Contents lists available at Science-Gate

International Journal of Advanced and Applied Sciences

Journal homepage: http://www.science-gate.com/IJAAS.html

A security framework to protect ePHI in Saudi Arabia's healthcare infrastructure

Naif Hakami, Hazzaa Alshareef, Maha Helal *

College of Computing Informatics, Saudi Electronic University, Riyadh, Saudi Arabia

ARTICLE INFO

Article history:
Received 22 November 2023
Received in revised form
1 April 2024
Accepted 18 April 2024

Keywords:
Patient privacy
Data integrity
Cybersecurity framework
ePHI protection
Healthcare sector

ABSTRACT

Today, protecting patient privacy and ensuring the accuracy and integrity of their data are the two most crucial concerns in the healthcare field. Unauthorized access or changes to patients' private health records can lead to serious issues. Moreover, if healthcare providers fail to update a patient's records quickly, it could result in dangerous, even life-threatening situations. Attacks on hospital computer systems also present a significant danger to patient care. Establishing strong security measures and procedures through cybersecurity frameworks can help protect sensitive patient information, known as electronic protected health information (ePHI). The Security Rule by Health Insurance Portability and Accountability Act (HIPAA), a well-established set of security guidelines, focuses on safeguarding ePHI held by healthcare organizations and their associates. This paper suggests creating a Data Cybersecurity Framework (DCF) specifically for the healthcare sector in Saudi Arabia. This framework aims to shield ePHI and align with the security recommendations of the HIPAA Security Rule. The development of this proposed framework involved consultations with healthcare cybersecurity experts and concentrated on the healthcare system in Saudi Arabia. The research concludes that enhancing the protection of patient information and raising public awareness requires the joint efforts of various entities, including government bodies.

1. Introduction

Primary, secondary, and tertiary healthcare have all received significant funding and attention from the Saudi government. As a result, Saudi citizens' health has improved dramatically over the past few decades. In Saudi Arabia, there is a growing concern that electronic health systems are being underutilized. King Faisal Specialist Hospital and Research Centre, the National Guard Health Affairs, the Medical Services of the Army Forces, and university hospitals are only a few facilities that have begun implementing e-health and electronic information systems. The Ministry of Health (MOH) has set aside SR 4 billion (US$ 1.1 billion) over the course of four years to fund a development strategy for public sector e-health services (2008 – 2011). Improved utilization of e-health initiatives and the introduction of a complete national health information system necessitate increased collaboration among various healthcare providers (Almalki et al., 2011).

Confidentiality and accuracy of patient information are of paramount importance in healthcare settings (Duggineni, 2023). Patient's health is at risk if their personal information is compromised or altered in healthcare systems. Cyberattacks on healthcare infrastructure also pose a significant risk to patient care (Hathaliya and Tanwar, 2020; Keshta and Odeh, 2021). Enhancing cybersecurity was clearly integral to the Kingdom's Vision 2030, as it plays a fundamental role in preserving and supporting information technologies and strengthening the digital infrastructure (Al-Kahtani et al., 2022).

Since the Office for Civil Rights of the Department of Health and Human Services (HHS) began providing summaries of healthcare data breaches on its website in October 2009, the Health Insurance Portability and Accountability Act (HIPAA) Journal has been compiling statistics on healthcare data breaches (hipaajournal.com). The HHS Office has received 4,419 reports of healthcare data breaches involving 500 or more records between 2009 and

* Corresponding Author.
Email Address: mhelal@seu.edu.sa (M. Helal)

https://doi.org/10.21833/ijaas.2024.04.019
Corresponding author's ORCID profile:
https://orcid.org/0000-0002-3834-4410
2313-626X/© 2024 The Authors. Published by IASE.

2021. Approximately 314,000,618 medical records were compromised as a result of these breaches, which represents over 94.63% of the entire population of the United States in 2021. As of 2018, there was a daily report of healthcare data breaches affecting 500 or more records. In the space of four years, the rate has doubled. A daily rate of 1.95 healthcare data breaches involving 500 or more records was reported in 2021. Fig. 1 demonstrates the number of data breaches from 2009 to June 2022.

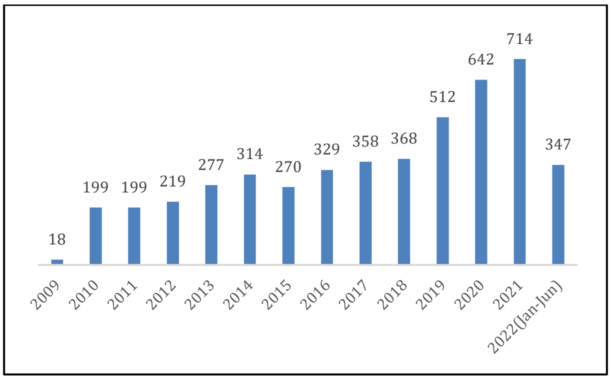

Fig. 1: Number of data breaches in the healthcare industry by year

Even though healthcare organizations have improved considerably at detecting hacking incidents, research shows that hacking is currently the primary source of healthcare data breaches (Seh et al., 2020). While the statistics indicate that there were fewer hacking issues in the early years, this could be due to the fact that hacking incidents and malware infections were not easily detected before 2018. Fig. 2 displays healthcare hacking incidents from 2009 to June 2022.

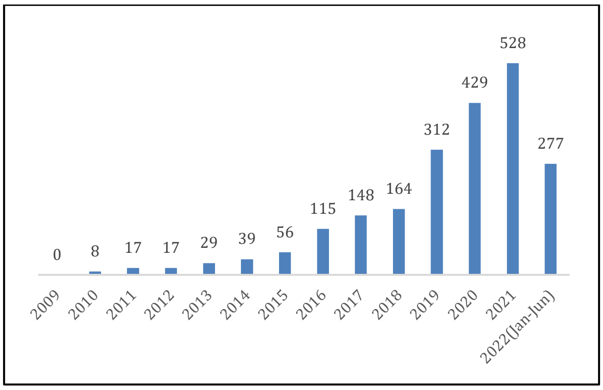

Fig. 2: Number of healthcare hacking incidents by year

Regarding healthcare data, medical records are breached considerably more frequently than individual records in Saudi Arabia. Statistics have indicated that 75% of Saudis reported that their medical records had been compromised, but only 32% reported the same about their personal information. The most frequently reported types of compromised data are electronic medical records (25%), medical record numbers (25%), and health insurance ID numbers (24%). Consumers' contact information is the most sought-after piece of personal data, and 32% reported that it had been compromised in some way. Other fraudulent acts involving stolen IDs included obtaining prescriptions, seeking medical attention, and making purchases.

Similar research conducted in Saudi Arabia found that 75% of consumers had experienced a breach of their medical data (Alzahrani et al., 2022). However, only 32% reported that their personal information had been breached. This demonstrates that there are almost three times as many breaches in Saudi Arabia (35%) as in other countries that were examined. Laws in Europe and North America ensure that personal information is safe and secure. On the other hand, Saudi Arabia does not have regulations on data protection or guidelines for data security breaches. Therefore, Data Cybersecurity Controls (DCC) compliance is lacking in healthcare institutions in the country, and a sustainable plan for its implementation is absent.

This paper provides the essential factor in bringing the highest international data protection standards for the healthcare sector in the Saudi Arabian healthcare industry. The HIPAA Security Rule will significantly modify how organizations are permitted to store, manage, and use sensitive patient information. HIPAA empowers individuals to make more informed decisions about their healthcare. Limitations are imposed on the disclosure and use of patient information. For patient confidentiality, it lays out standards that hospitals, clinics, and other facilities must meet.

The primary focus of the research involves the examination of three security standards aimed at safeguarding ePHI: administrative safeguards, physical safeguards, and technical safeguards. It presents numerous precautions and measures within these domains to ensure adherence. The analysis uncovered significant deficiencies in security controls for ePHI protection and, therefore, proposed a security framework to address these gaps.

The remainder of this paper is structured as follows: Previous related work is presented in Section 2. This is followed by the details of the methodology in Section 3. The implementation setup is detailed in Section 4, and the results and discussions are presented in Section 5. Finally, Section 6 concludes this research and directs future work.

2. Literature survey

Marron (2022) implemented the HIPAA Security Rule and discussed how all regulated companies are required to follow the standards and guidelines for protecting patients' electronic protected health information (ePHI). ePHI that is created, received, maintained, or transmitted by a covered entity is required to be safeguarded from any risks, misuse, or unauthorized disclosures that could reasonably be expected to occur. Attallah et al. (2016) discussed how the Saudi MoH has made progress toward a national Health Information Exchange (HIE) as a top goal. The findings indicate that the literature contains numerous challenges and opportunities that may affect how Saudi Arabia implements the national HIE strategy. Data formatting, semantic ontology, and establishing an HIE infrastructure were named as the three main obstacles to HIE. Improvements in healthcare quality and cost savings were also cited as opportunities for Saudi Arabia to take advantage of when putting the HIE into action.

