policy. Practices are also recommendations or examples that are adopted from a reputable organization to help in complying with a policy, whereas procedures are step-by-step instructions users are to follow to accomplish a particular task in fulfillment of the security policy.

Scope, Contribution, and Research Questions

In assessing the information security practice of health care staff, there is a need to determine the state of security practice in the health care organization and compare it to a benchmark to determine the level of compliance with information security of the health care staff of that organization. Therefore, we opine that the legal aspect of the information security requirement is necessary to serve as the yardstick in measuring health care staff's security practices. A major reason is that a violation of any legal requirement has a huge consequence on the offending individual or company, including heavy fines, imprisonment, and payments of restitution. Therefore, aiming to comply with the legal aspect of information security requirements by using it as a yardstick will lead to unconscious compliance with the laws of that jurisdiction.

Information security requirement does not only involve legal requirements but also includes ethical security considerations of information system users [37]. However, this study focuses on the legal requirements of information security in health care such as constitutional law, statutory law, regulations, case law, and chatters. Other legal sources considered in this study include information security policies and their supported instruments, such as information security standards, guidelines, and practices.

This study seeks to address issues of incomprehensiveness in considering the legal requirements for analyzing health care security practices in Norway, Ghana, and Indonesia. This has become necessary, as there have been initiatives to measure the security practices of health care staff in these countries in various projects [16]. The problem is that there is no comprehensive and state-of-the-art study of the legal requirements of information security that can serve as a baseline for assessing security practices in health care. A random and nonsystematic approach to adopting legal information security requirements in real studies could undermine the quality of the study if the baseline for the measurement is wrong. Therefore, we adopted a comprehensive, systematic scoping review approach to establish our baseline legal requirements for future imperial studies and further developed a framework to guide future related studies.

Methods

Overview

A scoping review was conducted to explore information security and privacy requirement in health care following the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) statement [1].

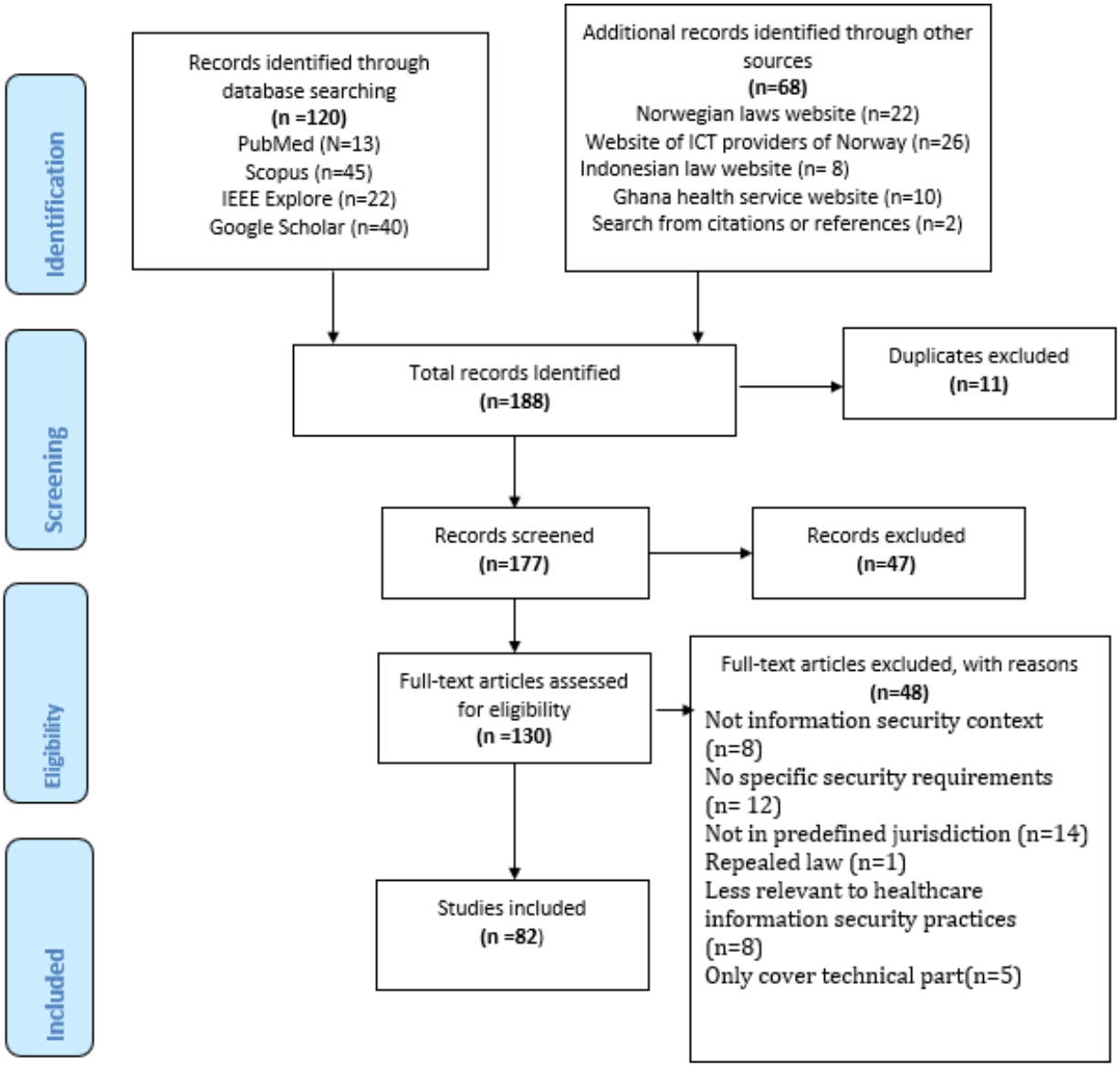
Various types of systematic studies include systematic mapping, scoping, and systematic literature review [51-54]. Systematic mapping studies rely on general research questions aimed at determining research trends or state-of-the-art studies as opposed to a scoping method that is based on the categorization of the study into topics [51,52], whereas systematic literature review aims to accumulate data with more specific research focus and synthesis. Therefore, in this study, a systematic scoping study was adapted. This section describes the methods and designs that were used to review the literature and conduct this study.

Search Strategy

The goal of the search is to search broadly to obtain comprehensive laws or rules termed here as *security requirements*. Therefore, we did not want to limit the identification of these requirements by searching through only scientifically published papers. This led to the inclusion of both scientific studies and other sources, shown in Figure 1. Therefore, the inclusion of scientific studies was intended to extract relevant laws. The sources of the security requirement were identified by conducting a literature search through several databases as follows: PubMed, Google Scholar, IEEE Xplore, and Scopus.

While reading the articles to identify the legal requirement, other relevant articles which were cited or referenced were also added in the studies and accounted for on the PRISMA diagram as *search from citations or references* as shown in Figure 1.

Figure 1. PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) diagram. ICT: information and communication technology.



In addition, we also performed manual searching through several law databases by reading all the laws under the health care category and selecting the relevant ones. The databases used were as follows:

- Legal, regulations, and directive databases for EU and Norway [55]
- Legal, regulations, directive, policy, and code of conduct databases for hospitals in Norway [55]
- Legal, regulations, and directive databases for Indonesia [56]
- Legal, regulations, directive, policy, and code of conduct databases for hospitals in Indonesia [57]
- Legal, regulations, and directive databases for Ghana [58]
- Legal, regulations, directive, policy, and code of conduct databases for hospitals in Ghana [59,60]

The literature search was conducted without time restrictions. For searching the scientific paper databases, we used the following keywords in the search string: (*Information security* OR *Cyber security* OR *Computer security*) AND *Healthcare* AND *Information system* AND (*law* OR *Regulation* OR *Directive* OR *Policy* OR *Standard*) AND (*European Union* OR *Norway* OR *Indonesia* OR *Ghana*). Meanwhile, for searching through law databases, we did not use any keywords. Instead, we read all the laws under the health care category and selected the relevant ones. The literature search was conducted from December 2020 to February 2021.

Eligibility Criteria

All studies involving laws, regulations, directives, policies, best practices, and standards in the health care security and privacy context in Norway and EU, Indonesia, or Ghana were eligible for review. The publication language was limited to English. Papers that did not meet the eligibility criteria or only described the technical part of security and privacy in health care without relying on legal or security governance requirements were excluded from the review. Only studies that describe the legal aspect of health care security and privacy in Norway and EU, Indonesia, or Ghana were eligible for review. Owing to the lack of resources, we focused on English scientific papers but only translated the identified local laws, which were relatively few.

Study Selection and Data Extraction

A PRISMA flow diagram of the literature search process is shown in Figure 1. The titles and abstracts of articles from the databases were screened for eligibility. Then, all articles that passed the first screening entered full-text screening and data extraction. Data extraction was performed using a predesigned data collection form. For each qualified article, data on study characteristics, such as the first author and publication year, were extracted. Furthermore, we extracted information consisting of the article information, name and type of the legal document, legal document authority, security requirement, privacy requirement, health care user category, domain, responsibility level, security, and privacy requirement, which is referred to in this study as data categorization, as shown in Table 1.

Table 1. Data extraction field description.

No	Category	Description
1	Paper information	Name, authors, and publication year of the paper
2	Legal document name	The name of the legal documents found in the paper
3	Legal document type	This defines the category of law such as regulation, constitutional law, directive, statutory law, policy, and guidelines found in the paper
4	Legal document jurisdiction	The country in which the legal document applies
5	Security requirement	The requirement about information security found in the legal document
6	Privacy requirement	These are the measures or rules that seek to protect the dignity of patients. These include the right to consent and the right to be forgotten to preserve the privacy of an individual
7	Health care user category	The category of users with the primary responsibility to implement or comply with the related requirement. These include management, end users, and all users. The management category includes top management such as CEOs[a], directors, managers, and officers with the responsibility of implementing and complying with the privacy and security requirement
8	Responsibility level	The user level is responsible for the requirement, and this defines the type of user category who is to take action to observe, enforce, implement, or comply with the security measure. Examples include management, end users, and all users. The management includes top-level staff such as the CEOs, directors, managers, and officers who are responsible for implementing and observing health care security practices. End users include all employees, consultants, suppliers, and others with access to the health system. All user-level categories include responsibilities that are concerned by management and end users
9	Security category	This refers to the security domain (eg, access control, security governance, access logs, and encryption) of the requirement
10	Privacy category	This refers to the privacy domain, such as consent and right to privacy, of the requirement and data protection

[a]CEO: chief executive officer.