In their research on protecting patient privacy when sharing patient-level data from clinical trials, Tucker et al. (2016) outlined the best practices for data anonymization/de-identification and controlled access to data, such as using DSAs. To encourage a method that strikes a balance between data utility and privacy risk, their guidelines can be used in healthcare research. The context in which data holders share data (for example, approved research proposals, legal and data security controls) was considered, as was the ability to efficiently and effectively prepare and deliver large volumes of data requests in a semi-automated fashion, the ability to align/standardize processes across data holders, and the practical considerations related to protecting patient privacy. In addition, Hussain et al. (2021) proposed a methodology for creating IoT context-aware security solutions for monitoring healthcare networks for harmful activity. An IoT-based ICU use case was developed to generate both benign and harmful traffic. This is accomplished with the help of an IoT traffic generator tool that is part of the proposed architecture.

In their work, Al Hamid et al. (2017) proposed the usage of fog computing to protect users' cloud-based multimedia data as part of the larger objective of safeguarding cloud data. With this in mind, they provided two photo galleries. Both the OMBD and the DMBD are hidden; the former is housed in the cloud, and the latter is utilized as a honeypot and is protected by fog. Consequently, the user always has access to the DMBD, and then unwanted access is identified. Only once a user's identity has been confirmed is he or she granted access to the OMBD. Setting the DMBD to its default value protects the primary multimedia data while the OMBD is stashed away in a gallery. An efficient tri-party authenticated key agreement mechanism between the user, the DPG, and the OPG based on symmetric cryptography has been proposed to aid in the aforementioned procedure.

Furthermore, Shah and Khan (2020) presented various secondary uses of EHR to provide researchers with valuable insights into how effective EHR data can be used in different domains, such as clinical research, public health surveillance, and clinical audits, to provide efficient, timely, and high-quality healthcare services to patients. Challenges related to secondary applications of EHR have also been discussed to ensure researchers are aware of the difficulties inherent in using EHR data for other purposes. In other research, Alabdulatif et al. (2019) discussed a secure edge of things for a smart healthcare surveillance framework. The evaluation of a case study with patient bio-signal data illustrates the suggested methodology. With their framework, the data will remain private and will be analyzed faster and more accurately. In addition, Tervoort et al. (2020) researched solutions for mitigating cybersecurity risks caused by legacy software in medical devices. They found 18 different approaches that worked effectively, all of which involved either IDS/IPS, communication tunneling, or hardware safeguards. Several methods have been implemented, such as emulating Bluetooth communications using mobile devices as a proxy, detecting anomalies based on a signal's behavior, and physically authenticating signs. These methods may be used to protect medical sensor networks and pacemakers alike. Most of these workarounds involve either tunneling unsecured wireless connections or detecting intrusions. Different types of medical devices call for other applications of these technologies.

3. Methodology

The main goal of this paper is to produce comprehensive and user-friendly guidance for securing ePHI in Saudi Arabia by implementing cybersecurity data rules. After analyzing existing cybersecurity policies, a series of interviews were conducted with cybersecurity experts working in the healthcare industry. As discussed in previous studies, there is no universal formula for selecting participants in research (Czernek-Marszałek and McCabe, 2024). However, researchers need to take several considerations into account when selecting participants, including the characteristics of the participants, the research context, the level of expertise in the field, and any ethical concerns. These considerations were taken into account while selecting cybersecurity experts to work in the healthcare industry. Each interview consisted of asking the expert a set of 28 questions. These questions covered the most important aspects of the various security methods that are currently used. The answers were verified for reliability by checking for any unusual patterns or biases. Subsequently, key findings were summarized, and charts were created to represent response patterns.

It became apparent that these security methods are very broad and do not address the pressing issue of adequately protecting patient data. This information is potentially harmful if obtained by an unauthorized party. From this point, it was apparent that conducting a thorough investigation review of research publications is essential. After examining a wide variety of framework approaches in the field of healthcare data protection, we concluded that we needed to make use of the most effective global methods to fill in the gaps in the controls that are now in place. In this regard, HIPAA provides definitive documentation and establishes procedures to preserve and safeguard digital healthcare data. We will keep ePHI secure based on the Security Rule of ePHI security principles: confidentiality, integrity, and availability. The Security Rule is a set of standards that must be met by all organizations subject to HIPAA. Fig. 3 shows the proposed method, which includes the security rules that should be followed and will be combined to make the data security control we need to put in place to meet the requirements. Three security rules are covered: Administrative Safeguards, Physical Safeguards, and Technical Safeguards. This paper offers several ways to help health sectors comply with regulations. It assists organizations in selecting security measures and controls to protect the ePHI they manage. It also helps in developing compliance plans that match the organization’s size and structure. The HIPAA Security Rule, a federal law, mandates all relevant entities to take necessary steps to safeguard their patients' personal health information. Additionally, this approach aids entities in their compliance efforts by recommending security practices and controls adequate for the protection of ePHI and advising on creating suitable compliance strategies based on the entity's size and composition.

3.1. Data cybersecurity framework (DCF)

A covered entity must ensure the security of any ePHI it creates, receives, maintains, or transmits, to prevent unauthorized use or disclosure. This research will adhere to the Security Rule, which is divided into six main sections. Each section comprises several standards and implementation specifications that a regulated entity needs to meet. Fig. 4 illustrates the six parts of the DCF. In this study, we will focus on implementing security protocols such as Administrative Safeguards, Physical Safeguards, and Technical Safeguards, along with their respective measures and controls that require attention.

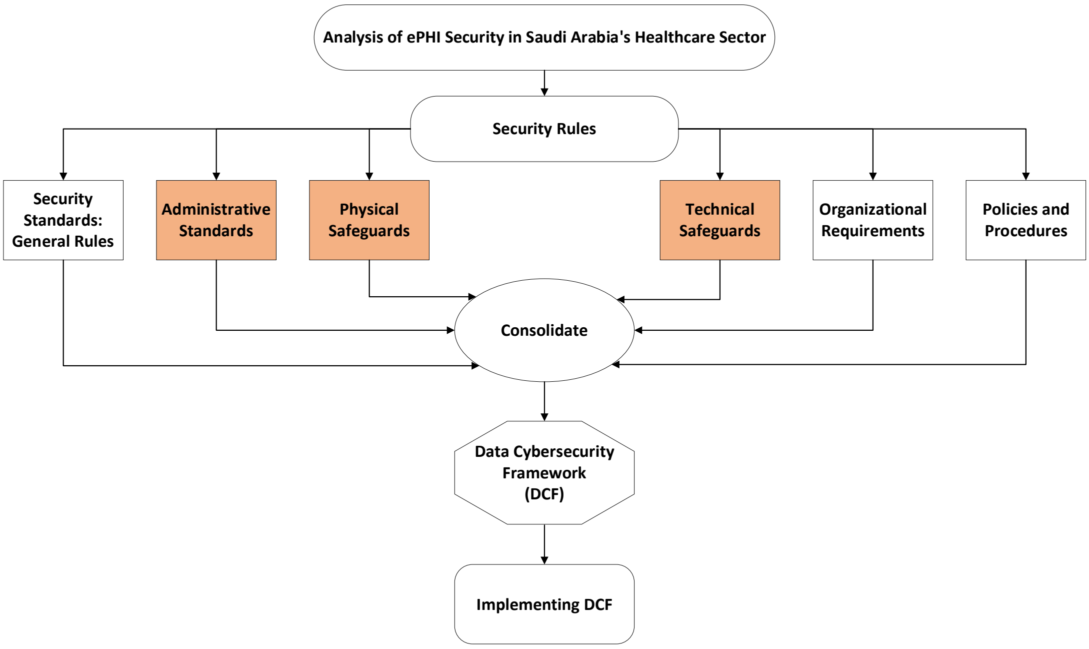
Analysis of ePHI Security in Saudi Arabia's Healthcare Sector
Security Rules
Security Standards: General Rules
Administrative Standards
Physical Safeguards
Technical Safeguards
Organizational Requirements
Policies and Procedures
Consolidate
Data Cybersecurity Framework (DCF)
Implementing DCF