Data Categorization

Data categorization was developed based on the objective and thorough literature reviews and author discussions. The categories were defined exclusively to assess, analyze, and evaluate the study, as shown in Table 1.

Literature Evaluation

After data extraction, all researchers independently checked the extracted data. A discussion between all researchers was held to resolve all discrepancies. The selected articles were assessed, analyzed, and evaluated based on the defined categories in Table 1 to evaluate the state-of-the-art security and privacy requirements. The percentages of the attributes of the categories were calculated based on the total number of counts (n) of each type of attribute. Some studies used multiple categories; therefore, the number of counts of these categories exceeded the total number of articles on the requirements presented in the study.

After data extraction, all researchers independently checked the extracted data. A discussion among all researchers was held to resolve any discrepancies.

Results

Study Selection

A total of 188 articles were identified through the literature search of the 10 databases. After duplicate deletion, 94.1% (177/188) of the articles remained for the next step. Titles and abstracts screening yielded in the exclusion of 26.6% (47/177) of the articles for not meeting eligibility criteria. Hence, 73.4% (130/177) of the articles entered the full-text screening for eligibility. After the second screening, 36.9% (48/130) of the articles were eliminated from the review for various reasons, with the main reasons being not in predefined jurisdictions (14/48, 29%) and not having specific information security and privacy requirements (12/48, 25%). To retrieve the list of excluded papers, a request can be sent to the authors. Finally, of the 130 articles in the full-text reading stage, 82 (63.1%) met the eligibility criteria and were included for review, as shown in Figure 1.

Study Characteristics

Of the 82 articles, 36 (44%) were scientific studies and the others were legal documents. A total of 75 unique legal documents were identified, including case law (n=1, 1%), charter (n=1, 1%), code of conduct (n=1, 1%), directives (n=7, 9%), guidelines (n=4, 5%), policies (n=27, 36%), recommendation (n=1, 1%), regulations (n=13, 17%), standards (n=4, 5%), and statutory law (n=16, 21%), as shown in Multimedia Appendix 1 and Table 2. The distribution of law jurisdictions is depicted in Multimedia Appendix 2 and Table 3. Of the 75 legal documents, 35 (47%) are from Norway, 9 (12%) from Ghana, 11 (15%) from Indonesia, and 17 (23%) from the EU and 3 (4%) are international laws, as presented in Table 4, Table 5, Table 6, Table 7, and Table 8, respectively. In total, 253 requirements were extracted from the legal documents, consisting of 173 (68.4%) security requirements and 80 (31.6%) privacy requirements, as shown in Multimedia Appendix 3. As shown in Multimedia Appendix 4, of the 173 security requirements, 143 (82.7%) are the management's responsibility to fulfill, 1 (0.6%) is the end users' responsibility, and 29 (16.8%) are all users' (management and end users) responsibility. Meanwhile, as shown in Multimedia Appendix 4, of the 80 privacy requirements, 70 (88%) need to be fulfilled by the management, 1 (1%) is the end users' responsibility, and 9 (11%) are all users' responsibility. Legal requirements are shown in Table 9; in addition, we classified the requirements into several categories, as shown in Tables 10 and 11.

Table 2. Types of laws (n=75).

No	Type of law	Count, n (%)
1	Case law	1 (1)
2	Charter	1 (1)
3	Code of conduct	1 (1)
4	Directive	7 (9)
5	Guideline	4 (5)
6	Policy	27 (36)
7	Recommendation	1 (1)
8	Regulation	13 (17)
9	Standard	4 (5)
10	Statutory law	16 (21)

Table 3. Count of laws based on jurisdiction (n=75).

No	Country	Count of laws, n (%)
1	Norway	35 (47)
2	Ghana	9 (12)
11	Indonesia	11 (15)
4	European Union	17 (23)
5	International	3 (4)

Table 4. Legal documents from Norway.

No	Legal document	Type
1	Code of conduct for information security and data protection in the health care and care services sector version 6.0 [61]	Code of conduct
2	Ministry of Government Administration, Reform and Church Affairs' requirements specification for PKI[a] for the public sector [62]	Guidelines
3	General principle to regional control system for information security and privacy [63]	Policy
4	Safety regulator legislation applicable to the enterprise group [63]	Policy
5	Organization of information security work [63]	Policy
6	Safety goals and level for acceptable risk of information security [63]	Policy
7	Security strategy [63]	Policy
8	Security instructions (signed version) [63]	Policy
9	ICT[b] services and information security for medical devices [63]	Policy
10	Requirements specification—ICT services and information security for MTU[c] [63]	Policy
11	Security principles and requirements for ICT infrastructure and applications [63]	Policy
12	Anonymization of health and personal information [63]	Policy
13	Use of data processor—treatment of personal information at other legal entity [63]	Policy
14	Use of email and fax [63]	Policy
15	Use of mobile phones [63]	Policy
16	Basis for posting in journal [63]	Policy
17	Storage, archiving, and deletion of health and personal information [63]	Policy
18	Crypto policy [63]	Policy
19	Password policy for the health trusts in Health South-East	Policy
20	Guidance for approval of data processing from secure third countries [63]	Policy
21	Requirements for coded research data	Policy
22	Use of email, fax, and SMS text messaging for communication with and about patients [63]	Policy
23	Regional policy for publishing and public services and DMZ[d] [63]	Policy
24	Description of identification procedure in Health South-East [63]	Policy
25	Use of logs for administrative purposes	Policy
26	Internal control information security [63]	Policy
27	Logging of activity and control of logs [63]	Policy
28	Regional security policy for cloud services [63]	Policy
29	Regulations relating to the Processing of Personal Data [64]	Regulation
30	Norwegian Personal Health Data Filing System Act [16,65,66]	Statutory law
31	Act relating to Patients' Rights	Statutory law
32	Act relating to the Processing of Personal Data [18]	Statutory law
33	Health Care Personnel Act [67,68]	Statutory law
34	Health Research Act [16]	Statutory law
35	Act relating to Public Supervision of the Health Service	Statutory law

[a]PKI: public key infrastructure.

[b]ICT: information and communication technology.

[c]MTU: medical technical equipment.

[d]DMZ: demilitarized zone.

Table 5. Legal documents from Ghana.

No	Legal document	Type
1	The GHS[a] Patient's Charter	Charter
2	The Medical Profession Regulation and the Infectious Diseases, Cap 78	Regulation
3	The Ghana National Health Insurance Regulations of 2004	Regulation
4	Data Protection Act of Ghana 843	Statutory law
5	The Republic of Ghana's Constitution	Statutory law
6	The National Identification Authority Act 707	Statutory law
7	Cybersecurity Act of Ghana 2020	Statutory law
8	Guidelines for the Use of CCTV[b] in GHS Facilities	Guidelines
9	Health sector ICT[c] policy and strategy	Policy

[a]GHS: Ghana Health Services.

[b]CCTV: closed-circuit television.

[c]ICT: information and communication technology.

Table 6. Legal documents from Indonesia.

No	Legal document	Type
1	Regulation of the Minister of Health of the Republic of Indonesia Number 269/2008 on Medical Record	Regulation
2	Undang-Undang Republik Indonesia Nomor 29 Tahun 2004 Tentang Praktik Kedokteran	Statutory law
3	Undang-Undang No. 36/2009 Pasal 103 ayat 1	Statutory law
4	Peraturan Menteri Kesehatan Republik Indonesia Nomor 55 Tahun 2013 Tentang Penyelenggaraan Pekerjaan Perekam Medis	Regulation
5	Undang-Undang Republik Indonesia No 36 Tahun 2014 Tentang Tenaga Kesehatan	Statutory law
6	Peraturan Pemerintah Republik Indonesia Nomor 46 Tahun 2014 Tentang Sistem Informasi Kesehatan	Regulation
7	UU 36 Tahun 2009 Tentang Kesehatan	Statutory law
8	Peraturan Menteri Kesehatan Republik Indonesia Nomor 36 Tahun 2012 Tentang Rahasia Kedokteran	Regulation
9	Undang-Undang Republik Indonesia Nomor 44 Tahun 2009 Tentang Rumah Sakit	Statutory law
10	Peraturan Menteri Kesehatan Republik Indonesia Nomor 82 Tahun 2013 Tentang Sistem Informasi Manajemen Rumah Sakit	Regulation
11	Peraturan Menteri Kesehatan Republik Indonesia Nomor 77 Tahun 2016 Tentang Sistem Klasifikasi Keamanan Dan Akses Arsip Dinamis Di Lingkungan Kementerian Kesehatan	Regulation

Table 7. Legal documents from the EU[a].

No	Legal document	Type
1	Penal Code [41,69]	Case law
2	Directive 95/46/EC	Directive [70,71]
3	NIS[b] Directive	Directive [72]
4	The directive on patients' rights in cross-border health care (Directive 2011/24)	Directive [73]
5	Directive 2009/136/EC amending Directive 2002/58/EC (Privacy Directive)	Directive
6	Data Protection and Privacy in Electronic Communications—e-Privacy Directive (it replaces Directive 97/66/EC) [74]	Directive
7	Directive 99/93/EC	Directive [75]
8	The Patients' Rights Directive (2011/24/EU) [73]	Directive
9	Recommendation CM/Rec(2019)2 of the Committee of Ministers to member states on the protection of health-related data [76]	Guidelines
10	GCP[c]	Guidelines [71]
11	Recommendation No. R (97) 5 of the Committee of Ministers to Member States on the Protection of Medical Data	Recommendation [77]
12	GDPR[d] [16,78-83]	Regulation
13	EU regulation and compliance of national and transborder data flows	Regulation
14	Medical Device Regulation 2017/745 of EU [41]	Regulation
15	Regulation 2014/910 (the *eIDAS*[e]*Regulation*) [78]	Regulation
16	A European standardization group for Security and Privacy of Medical Informatics (CEN TC 251/WG6[f]) [84,85]	Standard
17	GEHR[g]/CEN[h] standards ENV[i] 12265 and ENV 13606 [86,87]	Standard

[a]EU: European Union.
[b]NIS: Network and Information Security.
[c]GCP: Good Clinical Practice.
[d]GDPR: General Data Protection Regulation.
[e]eIDAS: electronic identification and trust services.
[f]CEN TC 251/WG6: Commission for European Normalization Technical Committee/Working Group 6.
[g]GEHR: Good European Health Record.
[h]CEN: European Committee for Standardization.
[i]ENV: Electronic Healthcare Record Communication for the exchange of electronic health records.

Table 8. International legal documents.

No	Legal document	Type
1	ISO[a] 27001	Standard
2	IEC[b] 80001-1:2010	Standard
3	The Universal Declaration of Human Rights	Statutory law

[a]ISO: International Organization for Standardization.
[b]IEC: International Electrotechnical Commission.

Table 9. Legal requirement used in the study.

No	Requirement	Count, n (%)	Reference
1	GDPR[a]	13 (21.67)	[16,78-82,88-94]
2	Directive 95/46/EC	10 (16.67)	[65,70,71,74,75,95-99]
3	Norwegian Personal Health Data Filing System Act	3 (5)	[16,100,101]
4	Act relating to Patients' Rights	2 (3.33)	[16,101]
5	Act relating to the Processing of Personal Data	2 (3.33)	[16,101]
6	Directive 2011/24/EU on patients' rights in cross-border health care	2 (3.33)	[73,90]
7	Health Care Personnel Act	2 (3.33)	[16,101]
8	Act relating to Public Supervision of the Health Service	1 (1.67)	[101]
9	Data protection and privacy in electronic communications—e-Privacy Directive	1 (1.67)	[75]
10	Directive 2002/58/EC	1 (1.67)	[65]
11	Directive 2009/136/EC	1 (1.67)	[74]
12	Directive 99/93/EC	1 (1.67)	[75]
13	EU regulation and compliance of national and transborder data flows	1 (1.67)	[89]
14	GEHR[b]/CEN[c] standards ENV[d] 12265 and ENV 13606	1 (1.67)	[102]
15	Good Clinical Practice	1 (1.67)	[71]
16	Health Research Act	1 (1.67)	[16]
17	IEC[e] 80001-1:2010	1 (1.67)	[97]
18	ISO[f] 27001	1 (1.67)	[89]
19	Medical Device Regulation 2017/745 of EU	1 (1.67)	[41]
20	Ministry Of Government Administration, Reform and Church affairs' Requirements specification for PKI[g] for the public sector	1 (1.67)	[65]
21	Penal Code	1 (1.67)	[41]
22	Recommendation CM/Rec(2019)2 of the Committee of Ministers to member States on the protection of health-related data	1 (1.67)	[76]
23	Recommendation No. R (97) 5 of the Committee of Ministers to Member States on the Protection of Medical Data	1 (1.67)	[77]
24	Regulation 2014/910 (the "eIDAS Regulation")	1 (1.67)	[103]
25	Regulation of the Minister of Health of the Republic of Indonesia Number 269/2008 on Medical Record	1 (1.67)	[83]
26	Regulations relating to the Processing of Personal Data	1 (1.67)	[101]
27	The Ghana Health Services Patient's Charter	1 (1.67)	[104]
28	The Ghana National Health Insurance Regulations of 2004	1 (1.67)	[104]
29	The National Identification Authority Act 707	1 (1.67)	[104]
30	The Republic of Ghana's constitution	1 (1.67)	[104]
31	The Universal Declaration of Human Rights	1 (1.67)	[104]
32	UNDANG-UNDANG No.36/2009 and Pasal 103 ayat 1	1 (1.67)	[105]
33	Undang-undang republik, Indonesia nomor 29, Tahun 2004 tentang, Praktik kedokteran	1 (1.67)	[106]

[a]GDPR: General Data Protection Regulation.

[b]GEHR: Good European Health Record.

[c]CEN: European Committee for Standardization.

[d]ENV: Electronic Healthcare Record Communication for the exchange of electronic health records.

[e]IEC: International Electrotechnical Commission.

[f]ISO: International Organization for Standardization.

[f]PKI: public key infrastructure.

Table 10. Security requirement category distribution (n=173).

No	Security requirement category	Count, n (%)
1	Data processing	14 (8.1)
2	Data protection officer	14 (8.1)
3	Right of access	13 (7.5)
4	Security by design	13 (7.5)
5	Access control	12 (6.9)
6	Email processing	10 (5.8)
7	Logs	9 (5.2)
8	Password	7 (4.1)
9	Encryption	6 (3.5)
10	Health data storage	6 (3.5)
11	Mobile phone processing	4 (2.3)
12	Privacy by design	4 (2.3)
13	CIA[a] measures	3 (1.7)
14	Data controller	3 (1.7)
15	Personal data	3 (1.7)
16	Third countries	3 (1.7)
17	Data protection	3 (1.7)
18	Backup	2 (1.2)
19	Documentation	2 (1.2)
20	Electronic signature	2 (1.2)
21	Establish security governance	2 (1.2)
22	Least privileges	2 (1.2)
23	Medical devices	2 (1.2)
24	Right to be informed	2 (1.2)
25	Risk management	2 (1.2)
26	Security governance	2 (1.2)
27	Third parties	2 (1.2)
28	Data breach	2 (1.2)
29	Use of ISO[b] standards	2 (1.2)
30	Consent	1 (0.6)
31	Data aggregation	1 (0.6)
32	Incident reporting	1 (0.6)
33	Internal control	1 (0.6)
34	Data transfer to non-EU[c] countries	1 (0.6)
35	Deletion of health data	1 (0.6)
36	Establish security policies	1 (0.6)
37	Health care data hosting	1 (0.6)
38	Identity	1 (0.6)
39	Internal and external threats	1 (0.6)
40	Mobile devices	1 (0.6)
41	Monitoring of NIS[d] Directives	1 (0.6)

No	Security requirement category	Count, n (%)
42	Patients from other member states	1 (0.6)
43	Physical security	1 (0.6)
44	Professional secrecy	1 (0.6)
45	Protection against security incidents	1 (0.6)
46	Providing information to patients from a member state	1 (0.6)
47	Risk assessment	1 (0.6)
48	Risk mitigation	1 (0.6)
49	Sanction	1 (0.6)
50	Technological security measures	1 (0.6)
51	Training and education	1 (0.6)

[a]CIA: confidentiality, integrity, and availability.

[b]ISO: International Organization for Standardization.

[c]EU: European Union.

[d]NIS: Network and Information Security.

Table 11. Privacy requirement category distribution (n=80).

No	Privacy requirement category	Count, n (%)
1	Consent	13 (16)
2	Disclosure of health data	12 (15)
3	Privacy by design	8 (10)
4	Right to privacy	8 (10)
5	Right of access	7 (9)
6	Data protection	6 (8)
7	Data processing	3 (4)
8	Personal data	3 (4)
9	Punitive measures of security and privacy violation	3 (4)
10	How to record health data	2 (3)
11	Privacy rights	2 (3)
12	Storage of health records	2 (3)
13	CIA[a] measures	1 (1)
14	Data collection purpose	1 (1)
15	Deletion of health data	1 (1)
16	Electronic signatures	1 (1)
17	Mobile phone processing	1 (1)
18	Professional secrecy	1 (1)
19	Purpose of health care data processing	1 (1)
20	Right to be forgotten	1 (1)
21	Right to object	1 (1)
22	Termination of consent	1 (1)
23	Third parties	1 (1)

[a]CIA: confidentiality, integrity, and availability.

Findings

The following sections present and describe a series of findings, including law by type, law by jurisdiction, requirement by type, requirement by responsibility level, and identified security and privacy requirements and their categorizations.

Law by Type

The types of laws identified in this work are presented in Multimedia Appendix 1 and Table 2. A total of 75 legal requirements were identified in this review. The most common types of laws that were used are policies (27/75, 36%), statutory law (16/75, 21%), regulations (13/75, 17%), directive (7/75, 9%), standards (4/75, 5%), and guidelines (4/75, 5%), but recommendation, code of conduct, charter, and case law accounted for the lowest proportion. It is worth noting that the 27 policies were all collected from information security policy documents of the health care facilities of the southeast region in Norway as their internal control measures of information security and privacy measures.

Law by Jurisdiction

The specific legal documents from Norway, Ghana, Indonesia, the EU level, and the international level are listed in Table 4, Table 5, Table 6, Table 7, and Table 8, respectively, and Norway has almost half (36/75, 48%) of the laws pertaining to information security and privacy, which were identified in this work and shown in Multimedia Appendix 2 and Table 4. This was followed by the EU (17/75, 23%). The southeast health region in Norway developed approximately 27 policies, which also accounted for the larger proportion of the laws in Norway than that in other countries, as shown in the bar chart of the law jurisdiction distribution in Multimedia Appendix 2.

Identified Legal Requirement

Of the 82 requirement sources, 36 (44%) were articles that considered at least one of the identified requirements, whereas the others were legal documents. In total, 75 unique legal documents were identified, and 33 legal documents were identified to have been considered in the papers as shown in Table 9.

Moreover, as shown in Table 9, among all the legal documents, the GDPR (13/60, 22%) is the most common regulation that was used in the articles that relied on legal requirements, followed by Directive 95/46/EC (10/60, 17%), which has already been repealed and replaced by the GDPR. Some acts from Norway, as well as directive from the EU, have also been referred to several times, such as the Norwegian Personal Health Data Filing System Act (3/60, 5%), Act relating to Patients' Rights (2/60, 3%), Act relating to the Processing of Personal Data (2/60, 3%), Directive 2011/24/EU on patients' rights in cross-border health care (2/60, 3%), and Health Care Personnel Act (2/60, 3%).

Security and Privacy Requirements

According to Multimedia Appendix 3, most legal requirements extracted are security requirements (173/253, 68.4%), whereas the rest are privacy requirements (80/253, 31.6%).

Requirements by Responsibility Level

The identified responsibility level of users includes management, end users, and all users. The management level has more security and privacy responsibility and stipulation than the end users. As shown in Multimedia Appendices 4 and 5, documents list the security and privacy requirements only for end users.