Fig. 3: Illustration of proposed methodology

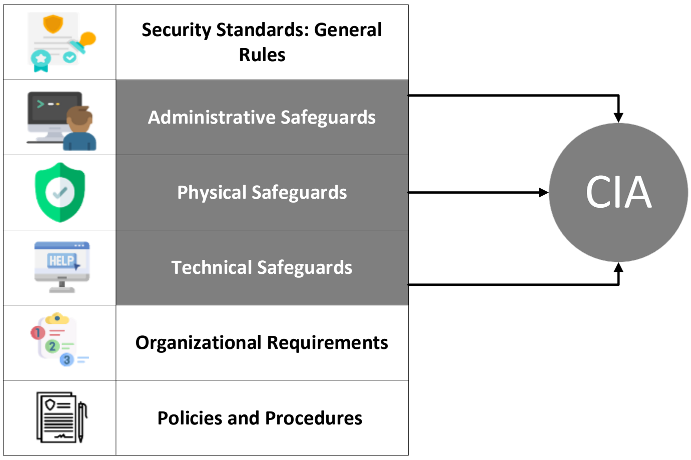
Security Standards: General Rules
Administrative Safeguards
Physical Safeguards
Technical Safeguards
Organizational Requirements
Policies and Procedures
CIA
HELP

Fig. 4: Illustration of the data cybersecurity framework (DSF)

The Security Rule sets out general requirements that all regulated entities must follow, allowing flexibility in approach. It defines standards and implementation specifications, both mandatory and addressable, and outlines the decisions a regulated entity must make concerning addressable specifications. It also requires security measures to ensure the ongoing protection of ePHI. To effectively manage the selection, development, implementation, and maintenance of security measures to protect ePHI, administrative actions, policies, and procedures are essential. These measures involve overseeing the conduct of the workforce in relation to the safeguarding of information. Security, in this context, includes physical and technical safeguards. Physical safeguards refer to measures that protect an organization's electronic information systems, physical structures, and equipment from threats like environmental hazards and unauthorized access. Technical safeguards involve the tools and protocols used to secure sensitive data such as electronic medical records. Organizational requirements dictate the inclusions in group health plans and the stipulations in contracts between a covered entity and a business associate, or between a business associate and a subcontractor. Entities must meet all standards and implementation specifications of the Security Rule and implement reasonable and appropriate policies and procedures to ensure compliance. The Rule also requires the creation of written (or electronic) documentation detailing necessary policies, procedures, actions, activities, or assessments to maintain compliance (Marron, 2022).

4. Implementation setup

Protections that are specific to each need of the Security Rule are detailed below. The relevant criteria are provided in a uniform table format and are categorized per the HIPAA Security Rule standards. The aim is to enlighten regulating entities on how to meet the Security Rule's recommendations. When a regulating entity puts the Security Rule into action, these tables can be used as guidelines for these entities. However, they are not meant to be inclusive in implementing the Security Rule. Table 1 presents the security management process. The HIPAA standards are properly defined in Table 1. The security responsibilities as per HIPAA standards are defined in Table 2. Furthermore, Table 3 shows the workforce security policies.

The details related to information access management for authorizing access to ePHI are defined in Table 4. As per HIPAA standards, the implementation of security awareness and training programs for all members of its workforce is required, as mentioned in Table 5. As per HIPAA standards, policies and protocols that control physical access to both electronic information systems and the respective facilities are required to be developed and enforced, ensuring only authorized personnel can gain entry, as highlighted in Table 6. Different physical safeguard requirements, such as physical access to workstations and devices, and analysis of access risk factors are presented in Table 7. Table 8 shows the device and media controls, such as methods of final ePHI disposal, procedure for reuse of electronic media, maintaining Accountability for Hardware and Electronic Media, and Developing Data Backup and Storage Procedures. In addition, the access control details are provided in Table 9. According to HIPAA standards, it is important to protect health information from destruction or improper alternation. Table 10 shows the information related to technical safeguards and integrity. Furthermore, person or entity authentication is also one of the important things to consider, and the details are provided in Table 11. Finally, Table 12 highlights the details of transmission security, which includes the identification of any possible unauthorized sources that may be able to intercept and/or modify the information, develop and implement transmission security policies and procedures, and implementation of integrity control and encryption.

5. Results and discussion

This research fills a gap in the literature by analyzing three security criteria for protecting ePHI: administrative safeguards, physical safeguards, and technical safeguards. There are nine different precautions outlined in the administrative safeguards. In addition, there are five measures of technical security and four of physical security to ensure compliance. Our scope is to cover the following three security rules to protect ePHI: administrative safeguards, physical safeguards, and technical safeguards.

In administrative safeguards, we apply administrative actions, policies, and procedures to manage the selection, development, implementation, and maintenance of security measures to protect ePHI and to manage the conduct of the covered entity's workforce related to the protection of that information. In addition, to protect its electronic information systems and related buildings and equipment from natural and environmental hazards and unauthorized intrusion, a covered entity must implement physical safeguards. Covered organizations must think about every possible way that ePHI could be accessed outside of the organization. The healthcare organization's office, employees' homes, and even a separate physical storage center all need to meet the highest standards of security. With regards to technical safeguards, we achieve this compliance by using a variety of access control mechanisms and technical controls, as was discussed earlier in the section on technical safeguards. In most information systems, users have access to several different types of technical controls and methods for limiting who can access data. There is no mention of a particular system of access control in the Security Rule.

Throughout the course of the interviews, officers in charge of policies and procedures responded to a total of 28 questions listed in Table 13 to evaluate the effectiveness of the safeguards that had been put into place. The information below comes from interviews with healthcare IT experts and is presented in Table 14 (Compliance Interview-Overall Compliance Level).

Table 1: Security management process

1. Administrative safeguards; 1.1. Security management process		
HIPAA Standard: Implement policies and procedures to prevent, detect, contain, and correct security violations (Marron, 2022)		
Security control	Definition	Questions to consider
1.1.1 Identify all ePHI and related IT systems	Locate the points of entry, movement, storage, and exit for ePHI, as well as the points at which it is created, received, used and released inside the organization; To begin, you must pinpoint all the locations that store ePHI. To properly secure ePHI, it is important to identify mobile devices, medical equipment, and medical IoT devices that store, process, or transmit ePHI; All devices and programs used to gather, store, process, or communicate ePHI must be included It is important to analyze corporate operations and confirm control and ownership of information system components; The hazards to ePHI should be evaluated in light of a potential merger or acquisition. After a business merger or purchase, ePHI may end up in locations where it was not originally intended to be kept, processed, or communicated	Have all ePHI created, maintained, processed, or sent by the business been cataloged? Is there a regular procedure in place to take stock of the company's hardware and software? Are the devices and programs that store or transfer ePHI known to exist? Does it include things like USB? Is the current state of the organization's systems recorded, including their interrelationships?
1.1.2 Conduct risk assessment	To ensure the privacy, security, and availability of ePHI, covered entities and their business associates must conduct a risk analysis	Where can we find the results of security tests, security requirements, audit comments, and/or risk assessments that have been conducted in the past? How much information can be gleaned from sources like the US-CERT, the OIG, virus warnings, and vendors? How vulnerable are the systems that house, process, or transmit ePHI to human, natural, and environmental hazards? What safeguards are in place, and what are the plans? Have the likelihood and impact of the relevant threats and vulnerabilities been determined? Have risk assessments been performed on pertinent threats and vulnerabilities?
1.1.3 Implement a risk management program	It is recommended that risk management be undertaken consistently in order to previous decisions, update risk likelihood and impact levels, and evaluate the efficacy of previous repair efforts; Identify the level of risk a company is willing to take, how often risk is managed, who is responsible for it, and what evidence is needed	Are the company's top brass and management team participating in making risk assessments and taking appropriate action? Have risk management policies been established? When it comes to risk management, does the regulated business need to bring in additional resources (such as outside expertise)? Do the existing protections guarantee the privacy, security, and accessibility of all ePHI? Can reasonably anticipated uses and disclosures of ePHI that are not permitted by the Privacy Rule be prevented by the current safeguards? When it comes to safeguarding ePHI, has the regulated entity taken into account the findings of risk assessments and risk management processes in making their decision on which controls to put in place? Is ePHI secure and free of all known dangers and hazards, as far as the regulating body is aware? Are all policies and procedures being followed by the regulated entity's staff?
1.1.4 Acquire IT systems and services	Cloud services and other third-party IT systems can aid regulated businesses in protecting ePHI. However, they might also bring new risks to ePHI security. The HIPAA Security Rule does not require the purchase of specific technologies, but additional hardware, software, or services might be necessary to secure data adequately. When selecting IT solutions, consider the following factors: the compatibility of the IT solution with the intended environment; the required level of data confidentiality; the organization's security policies, procedures, and standards; and other essential requirements such as resource availability for operation, maintenance, and training	Will the new security measures be compatible with the current IT infrastructure? Have the organization's security needs been compared to the safety mechanisms of the current and prospective IT infrastructure? Are the potential benefits of the investment outweighing the costs in light of the known security risks? Has a plan for training been established?
1.1.5 Create and deploy policies and procedures	Take action on the chosen managerial, operational, and technical controls to reduce the risks that have been identified; Develop policies that define who does what, and who is ultimately accountable for each control's successful implementation; Make a plan outlining the steps to be taken to complete various security-related duties Schedule regular policy and process reviews	Does the regulated entity have a written organizational risk assessment/ management policy outlining roles, responsibilities, reporting, and reporting requirements for the risk management program? Are there established safety regulations and procedures? Is there a written procedure for keeping the system safe? Is there a formal backup strategy in place? Does the company have a system in place for informing employees who will be impacted by new policies and procedures? Is there regular policy and procedure review and revision?
1.1.6 Develop and implement a sanction policy	Retaliate against employees who violate the security rules and procedures of the covered company or business associate in an acceptable manner; Execute sanction policy when situations emerge; create rules and procedures for implementing appropriate sanctions (e.g., reprimand, termination) for violation of the organization's security policies	Does the entity in scope already have in place sanction policies and processes that are adequate to fulfill the duties of this implementation specification? Could the language concerning infractions of these rules and processes be added to the existing punishment policies if this is not possible? Is there a protocol for dealing with fraud, abuse, and other forms of mistreatment of the system? Have workers been informed of the repercussions of breaching ePHI in any way (via access, use, or disclosure)?
1.1.7 Implement the information system activity review and audit process	It is time to start keeping track of everything and conducting audits	Is there a plan for measuring how well the review process is working? When necessary, how will the review procedures be updated?