Security Category

The security requirements extracted from all the studies cover various aspects, such as data processing, data protection officer, right of access, security by design, access control, email processing, logs, and password, as shown in Table 10. In this study, security requirements relating to data processing (14/173, 8.1%), data protection officer (14/173, 8.1%), right of access (13/173, 7.5%), security by design (13/173, 7.5%), access control (12/173, 6.9%), email processing (10/173, 5.8%), logs (9/173, 5.2%), password (7/173, 4%), encryption (6/173, 3.5%), and health data storage (6/173, 3.5%) were identified to be commonly adopted in the legal requirements, as shown in Table 10.

Privacy Category

The privacy requirement categories that were realized in this work are shown in Table 11.

The areas that were mostly required by the legal instruments are consent (13/80, 16%), disclosure of health data (12/80, 15%), privacy by design (8/80, 10%), right to privacy (8/80, 10%), right of access (7/80, 9%), data protection (6/80, 8%), data processing (3/80, 4%) and punitive measures (3/80, 4%).

Discussion

Principal Findings

The main purpose of this study is to comprehensively identify, assess, and synthesize the appropriate legal requirements and security governance tools of information security to serve as a yardstick for modeling and analyzing health care security practices. A scoping review of these requirements was conducted to include various categories, as presented in Table 1. The most used categories identified in this study are listed in Table 12. For instance, among various types of laws that were identified in this study (Multimedia Appendix 1), the most used types of law are the policies, statutory law, regulations, and directives, as shown in Table 12.

Table 12. Summary of the most used categories.

No	Category	Most used
1	Type of law	Policy, statutory law, regulation, and directive
2	Jurisdiction	Norway and European Union
3	Requirement type	Security requirement
4	Responsibility level	Management
5	Security requirement category	Data processing, data protection officer, right of access, security by design, access control, email processing, logs, password, encryption, and health data storage
6	Privacy requirement category	Consent, disclosure of health data, privacy by design, right of access, and data protection

Security Requirement Responsibility Level Distribution

As defined in Table 1, the responsibility level of the requirement is the level of user categories that take action to observe, enforce, implement, or comply with the security measure. Examples include management, end users, and all users. Management includes top-level staff, such as the chief executive officers (CEOs), directors, managers, and officers, who are responsible for implementing and observing health care security practices. All users include all employees, consultants, suppliers, and others with access to the health care system and with the responsibility to comply with security and privacy requirements. The end users' level includes only those user categories that have access to the health care system with the purpose of accessing and performing specified tasks. Such users include nurses, doctors, pharmacies, record management, and patients' EHRs for therapeutic reasons.

As shown in Multimedia Appendices 4 and 5, the management level was identified to be mostly responsible for information security and privacy requirements, followed by *all users* This implies that in most information security and privacy requirement categories such as access control, password management, consent, and incident reporting, as outlined in Tables 10 and Tables 11, the management level has more responsibility. The management user category includes the CEO, chief information officer, chief information security officer, all directors, and all managers responsible for formulating, designing, and implementing privacy and security policies for compliance [37]. The top-management user category, such as the CEO, chief information officer, and chief information security officer, is responsible for coming out with the information security governance requirement based on prevailing laws pertaining to information security. Directors and managers then ensure that the policies, guidelines, standards, and best practices are appropriately designed and implemented. They also need to create awareness and ensure that all personnel are adequately trained in these requirements. Essentially, impact assessments such as privacy and security are also conducted by the management. To ensure compliance, these policies need to be monitored and evaluated. Management, therefore, has a major proportion of responsibility because of all these broad activities being performed toward enhancing security.

In addition, the *all users* category consists of all employees such as the management level and end users including temporal workers and contractors who have the responsibility to enforce and comply with the requirements. The *all users* category of the level of responsibility involves requirements that need the attention of both management and end users. For instance, access control requires management to incorporate it into the development of systems. However, end users must also be responsible for their access control–related behaviors, including password management. The *end users* level includes those health care workers who are given access to a system based on their need to use that system for therapeutic purposes [61]. Examples include the end users of an EHR system. This group of users is mostly large in number but does not have an enormous number of responsibilities as compared with the management group, as shown in Multimedia Appendices 4 and 5.

Requirement Types (Security and Privacy)

A total of 2 kinds of measures were extracted from the legal documents in this study, namely, security and privacy requirements. The legal documents contain at least one of the two kinds of measures: privacy, security, or both. Furthermore, >1 requirement was found in some of the sources of the legal documents, and this resulted in more legal requirements compared with the number of identified sources, as shown in Table 9. After the identification and extraction process, 173 security requirements and 80 privacy requirements were identified, as shown in Multimedia Appendix 3. The findings indicate that there are more security requirements than privacy requirements identified in this study. The main reason is that many policies in Norway describe security requirements, as shown in Multimedia Appendix 1 and Table 4. Most of these policies were developed to address security requirements such as email use, crypto policy, password policy, and access control logging, which resulted in the number of security requirements surpassing the number of privacy requirements.

Law by Type

From Table 2, a total of 10 types of laws were identified in this study, including case law, charter, code of conduct, directives, guidelines, policies, and recommendations. Others include regulations, standards, and statutory law, of which the most used type of laws are policies (27/75, 36%), statutory law (16/75, 21%), regulations (13/75, 17%), directives (7/75, 9%), standards (4/75, 5%), and guidelines (4/75, 5%), as shown in Table 12. The standards that were identified are only from the EU and international levels with which Norway is bound to comply. In addition, none of the countries has standards as far as what we have collected. This could be due to the level of maturity of IT development in health care in each country. Finally, only a few

documents were categorized into case law, charter, recommendation, and code of conduct.

One of the most influential legal documents that covers almost every general aspect, as mentioned is the GDPR, as shown in Table 9, to which data controllers, data processors, and data subjects need to comply. It is worth mentioning that pursuant to the GDPR, "a data controller is a legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data," whereas a data processor means a legal person, public authority, agency, or other body that processes personal data on behalf of the controller [107]. A data subject is any identified or identifiable person whose data are processed by the data processor. ISO 27001 provides a framework for managing security issues in health care including the measures covering information security policies, organization of information security, human resource security, asset management, media handling, access control, cryptography, physical and environmental security, operational security, communications security, system acquisition, development and maintenance, supplier relationships, and information security incident management through ISO 27799 [14]. Health care has extended needs in these areas, which is why ISO 27799 was developed for use in conjunction with ISO 27001. This provides room to address the security and privacy requirements that have not been fully covered in ISO 27001.

The widely used model, namely, the CIA triad, which is the balanced protection of CIA of data [108], is the foundation and basis of many laws and regulations including the GDPR, Recommendation CM/Rec (2019)2 of the Committee of Ministers to member states on the protection of health-related data, Directive 2009/136/EC amending Directive 2002/58/EC (Privacy Directive), Medical Device Regulation 2017/745 of EU, and Regulation 2014/910 (the *eIDAS Regulation*) at the EU level, as well as the Norwegian Personal Health Data Filing System Act, Act relating to the Processing of Personal Data, and Act relating to Patients' Rights as shown in Table 9.

Law by Country

The legal documents were identified from 3 countries: Norway, Ghana, and Indonesia. Norway has the most legal documents for this study at 47% (35/75), whereas Ghana and Indonesia provide only 12% (9/75) and 15% (11/75) of the documents, respectively. The main reason Norway has far more relevant legal documents than the other 2 countries is that Norway has many policies that describe specific details on security and privacy requirements. Furthermore, we also identified some legal documents from the EU (17/75, 23%) and some international laws (3/75, 4%). Most EU documents are directives and regulations that should be adopted by EU members, including Norway. Meanwhile, the international laws include 2 ISOs and 1 statutory law, which should be adopted by all countries.

Security and Privacy Policies in Norway, Ghana, and Indonesia

The privacy requirements in this study focused on patients' consent to the processing of their personal data and the processing and storage of medical records, as shown in Table 11. The requirements for processing personal information include that the data subjects must consent to the use of their data captured and collected in the first place [109]. Patients have the right to object to the processing of their personal health data (Norwegian Personal Health Data Filing System Act [110]) and are entitled to their information not to be disclosed to a third party without their consent [111]. The Health Research Act in Norway stipulates that more detailed requirements regarding consent must be informed, voluntary, express, and documented [112]. As for the processing of medical records, it is specifically stated in Indonesian laws that the medical data should be kept confidential by the management level to protect the patients and hospitals must protect archived physical records [106].

Security and privacy requirements in Norway, Ghana, and Indonesia all contain laws to protect the CIA of health care data. As shown in Multimedia Appendix 2, almost 46% (35/75) of the laws were developed by Norway, and most of the information security and privacy policies were developed by Norwegian health care facilities to meet the CIA requirements of health care data and information, as compared with Indonesia and Ghana. The variance could arise from various reasons, including advancement in the application of ICT in health care between European and African countries [113,114], and culturally related factors among the 3 countries. Norway is one of the countries in Europe that might have been more advanced in the use of ICT in health care than Ghana and Indonesia and have therefore adopted more legal requirements than Ghana and Indonesia. In addition, Norway is affiliated with the EU through the European Economic Area and is therefore bound to adopt the legal requirements, such as the GDPR and Network and Information Security Directive. In addition, EU countries, including Norway, are concerned with privacy [114]. This may have been one of the reasons for the adoption of more legal requirements to comprehensively enhance privacy and security measures.

Framework

On the basis of our findings on security requirements, we present a framework in this section to provide directions for future imperial research in health care security practices. The framework consists of comprehensive security practices (drawn from the security requirements) and categories of health care staff in health care information security practices. It also includes analysis methods, the actual measure of security practices in a typical hospital, a gap or security failures, and an incentivization module, as shown in Figures 2 and 3 and as described as follows:

- Comprehensive security requirements: these include both privacy and security requirements that have been identified in the legal and security governance requirements in this study, as shown in Tables 10 and 11. These requirements are to be observed by all categories of health care workers. These requirements serve as the benchmark to be complied with by all categories of health care staff.
- Categories of users: these include management, all users, and the end users of a typical hospital. These categories of

users must observe the required security practices at their respective levels, as shown in Figure 2.

- Analysis methods: in assessing health care security practices, various methods must be identified and used, as shown in Figure 2. These include a hybrid survey consisting of both qualitative and quantitative approaches [6,16-115]. Attack-defense simulation is when the investigator acts as the adversary to gain access to health care resources by using various techniques, including social engineering, brute-force attack, and SQL injection, depending on the goal of the attacker. Data analysis with machine learning can also be adopted to analyze logs of health care staff to determine abnormal access and maliciousness. The analysis method obtains inputs from the comprehensive required security and privacy practices fused with the various levels of health care staff user categories.
- In addition, health care staff have various characteristics that can be traced in the psychological-social and cultural contexts, social engineering, and access logs [16].
- These qualities also serve as input to the study approach.
- The actual measure of security practices was then determined from the assessment and compared with the required security and privacy practices.
- Security failures are gaps or deltas in the security practices that are determined if, after assessment, the hospital is not able to fully comply with all the identified requirements.
- Security and privacy enhancement measures: security failures can be improved with security and privacy enhancement measures, such as incentive measures and improving on factors that influence security failures. For instance, health care staff can be treated with various incentivization measures to improve their security-conscious care behavior. The assessment can then be conducted to determine the effectiveness of the treatment.

Information security and privacy requirements change based on or assessed threats, thus requiring changes in various laws. Therefore, the framework is such that the study can always be repetitive, as shown in Figure 2, to assess and identify related security and privacy gaps among health care workers in their application of ICT in health care. In Figure 2, the framework implementation is simplified, and security requirements are identified for security and privacy behavior assessment. The findings were compared with the required security behavior. Identified gaps can always be improved through cybersecurity and privacy incentives.

Figure 2. Legal requirement framework.

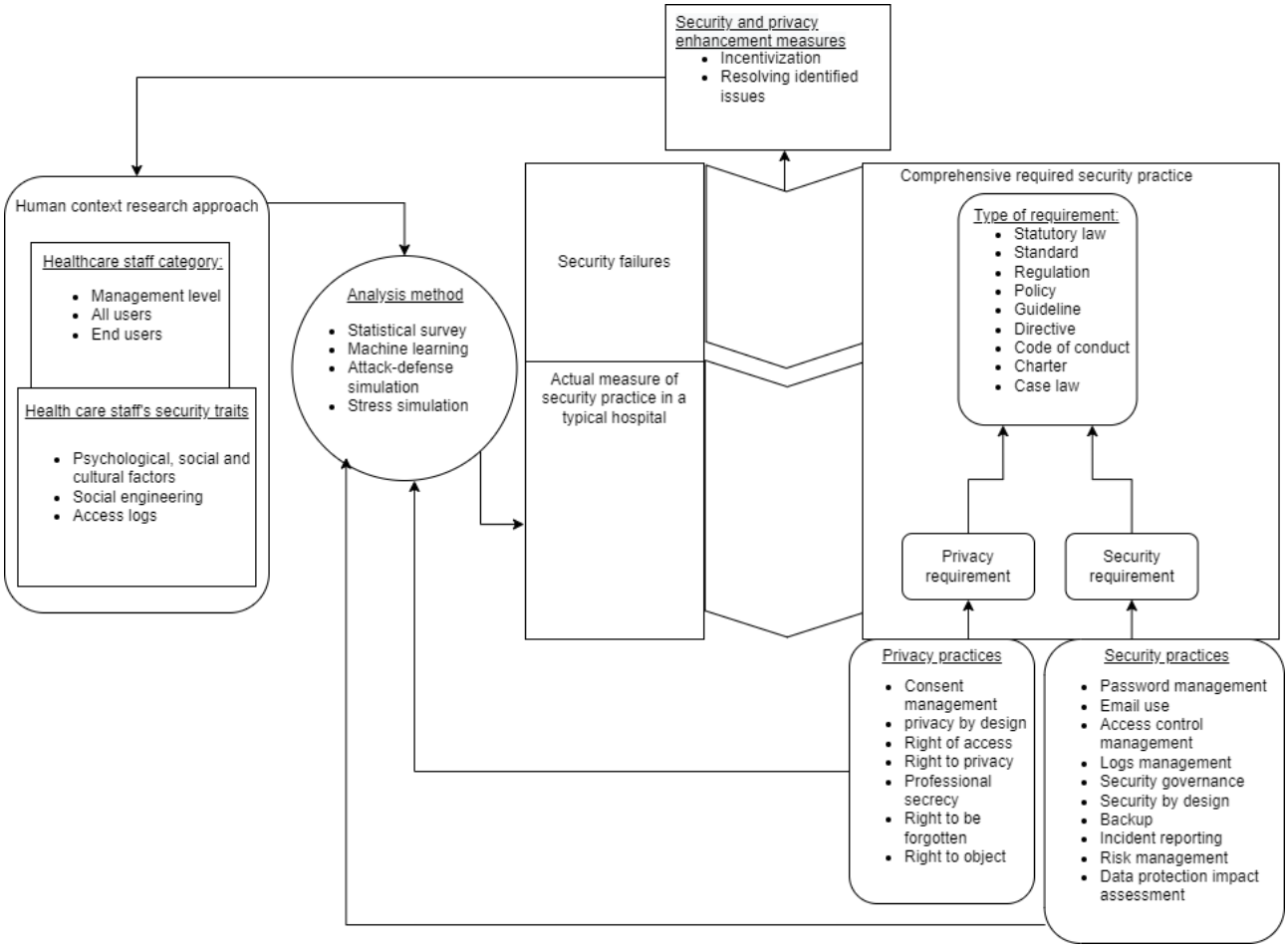
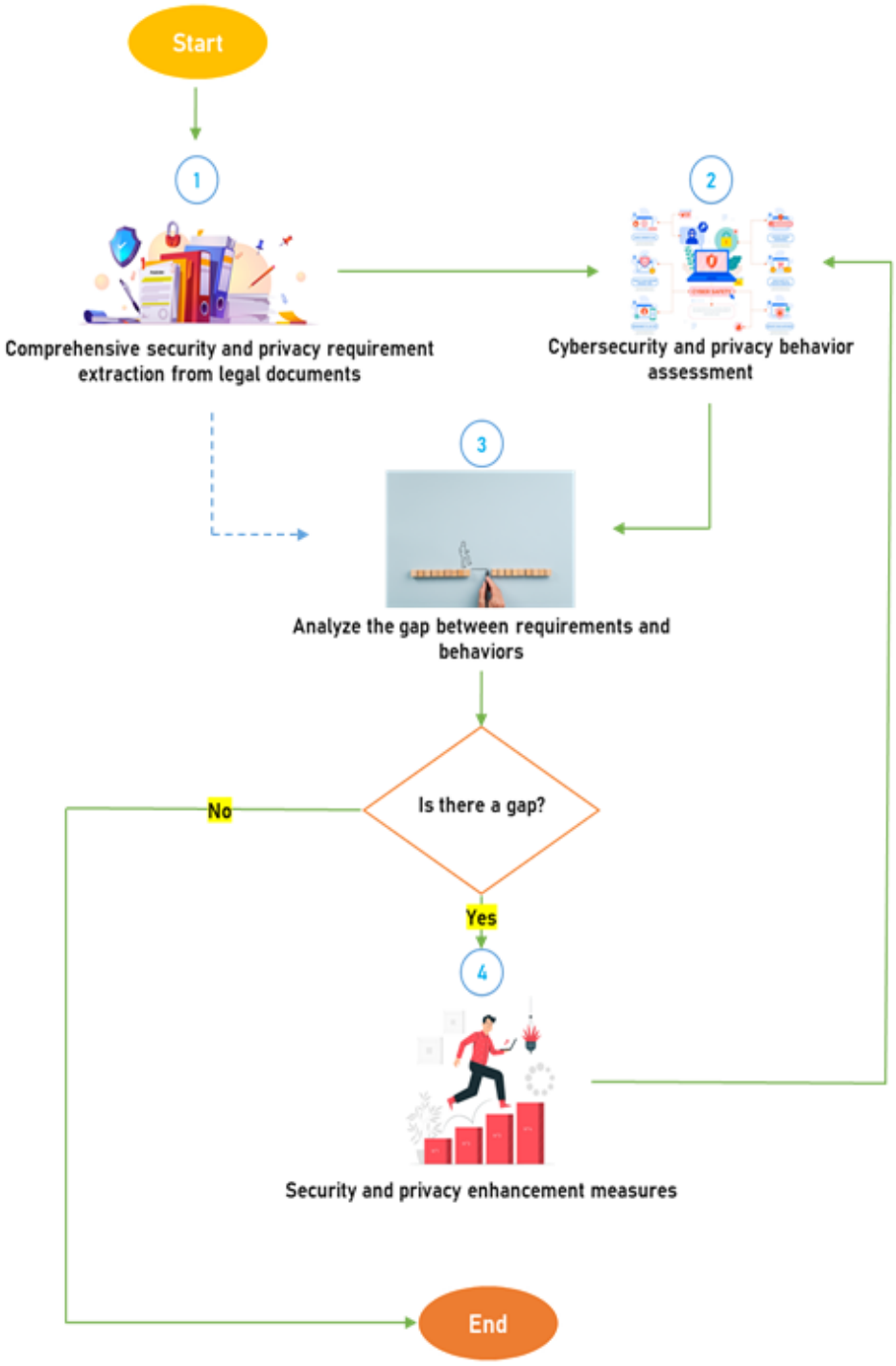


Figure 3. Measurement flowchart.



Conclusions

Amidst various information security solutions, data breaches continue to increase, especially in the area of the health care staff information security practice. This has attracted research interest in modeling and assessing health care staff's information security practices toward improving their security-conscious care behavior.

However, there is no holistic benchmark that serves as a yardstick in assessing health care information security practices comprehensively. To this end, we systematically reviewed information security requirements in health care in the context of legal requirements and information security governance tools for comprehensive security and privacy requirements in health care in Norway, Indonesia, and Ghana. Approximately 173 security requirements covering data processing, right of access, security by design, access control, email processing, logging, password, encryption, health care data storage, data processing officer, and so on were identified, as shown in Table 10.