Table 2: Assigned security responsibility

1. Administrative safeguards; 1.2. Assigned security responsibility		
HIPAA Standard: Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the covered entity or business associate (Marron, 2022)		
Security control	Definition	Questions to consider
1.2.1 Select a security official to be assigned responsibility for HIPAA security	Find the person who is ultimately accountable for security Pick a person who can evaluate security effectiveness to operate as the central point of contact for security planning, execution, and oversight	Is the security official able to effectively communicate and collaborate with the company's most senior leaders, including the CEO, CIO, COO, and general counsel? Who inside the company is tasked with taking on system risks on the company's behalf?
1.2.2 Assign and document the individual's responsibility	Job descriptions are useful for recording the tasks that have been delegated to a certain person Make sure everyone in the company is aware of their new responsibilities	Is there a detailed job description outlining all of the security guard's responsibilities? Have employees been made aware of whom to contact in the event of a security breach?

Table 3: Workforce security

1. Administrative safeguards; 1.3. Workforce security		
HIPAA Standard: Implement policies and procedures to ensure that all members of its workforce have appropriate access to ePHI, and to prevent those workforce members who do not have access from obtaining access to ePHI (Marron, 2022)		
Security control	Definition	Questions to Consider
1.3.1 Implement policies and procedures for authorization and/or supervision	Establish measures to control who may access ePHI and where it can be accessed by workforce members	Have proper lines of command and reporting been set up? Have employees been informed of who their managers are and what they do?
1.3.2 Establish clear job descriptions and responsibilities	Clearly outline everyone's responsibilities in every department To ensure the safety of the employees and property, it is important to provide enough management, training, and access Document who has access to ePHI, when they have it, what they may do with it, and under what conditions	Does each position have a defined job description, and do those descriptions reflect the level of ePHI access that position requires? Do you regularly evaluate and update these job descriptions? Have employees received copies of their job descriptions and been briefed on the privileges and restrictions that come with their positions?
1.3.3 Establish criteria and procedures for hiring and assigning tasks	Verify that employees possess the expertise required to carry out their duties (e.g., positions involving access to and use of sensitive information) Make sure these criteria are considered while filling open positions.	Have the skills and experience of applicants been compared to the requirements of the open positions? Have determinations been made that candidates for certain positions can undertake the tasks associated with those positions?
1.3.4 Establish a workforce clearance procedure	Create checks and balances to make sure only authorized workers can access sensitive ePHI It is imperative to do proper screening of individuals who will have access to ePHI Set up a system to get permission from relevant bodies before gaining access to sensitive areas, and stick to it	Is there a plan in place that helps those who have been given special permissions to use the system? Is it standard practice to contact past employers and schools mentioned by applicants? Were proper and acceptable background checks conducted? How to ensure that only the right people in your organization get access to sensitive data?
1.3.5 Establish termination procedures	Whenever an employee's employment or other relationship with the company comes to an end, there should be a plan in place for how access to ePHI will be revoked Create a standardized plan for returning ID badges, keys, and other access control devices to former employees Revoke access to computers (by changing passwords) and physical locations (by resetting security codes/PINs).	Is there a clear distinction between the processes for an employee's voluntary termination (such as retirement, promotion, transfer, or change of employment) and an employee's involuntary termination (such as termination for cause, reduction in force, involuntary transfer, criminal or disciplinary actions)? Is there a standard checklist for all action items that should be completed when an employee leaves (e.g., return of all access devices, deactivation of logon accounts [including remote access], and delivery of any needed data solely under the employee's control)? Is it necessary to inform other companies to terminate the employee's access to any accounts used for work purposes?

Table 4: Information access management

1. Administrative safeguards; 1.4. Information access management		
HIPAA Standard: Implement policies and procedures for authorizing access to ePHI (Marron, 2022)		
Security control	Definition	Questions to Consider
1.4.1 Isolate healthcare clearinghouse functions	Clearinghouses that are subsets of larger organizations are required to take precautions to prevent their parent company from gaining access to their ePHI Check if any part of the covered entity performs the functions of a healthcare clearinghouse as defined by the HIPAA Security Regulation; if none do, document that fact. Every internal clearinghouse must have access policies in place that are compliant with the HIPAA Privacy Rule	Is there a set of rules and procedures in place to safeguard ePHI if healthcare clearinghouse operations are carried out? Is the healthcare clearinghouse a component of a larger firm that uses the same servers and other IT infrastructure? Does the healthcare clearinghouse have its dedicated employees, or does it collaborate with other businesses? Has the healthcare clearinghouse been given its dedicated network or subsystem, if one can be found to be practical and effective?
1.4.2 Implement policies and procedures for authorizing access	Adopt methods of providing access to ePHI, such as a workstation, transaction, program, process, or other means Workforce members' access to ePHI must be decided upon and documented To limit who can see ePHI, a justification must be made first The first step is to decide on an access control method (e.g., identity-based, role-based, or other reasonable and appropriate means of access) Determine and record the policies and procedures for providing privileged users with access to ePHI Based on the risk assessment, decide if a combination of access control measures is sufficient for ePHI security Find out if there may ever be a time when outsiders need direct access to ePHI.	Has access been granted after proper authorization and clearance procedures? Are there permissions settings in place within the company's IT infrastructure? Do written job descriptions exist that appropriately represent assigned activities and responsibilities and uphold the division of duties? Are there written policies outlining who will be permitted access to ePHI and how? Does the company permit access to ePHI remotely? How is ePHI secured? (Is it through identity-based, role-based, location-based, or other method?) To what extent do users who need access to administrative controls need to be authenticated?
1.4.3 Implement policies and procedures for access establishment and modification	Establish, document, review, and amend an individual's right of access to a system, transaction, program, or process by the covered entity's or business associate's access authorization policy Set guidelines for approving requests to view ePHI Access to ePHI requires official authorization from the competent authority To guarantee that access to ePHI is still authorized and required, it is important to conduct regular reviews of the relevant personnel's access privileges.	Are responsibilities divided such that each worker only has access to their specific, job-related ePHI? Are choices about access properly documented, authorized, and retained? How often is access to ePHI assessed (to make sure it's still necessary)? Are reviews of access to ePHI and related decisions recorded and kept? Are records kept of who gets access to ePHI and how that access is granted and revoked?

Table 5: Security awareness and training

1. Administrative safeguards; 1.5. Security awareness and training		
HIPAA Standard: Implement a security awareness and training program for all members of its workforce (including management) (Marron, 2022)		
Security control	Definition	Questions to Consider
1.5.1 Conduct a training needs assessment	Establish what training requirements exist within the company Key individuals should be interviewed and included in determining security training requirements Determine training needs through the study of prior occurrences and responses to those analyses Determine what training is lacking or requires reinforcement, improvement, or periodic reminders by reviewing organizational behavior concerns, historical occurrences, and/or breaches	In what ways may education, training, and awareness be improved? Which ones are necessary? Is there a system in place to keep track of potential areas of weakness and identify new threats? Should employees be educated on the latest security dangers (such as phishing and ransomware)? Does the business use any devices (such as medical IoT) or technologies that could compromise ePHI? If so, does the team need training on those technologies? How are these requirements currently being met, and how effective are current solutions?
1.5.2 Develop and approve a training strategy and a plan	Throughout the security awareness and training program, focus on the specific HIPAA policies that call for such awareness and training Organizational norms for the security of ePHI must be established Documenting the security awareness and training program's goals, intended audiences, learning objectives, deployment strategies, assessment and measurement tools, and training cycles is essential	Is there a system in place to provide security awareness training to all employees, including those who work remotely? What kind of security training is needed to handle certain technical issues based on job responsibility? When should classes be held so that regulatory requirements can be satisfied on time?
1.5.3 Develop appropriate awareness and training content, materials, and methods	Choose what will be included in the training materials, keeping in mind timely issues (such as phishing and email security) that must be addressed to safeguard ePHI Update the plan with relevant and timely data from sources such as email alerts, online IT security daily news websites, and publications Think about employing a wide range of media and channels, tailoring to the approach of the company's needs in terms of workforce size, geography, education level, etc To keep ePHI safe, training should be a continual, ever-evolving process in response to environmental and operational changes.	Is the focus of training and awareness activities well-aligned with the dangers and weaknesses found in risk analysis? Does the company regularly analyze whether or not the training and awareness it provides are relevant in light of changes to the risk assessment and new dangers? Can workers easily access and read over the company's security policies and procedures? Do workers know whom to call and what to do in the event of a security breach? Do workers know what would happen if they don't follow the rules? Are the security policies communicated to workers? Do employees have to deal with physical laptop security risks and information security difficulties while traveling, teleworking, or working remotely? Are there any training resources that the regulated entity has looked into? Is there a security training team in place to provide instruction? And who will teach those who need it?
1.5.4 Implement the training	Put together a plan and timetable for the training that will be required to implement the plan Distribute security messages throughout a business using any feasible method, such as newsletters, screensavers, video recordings, email messages, teleconferencing sessions, staff meetings, and online training	If security is a priority, has every worker received the training they need? What happens if workers don't take the training classes they're supposed to?

Table 6: Facility access controls

2. Physical safeguards; 2.1. Facility access controls		
HIPAA Standard: Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed (Marron, 2022)		
Security control	Definition	Questions to consider
2.1.1 Conduct an analysis of existing physical security vulnerabilities	Do a thorough audit of the premises and locate any weaknesses in the building's current physical protection measures Assign severity levels to each vulnerability, and check that authorized users have access Identify the locations, such as data centers, that need access controls to protect ePHI.	Are there locks and cameras on off-limits places if they seem reasonable and appropriate? Can unauthorized people access or view data stored on computers? Where ePHI is stored, how secure are the entry and exit points? Is there an established set of guidelines for getting into and making use of the space and its resources? Are there potential environmental calamities that might be either natural or caused by humans?
2.1.2 Identify corrective measures	Determine and allocate responsibility for the actions and activities necessary to address problems, and ensure that proper physical access is granted Create and implement policies and procedures to guarantee that the right parts of the building receive the right upgrades and maintenance at the right times.	Whose duty is it to ensure safety? Is there someone on staff besides the security professional accountable for the safety of the building and its contents? Have policies and procedures been established for controlling access to the facility? Should they be changed? What kind of education will workers need to follow the rules and regulations? In what ways will progress and outcomes be recorded?
2.1.3 Develop a facility security plan	The institute should measure to prevent break-ins, tampering, and theft of the building and its contents ePHI in the custody of a regulated entity must be protected by appropriate physical security measures Be sure to document the stock of the building, as well as the physical maintenance records and the evolution of any alterations Locate all entrances and exits and take stock of the current security measures	Is there a record of the buildings and the current safety measures taken? To what extent are the premises (outside, interior, equipment, access controls, maintenance records, etc.) secured at present? Is there a member of staff besides the security professional who is in charge of the building layout? Is there a backup plan, and if not, is one being formulated?
2.1.4 Develop access control and validation procedures	Provide access to authorized personnel and visitors while keeping out unauthorized individuals by establishing procedures to control and validate a person's access to facilities based on their role or function, such as visitor control and control of access to software programs for testing and revision	What are the rules and regulations for screening employees, outside contractors, guests, and new hires? Do the procedures specify which users, groups, or job functions may access the software for evaluation and improvement? In each building, how many different types of entry points are there? Are monitoring devices needed?
2.1.5 Maintain maintenance records	Establish policies and procedures for recording changes made to the building's infrastructure that affect security (e.g., hardware, walls, doors, and locks).	Does the organization have rules and processes in place that outline the best way to record changes made to the security-related elements of a building? Do you keep track of when hardware, walls, doors, and locks need fixing and when they are fixed?

Table 7: Workstation security

2. Physical safeguards; 2.2. Workstation security		
HIPAA Standard: Implement physical safeguards for all workstations that access ePHI to restrict access to authorized users (Marron, 2022)		
Security control	Definition	Questions to Consider
2.2.1 Identify all methods of physical access to workstations and devices	List all of the methods by which anyone can get to the computers and other equipment used in the production, storage, processing, or transmission of ePHI. Take into account the wide variety of computing devices, including medical devices, medical IoT devices, tablets, smartphones, etc Think about any mobile devices that leave the physical facility, as well as remote workers who access devices that create, store, process, or transmit ePHI	Is there a list of where all the devices are at the moment? How about in public places? Are there any devices available for use? Is ePHI created, accessed, stored, processed, or sent using portable computers (laptops, desktops, etc.) as workstations?
2.2.2 Analyze the risk associated with each type of access	Determine which type of access identified in Key Activity 1 poses the greatest threat to the security of ePHI	Does equipment ever leave the building, or is any equipment stored in a place where it could be misused, stolen, or accessed by unauthorized parties?
2.2.3 Identify and implement physical safeguards for workstations and devices	Reduce the likelihood of unauthorized access to ePHI by putting in place physical safeguards and other security measures Other protections, such as: - limiting device capabilities to access ePHI - limiting user rights to access ePHI, should be considered if there are obstacles to physically safeguarding devices and/or the facility where they are located Encrypting Hardware Protections that are extremely difficult to bypass (like multi-factor authentication) and a lock on the screen Controlling hardware (e.g., Mobile Device Management [MDM], Endpoint Detection and Response [EDR]) Workforce training and education concerning the dangers of remote and mobile computing to ePHI	How to ensure that only authorized individuals can access ePHI? What kinds of safety measures (such as secured doors, screen barriers, cameras, and guards) are in place? Is it necessary to use more stringent physical measures to keep electronic personal data secure? Should any equipment be moved to improve the building's physical safety? Have staff members received security training? What percentage of the organization's gadgets does not belong to it?

Table 8: Device and media controls

2. Physical safeguards; 2.3. Device and media controls		
HIPAA Standard: Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain ePHI into and out of a facility, and the movement of these items within the facility (Marron, 2022)		
Security control	Definition	Questions to Consider
2.3.1 Implement methods for the final disposal of ePHI	Adopt measures to dispose of ePHI and any associated hardware or electronic media Figure out and record the best ways to dispose old computer parts, programs, and data Make sure ePHI is permanently deleted	What types of ePHI does the company generate, maintain, process, and send, and on what storage mediums does this occur? Is information kept in rewritable forms (such as flash drives) that can be easily transported and reused? Have policies and procedures been established and followed regarding the deletion or destruction of ePHI and/or the hardware and media on which ePHI is stored? Is there a way to permanently delete information from all storage devices?
2.3.2 Develop and implement procedures for the reuse of electronic media	Put in place measures to ensure that ePHI is deleted from storage devices before they are reused Be sure that any electronic material you have used to store ePHI cannot be accessed or used again Learn to recognize removable media and explain how to use it effectively Be sure that any medium that has previously held ePHI has been purged before being reused to store more data	Is there already a set of rules and regulations in place for recycling computers and other electronic devices? Had previously stored ePHI been completely removed from any repurposed media? Is there a single point of contact or department in charge of managing data deletion and hardware/ software refurbishment? Are personnel aware of the dangers to ePHI that can arise from recycling hardware and software?
2.3.3 Maintain accountability for hardware and electronic media	Keep track of where your hardware and electronic media have been and who has been handling them Prevent the accidental disclosure or sharing of ePHI Have someone keep track of who receives and returns any devices used to access ePHI	Is there a system in place to track who has access to and where ePHI-containing hardware and electronic media are stored? How and where is information kept (on what medium)? What procedures already exist to track hardware and software within the organization (e.g., an enterprise inventory management system)? Do mechanisms exist to externally trace electronic media containing or used to access ePHI if employees are permitted to remove such media? When it comes to computer hardware and software, whose job is it to keep track of it?
2.3.4 Develop data backup and storage procedures	Where necessary, before relocating any ePHI, make an exact copy of all relevant files For the sake of ePHI, make sure to back up all data before relocating any machines	Is there a protocol in place to back up ePHI before a server or computer is relocated? If data is destroyed during shipment or movement of electronic media holding ePHI, are backup files maintained offshore to ensure data availability? What would happen to the business if data lost for a while when media was being moved or transported?