In addition, approximately 80 privacy requirement categories were identified and included consent, disclosure of health data, privacy by design, right to privacy, right of access, data protection, data processing, personal data, and punitive. measures, as shown in Table 11. On the basis of these findings,

a framework for modeling, analyzing, and developing effective security countermeasures, including incentivization measures, was developed, as shown in Figures 2 and 3. Following this framework, research results of health care security practices would be more reliable and effective than relying on incomprehensive security requirements. However, we observed some limitations that should be considered in future studies. For instance, there may be more standards in information security, but we focused on health care–related information security standards from the scientific papers that we searched for based on the scope we set. Therefore, it may not be an exhaustive list of information security standards. Although we have identified the requirements and practices, in this framework, our work has not taken measures to narrow down the gap between requirements and practices by way of a real implementation. This is another limitation, and will be the next step in future work.

Having postulated this, the framework must be implemented to assess its effectiveness for general use. This framework will serve as a guideline for assessing security practices in health care.

Conflicts of Interest

None declared.

Multimedia Appendix 1

Law type distribution.
[PNG File , 58 KB-Multimedia Appendix 1]

Multimedia Appendix 2

Law jurisdiction distribution. EU: European Union.
[PNG File , 35 KB-Multimedia Appendix 2]

Multimedia Appendix 3

Requirement type distribution.
[PNG File , 91 KB-Multimedia Appendix 3]

Multimedia Appendix 4

Security requirement responsibility level.
[PNG File , 86 KB-Multimedia Appendix 4]

Multimedia Appendix 5

Requirement type distribution.
[PNG File , 65 KB-Multimedia Appendix 5]

References

1. Widup S. 2019 Verizon Data Breach Investigations Report. 2019. URL: https://www.nist.gov/system/files/documents/2019/10/16/1-2-dbir-widup.pdf [accessed 2022-03-22]
2. Devis J. The 10 biggest healthcare data breaches of 2019, so far. xtelligent Healthcare Media. 2019. URL: https://healthitsecurity.com/news/the-10-biggest-healthcare-data-breaches-of-2019-so-far [accessed 2022-03-22]
3. Yeng PK, Nweke LO, Woldaregay AZ, Yang B, Snekkenes EA. Data-driven and Artificial Intelligence (AI) approach for modelling and analyzing healthcare security practice: a systematic review. In: Intelligent Systems and Applications: Proceedings of the 2020 Intelligent Systems Conference (IntelliSys) Volume 1. Cham, Switzerland: Springer; Aug 25, 2020:1-18.
4. Attacks on health care in the context of COVID-19. World Health Organization. 2020 Jul 30. URL: https://www.who.int/news-room/feature-stories/detail/attacks-on-health-care-in-the-context-of-covid-19 [accessed 2022-03-22]
5. Brno University Hospital ransomware attack (2020). Cyber Law Toolkit. 2020 Mar 13. URL: https://cyberlaw.ccdcoe.org/w/index.php?title=BrnoUniversityHospitalransomwareattack(2020)&oldid=2290 [accessed 2022-03-22]
6. Muthuppalaniappan M, Stevenson K. Healthcare cyber-attacks and the COVID-19 pandemic: an urgent threat to global health. Int J Qual Health Care 2021 Feb 20;33(1):117 [FREE Full text] [doi: 10.1093/intqhc/mzaa117] [Medline: 33351134]
7. Cost of a Data Breach Report 2020. IBM. 2020. URL: https://www.ibm.com/account/reg/us-en/signup?formid=urx-46542 [accessed 2022-03-22]
8. Ayyagari R. An exploratory analysis of data breaches from 2005-2011: trends and insights. J Inf Priv Secur 2014 Jul 07;8(2):33-56. [doi: 10.1080/15536548.2012.10845654]

9. Moffit RE, Steffen B. Health Care Data Breaches: A Changing Landscape. Maryland Health Care Commission. 2017 Jun. URL: https://mhcc.maryland.gov/mhcc/pages/hit/hit/documents/HIT_DataBreachesBrief_Brf_Rpt_090717.pdf [accessed 2022-03-22]
10. Hjellen B. Hacking scandal shakes Finland-patients pressured for money. NRK. 2020 Oct 25. URL: https://www.nrk.no/urix/hacking-skandale-ryster-finland---pasienter-presset-for-penger-1.15214710 [accessed 2022-03-22]
11. A German hospital hacked, patient taken to another city dies. Associated Press. 2020 Sep 17. URL: https://www.securityweek.com/german-hospital-hacked-patient-taken-another-city-dies [accessed 2022-03-22]
12. Humer C, Finkle J. Your medical record is worth more to hackers than your credit card. Reuters. 2014 Sep 24. URL: https://www.reuters.com/article/us-cybersecurity-hospitals-idUSKCN0HJ21I20140924 [accessed 2022-01-22]
13. The Code of Conduct for information security and data protection in the healthcare and care services is a holistic approach to an information security policy for all organisations within the sector. Direktoratet for e-helse. URL: https://www.ehelse.no/normen/documents-in-english [accessed 2022-02-22]
14. Health informatics-Information security management in health using ISO/IEC 27002. International Organization for Standardization. 2016. URL: https://www.iso.org/standard/62777.html [accessed 2022-01-22]
15. Cannoy SD, Salam AF. A framework for health care information assurance policy and compliance. Commun ACM 2010 Mar;53(3):126-131. [doi: 10.1145/1666420.1666453]
16. Yeng PK, Yang B, Snekkenes EA. Framework for healthcare security practice analysis, modeling, and incentivization. In: Proceedings of the 2019 IEEE International Conference on Big Data. 2019 Presented at: BigData '19; December 9-12, 2019; Los Angeles, CA, USA p. 3242-3251. [doi: 10.1109/BigData47090.2019.9006529]
17. Patil HK, Seshadri R. Big data security and privacy issues in healthcare. In: Proceedings of the 2014 IEEE International Congress on Big Data. 2014 Presented at: BigData '14; June 27-July 2, 2014; Anchorage, AK, USA p. 762-765. [doi: 10.1109/bigdata.congress.2014.112]
18. Proposition 56 LS (2017-2018)/Act on the processing of personal data (the Personal Data Act). Ministry of Justice and Public Security. 2017. URL: https://www.regjeringen.no/no/dokumenter/prop-56-ls-/id2594627/ [accessed 2022-03-22]
19. Lewis B. How to tackle today's IT security risks. International Organization for Standardization. 2019. URL: https://www.iso.org/news/ref2360.html [accessed 2022-03-22]
20. Nadeau M. General Data Protection Regulation (GDPR): What you need to know to stay compliant. CSO India. 2020 Jun 12. URL: https://www.csoonline.com/article/3202771/general-data-protection-regulation-gdpr-requirements-deadlines-and-facts [accessed 2022-12-01]
21. Key Changes with the General Data Protection Regulation. General Data Protection Regulation. 2019. URL: https://eugdpr.org/the-regulation/ [accessed 2022-03-22]
22. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. European Commission. 2017. URL: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32016L1148 [accessed 2022-03-22]
23. Ghana Data Protection Act, 2012 (ACT 843). Data Protection Commission. 2012. URL: https://www.dataprotection.org.gh/index.php/data-protection/data-protection-acts-2012 [accessed 2021-12-22]
24. Yeng PK, Yang B, Snekkenes EA. Observational measures for effective profiling of healthcare staffs' security practices. In: Proceedings of the 43rd Annual Computer Software and Applications Conference. 2019 Presented at: COMPSAC '19; July 15-19, 2019; Milwaukee, WI, USA p. 397-404. [doi: 10.1109/COMPSAC.2019.10239]
25. Nweke LO, Yeng PK, Wolthusen SD, Yang B. Understanding attribute-based access control for modelling and analysing healthcare professionals' security practices. Int J Adv Comput Sci Appl 2020;11(2):683-690. [doi: 10.14569/ijacsa.2020.0110286]
26. Yeng PK, Yang B, Snekkenes EA. Healthcare staffs' information security practices towards mitigating data breaches: A literature survey. Stud Health Technol Inform 2019;261:239-245. [Medline: 31156123]
27. Kim J, Grillo JM, Boxwala AA, Jiang X, Mandelbaum RB, Patel BA, et al. Anomaly and signature filtering improve classifier performance for detection of suspicious access to EHRs. AMIA Annu Symp Proc 2011;2011:723-731 [FREE Full text] [Medline: 22195129]
28. Box D, Pottas D. Improving information security behaviour in the healthcare context. Proc Technol 2013;9:1093-1103. [doi: 10.1016/j.protcy.2013.12.122]
29. Box D, Pottas D. A model for information security compliant behaviour in the healthcare context. Proc Technol 2014;16:1462-1470. [doi: 10.1016/j.protcy.2014.10.166]
30. How to preventing social engineering attacks protect your business data. RMON Networks. 2016 Oct 20. URL: https://rmonnetworks.com/prevent-social-engineering-phishing/ [accessed 2019-12-22]
31. Arce I. The weakest link revisited [information security]. IEEE Secur Privacy 2003 Mar;1(2):72-76. [doi: 10.1109/msecp.2003.1193216]
32. Assessment of the health trusts' prevention of attacks on their ICT systems-Office of the Auditor General of Norway annual report. Riksrevisjonen. 2020. URL: https://www.riksrevisjonen.no/contentassets/1855de07d48f4292a8d9b28fd8795af6/annualreport2020.pdf [accessed 2022-05-22]