Table 9: Access control

3. Technical safeguards; 3.1. Access control		
HIPAA Standard: Implement technical policies and procedures for electronic information systems that maintain ePHI to allow access only to those persons or software programs that have been granted access rights (Marron, 2022)		
Security control	Definition	Questions to consider
3.1.1 Analyze workloads and operations to identify the access needs of all users	Find a method of controlling entry To ensure that only authorized individuals, processes, and services have access to ePHI, it is important to take into account all applications and systems that store such information The process of providing and managing access should be made more cohesive with these actions	Can every program or service that stores or processes ePHI be named? Which user roles are established for these programs and databases? Is restricted access maintained for systems housing ePHI? Where does the ePHI that these programs and services rely on now reside (i.e., computer, network drive, database)?
3.1.2 Identify technical access control capabilities	Analyze the ePHI system's access control features Find out if the current infrastructure of the network can restrict access to the systems containing ePHI (e.g., network segmentation) Use information access management policies and procedures to restrict access to ePHI to only those who need it	How does someone get into the systems to look at data or change it? Asking if the regulated business can demonstrate that the identified technical access controls allow only authorized users to access ePHI by the policies and procedures established for information access management.
3.1.3 Ensure that all system users have been assigned a unique identifier	Provide a one-of-a-kind identifier for each user so that their actions within the system may be tracked back to them Make sure the system logs contain all the information needed for auditing and other relevant business purposes	To what extent (in terms of length and content) should the identification be determined? Which is preferable: a unique identifier chosen by the individual, one assigned by the organization, or one produced at random? Can ePHI access be monitored using the user's identifier?
3.1.4 Develop access control policy and procedures	A formal policy for access control must be established to serve as a foundation for further procedure creation To make access control a reality, it's important to lay out requirements that are both doable and affordable	Have guidelines for user conduct been established and disseminated? When and how will norms be policed?
3.1.5 Implement access control procedures using selected hardware and software	Put the plan into action with the help of the tools already acquired	Who will be in charge of the security measures? Have the people who will be using the access control system in the future been given any training? How much time will it take to train users on the new access control system?
3.1.6 Review and update access for users and processes	Make following rules and regulations an integral part of doing business Assess the current state of access control systems and decide whether or not any adjustments are necessary Maintain the integrity of the regulated entity's information access management policies and procedures in light of any changes to the technical controls that affect a user's access to ePHI Users may need to change their access settings, so be sure to put in place a system for doing so They can get: - Access for the first time - More access - Access to systems and applications beyond what they already have	Have all new employees/ users received adequate training on how to keep data and systems secure? How can access to information and/or software can be gained as a new employee/ user? Is there a mechanism in place to assess the permissions granted to current users, services, and processes, and make any necessary adjustments? Do people and processes, as well as the systems that generate, store, process, and communicate ePHI, have access to just the data to which they are authorized? While analyzing the requirements for user and process access, has the regulated entity considered implementing an automated system?
3.1.7 Establish an emergency access procedure	Create a plan for accessing critical ePHI in a time of crisis when it can be obtained electronically If standard access is disabled or unavailable due to technical issues, you must devise a plan to ensure that business can continue as usual	Can ePHI be accessed in an emergency according to established policies and procedures? In what circumstances must the emergency access technique be used? Who can make this call, if anyone? Who is responsible for which tasks? Will systems have pre-configured settings and functions that allow the emergency access procedure, or will the mode need to be triggered by the system administrator or another authorized individual?
3.1.8 Terminate access if it is no longer required	If an individual's permission to access their ePHI has lapsed, they should immediately remove themselves from any further access To guarantee the principle of least privilege is followed, it is recommended to institute a recertification process for users	Are regulations being implemented to remove access by staff members who no longer need to know because they have changed assignments or have quit working for the organization? Does the company frequently review access requirements to make sure the least privilege is given to each user?

Table 10: Integrity

3. Technical Safeguards; 3.2. Integrity		
HIPAA Standard: Implement policies and procedures to protect ePHI from improper alteration or destruction (Marron, 2022)		
Security control	Definition	Questions to consider
3.2.1 Identify all users who have been authorized to access ePHI	Determine who, if anyone, is authorized to make changes to or delete ePHI It is recommended to tackle this Key Activity in tandem with Key Activity, which focuses on locating suspicious data sources	How are authorized users granted access? Do they have a legitimate reason for requiring access? Are they aware of how to make use of the data? Is there a record of who accessed the data and when?
3.2.2 Identify any possible unauthorized sources that may be able to intercept the information and modify it	Determine what kinds of attacks could lead to unauthorized changes to the ePHI (e.g., hackers, ransomware, disgruntled employees, and business competitors)	Where could potential threats to data security originate? When data is stored in a system, it raises the question, "How can we ensure that it remains unaltered? How can it be ensured that information is transmitted with as little chance of modification as possible?
3.2.3 Develop the integrity policy and requirements	Based on the analysis performed in Steps 1 and 2, create a formal (written) set of integrity standards	Have all relevant stakeholders discussed and approved the requirements? Has a formal policy been drafted and distributed to employees?
3.2.4 Implement procedures to address these requirements	Determine and execute measures to prevent unauthorized changes to ePHI Determine the methods and resources that need to be created or acquired to ensure integrity, then put them into action.	What other methods (such as quality control processes or reconstructing transactions and outputs) can be used to ensure the authenticity of ePHI if these are not enough? Does the organization have anti-malware, anti-ransomware, and file integrity monitoring technologies in place to protect ePHI against unauthorized changes or deletions?
3.2.5 Implement a mechanism to authenticate ePHI	Put in place digital checks to verify that ePHI has not been tampered with or deleted without authorization Possible integrity-checking mechanisms include: memory that can fix itself, and signatures in digital form	IS there a need to employ both electronic and non-electronic procedures to keep ePHI secure? Is there access to secure electronic authentication methods? Is there evidence that the electronic authentication technologies now available are compatible with other software and hardware?
3.2.6 Establish a monitoring process to assess how the implemented process is working	Check-in on the methods currently in place to see if they're meeting the goals Changes in technology and operating environments should prompt regular reviews of integrity processes to identify whether or not any adjustments are necessary	Do reports of information integrity issues exist, and if so, have they diminished after integrity processes were put in place? Is there more confidence that data integrity is being protected now that the process has been put into place?

Table 11: Person or entity authentication

3.3. Technical safeguards; 3.3. Person or entity authentication		
HIPAA Standard: Implement procedures to verify that a person or entity seeking access to ePHI is the one claimed (Marron, 2022)		
Security control	Definition	Questions to consider
3.3.1 Determine authentication applicability to current systems/applications	Determine the various authentication options. For the HIPAA Security Regulation, authentication is providing evidence that an individual is who they say they are Locate Authentication-Required Electronic Access Points (and that should require authentication if not currently required) Verify that such access points are correctly accounted for in the regulated entity's risk analysis (e.g., risks of unauthorized access from within the enterprise could be different from those of remote unauthorized access) Authentication is the process of determining the reliability of a source of transmission or the legitimacy of a person's claim to have been granted access to a restricted set of data or network resources	What options are there for methods of authentication: Is it possible to limit the risks of unauthorized access at each point of electronic access using the current authentication methods? Is there a way to estimate how much it will cost to implement each of the potential strategies in the setting? Should in-house help be relied on, or should it be possible to outsource it? Is it necessary to use passwords? Do these traits distinguish one person from another? Is multi-factor authentication being used? If that's the case, how and where does it operate?

Table 12: Transmission security

3. Technical safeguards; 3.4. Transmission security		
HIPAA Standard: Implement technical security measures to guard against unauthorized access to ePHI that is being transmitted over an electronic communications network (Marron, 2022)		
Security control	Definition	Questions to consider
3.4.1 Identify any possible unauthorized sources that may be able to intercept and/or modify the Information	Determine all entry points, internal channels, and exit points through which ePHI will go Determine transmission contexts (such as telemedicine or claims processing) in which ePHI may be accessed by, or altered by, unauthorized parties (e.g., hackers, disgruntled employees, business competitors) To determine the potential dangers to ePHI, the situations and routes that could lead to such dangers must be first recognized	Have all potential channels for ePHI transmission been mapped out? To what extent have situations and channels of transmission that represent a high risk to ePHI been identified using the risk assessment? Which safeguards prevent transmission vulnerabilities form ePHI? Have adequate safeguards been established for all possible transmission contexts and channels of ePHI? To what extent do broadcasts get monitored by trained personnel?
3.4.2 develop and implement transmission security policy and procedures	Provide a strict (written) protocol for the transfer of ePHI Determine the means of transmission that will be utilized to protect ePHI Determine what resources will be made available to back up the transmission security policy If necessary, put in place processes for sending ePHI utilizing hardware and/or software	Have the requirements been considered and accepted by key persons identified in the transmission of ePHI? Has a documented procedure been made available to users of the system?
3.4.3 Implement integrity controls	Include safeguards to prevent unauthorized changes to electronically transmitted ePHI up until the point it is deleted	When transmitting ePHI, what safeguards are in place to ensure patient confidentiality? What precautions would be taken to ensure the security of ePHI during transmission? Is there assurance that information is not altered during transmission?
3.4.4 Implement encryption	Protect ePHI by using a suitable encryption method	Is it acceptable to encrypt ePHI during transmission? Is encryption necessary to prevent data theft during transmission, given the results of the risk analysis? When communicating with people outside of the company, has the company explored using email encryption and automated confidentiality statements? Should the data be encrypted in this setting? Is it practical and affordable? Is there a list of available encryption algorithms and methods somewhere? Are the current encryption techniques and processes adequately safeguarding ePHI while transmitting over the internet? Is the hardware/ software used for electronic communications set up to prevent the use of a lower degree of encryption, which would provide insufficient protection for ePHI during transmission? Does the covered entity have the necessary personnel to manage a process for transmitting ePHI in a secure manner? To what extent do employees have expertise with encryption technology?

Table 13: Interview questions

Q	Administrative safeguards
1	Has all ePHI generated, stored, processed, and transmitted within the organization been identified?
2	Will new security controls work with the existing IT architecture?
3	Have employees been made aware of policies concerning sanctions for inappropriate access, use, and disclosure of ePHI?
4	Is there a complete job description that accurately reflects assigned security duties and responsibilities?
5	Have the staff members in the organization been notified as to whom to call in the event of a security problem?
6	Have chains of command and lines of authority been established?
7	Are there written job descriptions that are correlated with appropriate levels of access to ePHI?
8	Is there an implementation strategy that supports the designated access authorities?
9	Has a staff of the healthcare clearinghouse been trained to safeguard ePHI from disclosure to the larger organization, if required for compliance with the HIPAA Privacy Rule?
10	Do the organization's systems have the capacity to set access controls?
11	Does the organization grant remote access to ePHI?
12	Are duties separated such that only the minimum necessary ePHI is made available to each staff member based on their job requirements?
13	Is personnel access to ePHI regularly reviewed to ensure that access is still authorized and needed?
14	Is the organization monitoring current threats to determine possible areas of training needs?
15	Is there a procedure in place to ensure that everyone in the organization, including teleworkers and remote personnel, receives security awareness training?
16	Do employees know the importance of the timely application of system patches to protect against malicious software and the exploitation of vulnerabilities?
Q	**Physical safeguards**
17	Do policies and procedures already exist regarding access to and use of facilities and equipment?
18	Do the policies and procedures identify devices that access ePHI and those that do not?
19	Do the policies and procedures address the use of these devices for any personal use?
20	Do the policies and procedures specify where to place devices to only allow viewing by authorized personnel?
21	Are physical safeguards implemented for all devices that access ePHI to restrict access to authorized users?
22	Are policies and procedures developed and implemented that address the disposal of ePHI and/or the hardware and media on which ePHI is stored?
23	Is there a process for destroying data on all media?
24	Are employees appropriately trained on the security risks to ePHI when reusing software and hardware?
Q	**Technical safeguards**
25	Have all applications and systems with ePHI been identified?
26	Is access to systems containing ePHI only granted to authorized processes and services?
27	Are audit records generated for all systems/devices that create, store, process, or transmit ePHI?
28	Have all pathways been identified by which ePHI will be transmitted?

5.1. ePHI security analysis and recommendation

After analyzing the responses to the set of questions that were asked to cybersecurity experts, it was evident that there is a major lack of security control to protect ePHI. The achieved level of compliance for administrative safeguards, physical safeguards, and technical safeguards were only 44%, 63%, and 50%, respectively. The results are demonstrated in Fig. 5, Fig. 6, and Fig. 7.

Table 14: ePHI compliance interview - overall compliance level

Security rules	Overall security level
Administrative safeguards	43%
Physical safeguards	62%
Technical safeguards	50%

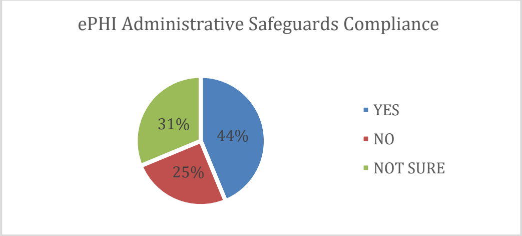

Fig. 5: ePHI administrative safeguards compliance

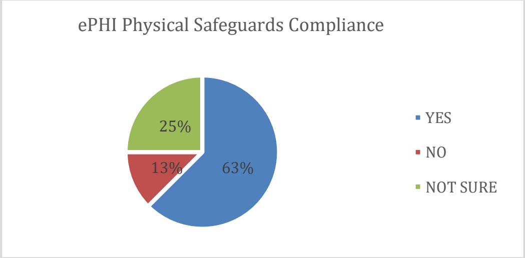

Fig. 6: ePHI physical safeguards compliance

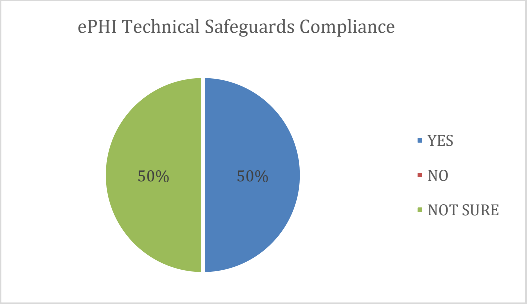

Fig. 7: ePHI technical safeguards compliance

5.2. Mitigation action to fix the missing controls

Table 15 presents the prospective points of improvement for the lost security measures that are present in the current security controls.

6. Conclusion and future work

This paper presents the compliance procedure that will clarify and simplify the protection of ePHI through the adoption of the HIPAA standards and the implementation of the three security rules, 18 security measures, and 87 security controls. Due to the many changes that are taking place around the globe, the safeguards and protections that are in place need to be continually modernized. The globe is currently seeing huge transformations in the digital infrastructure, the expansion of the use of data inside health institutions, and the involvement of the regular user or beneficiary of medical services. All these developments are taking place simultaneously. As a result of the cumulative effect of all these factors, security controls must be continually updated.

Table 15: Mitigation action

Q	Missing countermeasure	Security rule	Mitigation action	Security control
3	Have employees been made aware of policies concerning sanctions for inappropriate access, use, and disclosure of ePHI?	Administrative safeguards	Retaliate against employees who violate the security rules and procedures of the covered company or business associate in an acceptable manner; Execute sanction policy when situations emerge; create rules and procedures for implementing appropriate sanctions	1.1.6 develop and implement a sanction policy
5	Have the staff members in the organization been notified as to whom to call in the event of a security problem?	Administrative safeguards	Job descriptions are useful for recording the tasks that have been delegated to a certain person; Make sure everyone in the company is aware of their new responsibilities	1.2.2 assign and document the individual's responsibility
6	Have chains of command and lines of authority been established?	Administrative safeguards	Establish measures to control who may access ePHI and where it can be accessed by workforce members	1.3.1 implement policies and procedures for authorization and/or supervision
9	Has the staff of the healthcare clearinghouse been trained to safeguard ePHI from disclosure to the larger organization, if required, in compliance with the HIPAA privacy rule?	Administrative safeguards	Clearinghouses that are subsets of larger organizations are required to take precautions to prevent their parent company from gaining access to their ePHI	1.4.1 isolate healthcare clearinghouse functions
10	Do the organization's systems have the capacity to set access controls?	Administrative safeguards	Adopt methods of providing access to ePHI, such as a workstation, transaction, program, process, or other means	1.4.2 implement policies and procedures for authorizing access
11	Does the organization grant remote access to ePHI?	Administrative safeguards	Workforce members' access to ePHI must be decided upon and documented	1.4.2 implement policies and procedures for authorizing access
12	Are duties separated such that only the minimum necessary ePHI is made available to each staff member based on their job requirements?	Administrative safeguards	Establish, document, review, and amend an individual's right of access to a system, transaction, program, or process by the covered entity's or business associate's access authorization policy	1.4.3 implement policies and procedures for access establishment and modification
15	Is there a procedure in place to ensure that everyone in the organization, including teleworkers and remote personnel, receives security awareness training?	Administrative safeguards	Throughout the security awareness and training program, focus on the specific HIPAA policies that call for such awareness and training	1.5.2 develop and approve a training strategy and a plan
16	Do employees know the importance of the timely application of system patches to protect against malicious software and the exploitation of vulnerabilities?	Administrative safeguards	Employees should receive as much reasonable and relevant instruction as possible in the following areas: preventing, detecting, and reporting dangerous software; keeping track of login attempts and reporting anomalies; and making, updating, and protecting passwords	1.5.3 protection from malicious software, login monitoring, and password management
19	Do the policies and procedures address the use of these devices for any personal use?	Physical safeguards	Conceive and record protocols for handling devices that generate, store, process, or transmit ePHI.	2.2.2 identify the expected performance of each type of workstation and device
20	Do the policies and procedures specify where to place devices to only allow viewing by authorized personnel?	Physical safeguards	Make sure you've identified and thought through any potential dangers that could arise from a device's environment	2.2.3 analyze physical surroundings for physical attributes
24	Are employees appropriately trained on the security risks to ePHI when reusing software and hardware?	Physical safeguards	Put in place measures to ensure that ePHI is deleted from storage devices before they are reused	2.4.2 develop and implement procedures for the reuse of electronic media
27	Are audit records generated for all systems/ devices that create, store, process, or transmit ePHI?	Technical safeguards	Based on the regulated entity's risk assessment and other organizational variables, determine the appropriate extent of audit controls that will be necessary for information systems that hold or use ePHI	3.2.1 determine the activities that will be tracked or audited
28	Have all pathways been identified by which ePHI will be transmitted?	Technical safeguards	Determine all entry points, internal channels, and exit points through which ePHI will go	3.5.1 identify any possible unauthorized sources that may be able to intercept and/or modify the information

Within the context of Saudi Arabia, the authors have arrived at the realization that the research needs the cooperation of government agencies in the country to modify and improve the proposed security framework to comply with current compliances, as well as to increase awareness among various parts of the Saudi society. The industry is in the midst of a dramatic shift from paper to digital health records. It has developed methods to aid healthcare practitioners during this shift by standardizing administrative procedures, increasing productivity, and preserving the privacy of patient data. It is apparent that healthcare providers, insurance firms, and other organizations can easily share patient data. However, private details are included within ePHI, such as credit card numbers, social security numbers, and specifics about medical issues and procedures. Such confidential information has high value due to the identity theft risks it poses. Without HIPAA, healthcare providers would be under no obligation to safeguard this sensitive information, and they would face no consequences for failing to do so. Currently, healthcare facilities in Saudi Arabia are mandated by law to implement a comprehensive set of security measures to safeguard patients' health records. However, staff members and practitioners need to be educated on the importance of patient privacy. We believe the proposed security framework built on the rules set forth by HIPAA will address the identified gap and provide the healthcare infrastructure in Saudi Arabia with the security measures needed to safeguard ePHI.

Future work is planned to benchmark the proposed framework with other related work to ensure all aspects are covered. Moreover, a deeper analysis of the specific challenges and characteristics of the Saudi context in the healthcare system will be conducted to enrich the framework. Once a final version of the framework is ready, it will be implemented to evaluate its feasibility, suitability, and reliability and update the framework accordingly. Finally, for the purpose of enhancing the value of the framework and providing a holistic view, a comparison of the impact achieved with other countries and regions will be performed.

Compliance with ethical standards

Conflict of interest

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

References

Al Hamid HA, Rahman SM, Hossain MS, Almogren A, and Alamri A (2017). A security model for preserving the privacy of medical big data in a healthcare cloud using a fog computing facility with pairing-based cryptography. IEEE Access, 5: 22313-22328. https://doi.org/10.1109/ACCESS.2017.2757844

Alabdulatif A, Khalil I, Yi X, and Guizani M (2019). Secure edge of things for smart healthcare surveillance framework. IEEE Access, 7: 31010-31021. https://doi.org/10.1109/ACCESS.2019.2899323

Al-Kahtani N, Alrawiai S, Al-Zahrani BM, Abumadini RA, Aljaffary A, Hariri B, Alissa K, Alakrawi Z, and Alumran A (2022). Digital health transformation in Saudi Arabia: A cross-sectional analysis using healthcare information and management systems society' digital health indicators. Digital Health. https://doi.org/10.1177/20552076221117742 **PMid:35959196 PMCid:PMC9358341**

Almalki M, Fitzgerald G, and Clark M (2011). Health care system in Saudi Arabia: An overview. Eastern Mediterranean Health Journal, 17(10): 784-793. https://doi.org/10.26719/2011.17.10.784 **PMid:22256414**

Alzahrani AG, Alhomoud A, and Wills G (2022). A framework of the critical factors for healthcare providers to share data securely using blockchain. IEEE Access, 10: 41064-41077. https://doi.org/10.1109/ACCESS.2022.3162218

Attallah N, Gashgari H, Al Muallem Y, Al Dogether M, Al Moamary E, Almeshari M, and Househ M (2016). A literature review on health information exchange (HIE). In: Mantas J, Hasman A, and Gallos G (Eds.), Unifying the applications and foundations of biomedical and health informatics: 173–176. IOS Press, Amsterdam, Netherlands.

Czernek-Marszałek K and McCabe S (2024). Sampling in qualitative interview research: criteria, considerations and guidelines for success. Annals of Tourism Research, 104: 103711. https://doi.org/10.1016/j.annals.2023.103711

Duggineni S (2023). Impact of controls on data integrity and information systems. Science and Technology, 13(2): 29-35.

Hathaliya JJ and Tanwar S (2020). An exhaustive survey on security and privacy issues in Healthcare 4.0. Computer Communications, 153: 311–335. https://doi.org/10.1016/j.comcom.2020.02.018

Hussain F, Abbas SG, Shah GA, Pires IM, Fayyaz UU, Shahzad F, Garcia NM, and Zdravevski E (2021). A framework for malicious traffic detection in IoT healthcare environment. Sensors, 21(9): 3025. https://doi.org/10.3390/s21093025 **PMid:33925813 PMCid:PMC8123414**

Keshta I and Odeh A (2021). Security and privacy of electronic health records: Concerns and challenges. Egyptian Informatics Journal, 22(2): 177-183. https://doi.org/10.1016/j.eij.2020.07.003

Marron JA (2022). Implementing the health insurance portability and accountability act (HIPAA) security rule: A cybersecurity resource guide. National Institute of Standards and Technology, Gaithersburg, USA. https://doi.org/10.6028/NIST.SP.800-66r2.ipd

Seh AH, Zarour M, Alenezi M, Sarkar AK, Agrawal A, Kumar R, and Khan RA (2020). Healthcare data breaches: Insights and implications. Healthcare, 8(2): 133. https://doi.org/10.3390/healthcare8020133 **PMid:32414183 PMCid:PMC7349636**

Shah SM and Khan RA (2020). Secondary use of electronic health record: Opportunities and challenges. IEEE Access, 8: 136947–136965. https://doi.org/10.1109/ACCESS.2020.3011099

Tervoort T, De Oliveira MT, Pieters W, Van Gelder P, Olabarriaga SD, and Marquering H (2020). Solutions for mitigating cybersecurity risks caused by legacy software in medical devices: A scoping review. IEEE Access, 8: 84352-84361. https://doi.org/10.1109/ACCESS.2020.2984376

Tucker K, Branson J, Dilleen M, Hollis S, Loughlin P, Nixon MJ, and Williams Z (2016). Protecting patient privacy when sharing patient-level data from clinical trials. BMC Medical Research Methodology, 16(Suppl 1): 77. https://doi.org/10.1186/s12874-016-0169-4 **PMid:27410040 PMCid:PMC4943495**