33. Jensen J, Tøndel IA, Jaatun MG, Meland PH, Andresen H. Reusable security requirements for healthcare applications. In: Proceedings of the 2009 International Conference on Availability, Reliability and Security. 2009 Presented at: ARES '09; March 16-19, 2009; Fukuoka, Japan p. 380-385. [doi: 10.1109/ares.2009.107]
34. Power DJ, Politou EA, Slaymaker MA, Simpson AC. Towards secure Grid-enabled healthcare. Softw Pract Exper 2005 Jul 25;35(9):857-871. [doi: 10.1002/spe.692]
35. Hartvigsen G, Pedersen S. Lessons learned from 25 years with telemedicine in Northern Norway. University Hospital of North Norway, Norwegian Centre for Integrated Care. 2015 Jun 23. URL: https://www.isfteh.org/files/media/TitulPrefaceContent.pdf [accessed 2022-04-12]
36. Implementation of GDPR in health care sector in Norway. Direktoratet for e-helse. 2019. URL: https://tinyurl.com/yckn3srn [accessed 2022-03-22]
37. Whitman ME, Mattord HJ. Principles of Information Security. 4th edition. Boston, MA, USA: Cengage Learning; 2011.
38. EU GDPR Information Portal. General Data Protection Regulation. 2018. URL: http://eugdpr.org/.html [accessed 2021-03-22]
39. Nasiri S, Sadoughi F, Tadayon MH, Dehnad A. Security requirements of Internet of things-based healthcare system: a survey study. Acta Inform Med 2019 Dec;27(4):253-258 [FREE Full text] [doi: 10.5455/aim.2019.27.253-258] [Medline: 32055092]
40. Appari A, Johnson ME. Information security and privacy in healthcare: current state of research. Int J Internet Enterp Manag 2010;6(4):279-314. [doi: 10.1504/ijiem.2010.035624]
41. Yeng PK, Wolthusen SD, Yang B. Legal requirements towards enhancing the security of medical devices. Int J Adv Comput Sci Appl 2020;11(11):666-675. [doi: 10.14569/ijacsa.2020.0111181]
42. Donahue K, Rahman SM. Healthcare IT: is your information at risk? Int J Netw Secur Appl 2012 Sep 30;4(5):97-109 [FREE Full text] [doi: 10.5121/ijnsa.2012.4508]
43. Coleman J. Assessing information security risk in healthcare organizations of different scale. Int Congr Ser 2004 Jun;1268:125-130. [doi: 10.1016/j.ics.2004.03.136]
44. Vago S. Law and society. 10th edition. New York, NY, USA: Routledge; Aug 27, 2015.
45. Warren E. Legal, ethical, and professional issues in information security. Cengage Learning. 2018. URL: https://www.cengage.com/resource_uploads/downloads/1111138214_259148.pdf [accessed 2018-01-31]
46. Wellington KB. Cyberattacks on medical devices and hospital networks: legal gaps and regulatory solutions. Santa Clara High Technol Law J 2014;30:139.
47. Yang CM, Lin HC, Chang P, Jian WS. Taiwan's perspective on electronic medical records' security and privacy protection: lessons learned from HIPAA. Comput Methods Programs Biomed 2006 Jun;82(3):277-282. [doi: 10.1016/j.cmpb.2006.04.002] [Medline: 16730852]
48. Section II: Management controls. Chapter 5: Computer Security Policy. National Institute of Standards and Technology. 2014. URL: https://csrc.nist.rip/publications/nistpubs/800-12/800-12-html/chapter5.html [accessed 2021-12-22]
49. Fites PE, Kratz MP. Information systems security: a practitioner's reference. New York, NY, USA: Van Nostrand Reinhold; 1994.
50. Lobel J. Foiling the system breakers: computer security and access control. New York, NY, USA: McGraw-Hill; 1986.
51. Kitchenham B, Pearl Brereton O, Budgen D, Turner M, Bailey J, Linkman S. Systematic literature reviews in software engineering – a systematic literature review. Inf Softw Technol 2009 Jan;51(1):7-15. [doi: 10.1016/j.infsof.2008.09.009]
52. Booth A, Sutton A, Papaioannou D. Systematic approaches to a successful literature review. London, UK: Sage Publications; 2016.
53. Khan RA, Khan SU. A preliminary structure of software security assurance model. In: Proceedings of the 13th International Conference on Global Software Engineering. 2018 Presented at: ICGSE '18; May 27-29, 2018; Gothenburg, Sweden p. 137-140. [doi: 10.1145/3196369.3196385]
54. Petersen K, Vakkalanka S, Kuzniarz L. Guidelines for conducting systematic mapping studies in software engineering: an update. Inf Softw Technol 2015 Aug;64:1-18. [doi: 10.1016/j.infsof.2015.03.007]
55. Forskningsetikkens historie, akademisk frihet og publiseringsetikk. Forskningsetiske Komiteene. 2022. URL: https://www.forskningsetikk.no/ [accessed 2022-03-22]
56. Kementerian Hukum dan HAM RI. 2021. URL: https://peraturan.go.id [accessed 2019-03-01]
57. Produk Hukor. Biro Hukum Dan Organisasi - Kementerian Kesehatan Republik Indonesia. 2021. URL: http://hukor.kemkes.go.id/hukor/permenkes [accessed 2022-03-22]
58. Ghana's Constitution of 1992 with Amendments through 1996. Constitute Project. 2021 Aug 26. URL: https://www.constituteproject.org/constitution/Ghana_1996.pdf [accessed 2022-03-22]
59. Policy documents. Ministry of health, Republic of Ghana. 2020. URL: https://www.moh.gov.gh/policy-documents/ [accessed 2022-03-22]
60. Manuals Guidelines. Data protection Commission, Republic of Ghana. 2020. URL: https://www.dataprotection.org.gh/ [accessed 2022-03-22]
61. Key Issues. General Data Protection Regulation. 2014. URL: https://gdpr-info.eu/issues/ [accessed 2022-03-22]
62. Parsons K, McCormac A, Butavicius M, Pattinson M, Jerram C. Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). Comput Secur 2014 May;42:165-176. [doi: 10.1016/j.cose.2013.12.003]

63. HAIS-Q - a smart solution to cyber security. Department of Defence, Australian Government. 2017 Aug. URL: https://www.dst.defence.gov.au/podcast/hais-q-smart-solution-cyber-security [accessed 2022-03-22]
64. Code of conduct for information security and data protection in the healthcare and care services sector. Version 6.0. Norwegian Directorate of eHealth. 2020 Feb 5. URL: https://www.ehelse.no/normen/documents-in-english/_/attachment/download/f615c927-fdc5-4ac7-9c8e-99b0bd95ea9a:75611a1559201375f7cc62079fc6405ace48c841/Code%20of%20Conduct%20version%206.0%20(PDF).pdf [accessed 2021-06-22]
65. Mirkovic J, Bryhni H, Ruland CM. A framework for the development of ubiquitous patient support systems. In: Proceedings of the 6th International Conference on Pervasive Computing Technologies for Healthcare. 2012 Presented at: PervasiveHealth '12; May 21-24, 2012; San Diego, CA, USA p. 81-88. [doi: 10.4108/icst.pervasivehealth.2012.248594]
66. Act of 18 May 2001 Nº 24 on Personal Health Data Filing Systems and the Processing of Personal Health Data (Personal Health Data Filing System Act). Ministry of Health and Care Services. 2014. URL: https://tinyurl.com/2scfttpw [accessed 2022-03-22]
67. Management system for information security. Helse. 2020. URL: https://www.helse-sorost.no/informasjonssikkerhet-og-p [accessed 2022-03-22]
68. Act of 2 July 1999 No. 64 relating to Health Personnel, etc. Ministry of Health and Care Services. 2002. URL: https://www.regjeringen.no/no/dokumenter/act-of-2-july-1999-no-64-relating-to-hea/id107079/ [accessed 2022-03-22]
69. A framework for cybersecurity and cybercrime, and a contribution for peace, security and justice in cyberspace. In: Cyber Crime Law. Oslo, Norway: Juridika; May 18, 2017.
70. Herveg J. Data protection and the patient's right to safety. Eur J Health Law 2014 Jun;21(3):260-270. [doi: 10.1163/15718093-12341322] [Medline: 25065033]
71. Aryanto K. Ensuring patient privacy in image data sharing for clinical research: design and implementation of rules and infrastructure. University of Gronigen. 2016. URL: https://pure.rug.nl/ws/portalfiles/portal/28139340/Chapter_1.pdf [accessed 2022-03-22]
72. European Union (EU). Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. Official Journal of the European Union. 2016 Jul 19. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:194:FULL&from=EN [accessed 2022-03-22]
73. Quinn P, De Hert P. The Patients' Rights Directive (2011/24/EU) – Providing (some) rights to EU residents seeking healthcare in other Member States. Comput Law Secur Rev 2011 Sep;27(5):497-502. [doi: 10.1016/j.clsr.2011.07.010]
74. Kierkegaard P. Electronic health record: wiring Europe's healthcare. Comput Law Secur Rev 2011 Sep;27(5):503-515. [doi: 10.1016/j.clsr.2011.07.013]
75. Mossialos E, Thomson S, Ter Linden A. Information technology law and health systems in the European Union. Int J Technol Assess Health Care 2004;20(4):498-508. [doi: 10.1017/s0266462304001424] [Medline: 15609802]
76. Hiller J, McMullen MS, Chumney WM, Baumer DL. Privacy and security in the implementation of health information technology (Electronic Health Records): U.S. and EU compared. BUJ Sci & Tech L 2011;17:1-40.
77. Pereira C, Oliveira C, Vilaca C, Ferreira A. Protection of clinical data: comparison of European with American legislation and respective technological applicability. In: Proceedings of the International Conference on Health Informatics. 2011 Presented at: HEALTHINF '11; January 26-29, 2011; Rome, Italy p. 567-570. [doi: 10.5220/0003165505670570]
78. Di Iorio CT, Carinci F, Oderkirk J, Smith D, Siano M, de Marco DA, et al. Assessing data protection and governance in health information systems: a novel methodology of Privacy and Ethics Impact and Performance Assessment (PEIPA). J Med Ethics 2020 Mar 27:105948. [doi: 10.1136/medethics-2019-105948] [Medline: 32220868]
79. Todde M, Beltrame M, Marceglia S, Spagno C. Methodology and workflow to perform the Data Protection Impact Assessment in healthcare information systems. Inform Med Unlocked 2020;19:100361. [doi: 10.1016/j.imu.2020.100361]
80. Sousa M, Ferreira DN, Santos-Pereira C, Bacelar G, Frade S, Pestana O, et al. openEHR based systems and the General Data Protection Regulation (GDPR). Stud Health Technol Inform 2018;247:91-95. [Medline: 29677929]
81. Paluzzi M. Paying prices for swiped devices: addressing the issue of medical identity theft from unencrypted stolen laptops. University of Illinois Law Review. 2019 Sep 1. URL: https://www.illinoislawreview.org/wp-content/uploads/2019/09/Paluzzi.pdf [accessed 2022-04-12]
82. Yuan B, Li J. The policy effect of the General Data Protection Regulation (GDPR) on the digital public health sector in the European Union: an empirical investigation. Int J Environ Res Public Health 2019 Mar 25;16(6):1070 [FREE Full text] [doi: 10.3390/ijerph16061070] [Medline: 30934648]
83. Pinem AA, Fajrina HR, Shandyaduhita PI, Handayani PW, Hidayanto AN. Barriers for integration between hospitals and the Ministry of Health in Indonesia. In: Managing Intellectual Capital and Innovation for Sustainable and Inclusive Society: Proceedings of the MakeLearn and TIIM Joint International Conference. 2015 Presented at: MakeLearn and TIIM '16; May 27–29, 2015; Bari, Italy p. 807-817.
84. Anderson RJ. A security policy model for clinical information systems. In: Proceedings 1996 IEEE Symposium on Security and Privacy. 1996 Presented at: SECPRI '96; May 6-8, 1996; Oakland, CA, USA p. 30-43. [doi: 10.1109/secpri.1996.502667]

85. Mennerat F, Chabriais J. Do EHR communication standards account for imaging communication needs? In: Lemke HU, Inamura K, Doi K, Vannier MW, Farman AG, Reiber JH, editors. CARS 2002 Computer Assisted Radiology and Surgery. Berlin, Heidelberg: Springer; 2002:647-650.
86. Hu Y, Afzal J. Achieving eHealth interoperability via peer-to-peer communication using JXTA technology. Blekinge Institute of Technology. 2010 May. URL: https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.471.702&rep=rep1&type=pdf [accessed 2022-03-22]
87. Sari PK, Handayani PW, Hidayanto AN. Security value issues on eHealth implementation in Indonesia. IOP Conf Ser Mater Sci Eng 2020 Jul 01;879(1):012040. [doi: 10.1088/1757-899x/879/1/012040]
88. Seddon JJ, Currie WL. Cloud computing and trans-border health data: Unpacking U.S. and EU healthcare regulation and compliance. Health Policy Technol 2013 Dec;2(4):229-241. [doi: 10.1016/j.hlpt.2013.09.003]
89. Bincoletto G. Data protection issues in cross-border interoperability of Electronic Health Record systems within the European Union. Data Policy 2020 Mar 30;2:e3. [doi: 10.1017/dap.2020.2]
90. Rath TA, Colin JN. Adaptive risk-aware access control model for internet of things. In: Proceedings of the 2017 International Workshop on Secure Internet of Things. 2017 Presented at: SIoT '17; September 15, 2017; Oslo, Norway p. 40-49. [doi: 10.1109/siot.2017.00010]
91. Pulkkis G, Karlsson J, Westerlund M, Tana J. Secure and reliable Internet of Things systems for healthcare. In: Proceedings of the IEEE 5th International Conference on Future Internet of Things and Cloud. 2017 Presented at: FiCloud '17; Aug 21-23, 2017; Prague, Czech Republic p. 169-176. [doi: 10.1109/ficloud.2017.50]
92. Natsiavas P, Rasmussen J, Voss-Knude M, Votis K, Coppolino L, Campegiani P, et al. Comprehensive user requirements engineering methodology for secure and interoperable health data exchange. BMC Med Inform Decis Mak 2018 Oct 16;18(1):85 [FREE Full text] [doi: 10.1186/s12911-018-0664-0] [Medline: 30326890]
93. Saranto K, Kivekäs E, Kinnunen UM, Palojoki S. Lack of patient data privacy challenges patient safety. Stud Health Technol Inform 2018;251:163-166. [Medline: 29968628]
94. Andersen MR, Storm HH, Eurocourse Work Package 2 Group. Cancer registration, public health and the reform of the European data protection framework: abandoning or improving European public health research? Eur J Cancer 2015 Jun;51(9):1028-1038. [doi: 10.1016/j.ejca.2013.09.005] [Medline: 24120502]
95. Callens S, Cierkens K. Legal aspects of E-HEALTH. Stud Health Technol Inform 2008;141:47-56. [Medline: 18953124]
96. Nordland O, Sujan MA, Koornneef F, Bernsmed K. Assurance requirements for networked medical sensor applications. In: Proceedings of the 2015 IEEE International Conference on Industrial Technology. 2015 Presented at: ICIT '15; March 17-19, 2015; Seville, Spain p. 1838-1844. [doi: 10.1109/icit.2015.7125364]
97. Kierkegaard P. E-Prescription across Europe. Health Technol 2012 Dec 20;3(3):205-219. [doi: 10.1007/s12553-012-0037-0]
98. Klein GO. Standardization strategy from a European perspective. Int J Med Inform 1998 Feb;48(1-3):67-70. [doi: 10.1016/s1386-5056(97)00112-3] [Medline: 9600406]
99. Christiansen EK, Skipenes E, Hausken MF, Skeie S, Østbye T, Iversen MM. Shared electronic health record systems: key legal and security challenges. J Diabetes Sci Technol 2017 Nov;11(6):1234-1239 [FREE Full text] [doi: 10.1177/1932296817709797] [Medline: 28560899]
100. Brox EA. Information security in distributed health information systems in Scandinavia: a comparative study of external conditions and solutions for exchange and sharing of sensitive health information in Denmark, Norway and Sweden. Norwegian University of Science and Technology. 2006 Jun. URL: https://ntnuopen.ntnu.no/ntnu-xmlui/handle/11250/251121 [accessed 2022-03-22]
101. Kalra D. Electronic Health Record Standards. Yearb Med Inform 2018 Mar 07;15(01):136-144. [doi: 10.1055/s-0038-1638463]
102. Nalin M, Baroni I, Faiella G, Romano M, Matrisciano F, Gelenbe E, et al. The European cross-border health data exchange roadmap: case study in the Italian setting. J Biomed Inform 2019 Jun;94:103183 [FREE Full text] [doi: 10.1016/j.jbi.2019.103183] [Medline: 31009760]
103. Healy L, Lubeck P. Patient information privacy and security in Ghana: current policy and suggestions for the future. University of California Santa Cruz. 2012. URL: https://dca.ue.ucsc.edu/dca/winners/2012/159 [accessed 2022-04-12]
104. Setianto YD, Wahyuningrum SE. Medical device authentication and authorization protocol in Indonesian telemedicine systems. In: Proceedings of the 4th International Conference on Information Technology. 2019 Presented at: InCIT '10; October 24-25, 2019; Bangkok, Thailand p. 89-93. [doi: 10.1109/incit.2019.8912058]
105. Santoso I, Siahaan IS, Suharjito. Privacy modelling of sensitive data in universal healthcare coverage in Indonesia. In: Proceedings of the 11th International Conference on Knowledge, Information and Creativity Support Systems. 2016 Presented at: KICSS '16; November 10-12, 2016; Yogyakarta, Indonesia p. 1-6. [doi: 10.1109/KICSS.2016.7951437]
106. Høstgaard AM, Bertelsen P, Nøhr C. Methods to identify, study and understand end-user participation in HIT development. BMC Med Inform Decis Mak 2011 Sep 28;11:57 [FREE Full text] [doi: 10.1186/1472-6947-11-57] [Medline: 21955493]
107. Samonas S, Coss D. The CIA strikes back: redefining confidentiality, integrity and availability in security. J Inf Syst Secur 2014;10(3):21-45.
108. What are the GDPR consent requirements? General Data Protection Regulation. 2019. URL: https://gdpr.eu/gdpr-consent-requirements/ [accessed 2022-03-22]

109. Act of 18 May 2001 No. 24 on Personal Health Data Filing Systems and the Processing of Personal Health Data (Personal Health Data Filing System Act). Ministry of Justice and Public Security. 2017. URL: https://www.datatilsynet.no/globalassets/global/english/personal_health_data_filing_system_act_20100907.pdf [accessed 2022-03-22]
110. Yarney L, Buabeng T, Baidoo D, Bawole JN. Operationalization of the Ghanaian patients' charter in a peri-urban public hospital: voices of healthcare workers and patients. Int J Health Policy Manag 2016 Sep 01;5(9):525-533 [FREE Full text] [doi: 10.15171/ijhpm.2016.42] [Medline: 27694679]
111. ACT 2008-06-20 no. 44: Act on medical and health research (the Health Research Act). Universitetet I Oslo. 2008. URL: https://app.uio.no/ub/ujur/oversatte-lover/data/lov-20080620-044-eng.pdf [accessed 2022-03-22]
112. Yousefi A. The impact of information and communication technology on economic growth: evidence from developed and developing countries. Econ Innov New Technol 2011 Sep;20(6):581-596. [doi: 10.1080/10438599.2010.544470]
113. Ngwa W, Olver I, Schmeler KM. The use of health-related technology to reduce the gap between developed and undeveloped regions around the globe. Am Soc Clin Oncol 2020 May(40):227-236. [doi: 10.1200/edbk_288613]
114. Miltgen CL, Peyrat-Guillard D. Cultural and generational influences on privacy concerns: a qualitative study in seven European countries. Eur J Inf Syst 2019 Jan 28;23(2):103-125. [doi: 10.1057/ejis.2013.17]
115. Yeng PK, Yang B, Solvoll T, Nimbe P, Weyori BA. Web Vulnerability Measures for SMEs. Norsk Informasjonssikkerhetskonferanse 2019:1-16 [FREE Full text]

Abbreviations

CEO: Chief Executive Officer
CIA: confidentiality, integrity, and availability
EHR: electronic health record
EISP: enterprise or organizational information security policy
EU: European Union
GDPR: General Data Protection Regulation
ICT: information and communication technology
ISO: International Organization for Standardization
ISSP: issue-specific security policy
IT: information technology
PRISMA: Preferred Reporting Items for Systematic Reviews and Meta-Analyses

Edited by A Kushniruk; submitted 29.04.21; peer-reviewed by G Klein, F Ghezelbash, R Ciorap; comments to author 30.07.21; revised version received 25.09.21; accepted 03.02.22; published 25.05.22

Please cite as:
Yeng PK, Fauzi MA, Sun L, Yang B
Assessing the Legal Aspects of Information Security Requirements for Health Care in 3 Countries: Scoping Review and Framework Development
JMIR Hum Factors 2022;9(2):e30050
URL: https://humanfactors.jmir.org/2022/2/e30050
doi: 10.2196/30050
PMID: