Seminars in Medical Writing and Education. 2024; 3:498
doi: 10.56294/mw2024498

ORIGINAL

Risk Analysis of Data Privacy Violations in Digital Health Records and Patient Confidentiality

Análisis del riesgo de violación de la privacidad de los datos en los historiales médicos digitales y la confidencialidad de los pacientes

Sujayaraj Samuel Jayakumar[1], Kunal Meher[2], Udaybhanu Rout[3], Gujjala Srinath[4], Shivam Khurana[5], Sukhman Ghumman[6], Shilpi Singh[7]

[1]Forensic science, JAIN (Deemed-to-be University). Bangalore, Karnataka, India.
[2]Department of uGDX, ATLAS SkillTech University. Mumbai, Maharashtra, India.
[3]Department of General Medicine, IMS and SUM Hospital, Siksha 'O' Anusandhan (Deemed to be University). Bhubaneswar, Odisha, India.
[4]Centre for Multidisciplinary Research, Anurag University. Hyderabad, Telangana, India.
[5]Chitkara Centre for Research and Development, Chitkara University. Himachal Pradesh, India.
[6]Centre of Research Impact and Outcome, Chitkara University. Rajpura, Punjab, India.
[7]Department of Biotechnology and Microbiology, Noida International University. Greater Noida, Uttar Pradesh, India.

Cite as: Jayakumar SS, Meher K, Rout U, Srinath G, Khurana S, Ghumman S, et al. Risk Analysis of Data Privacy Violations in Digital Health Records and Patient Confidentiality. Seminars in Medical Writing and Education. 2024; 3:498. https://doi.org/10.56294/mw2024498

Submitted: 07-10-2023 **Revised:** 09-01-2024 **Accepted:** 12-05-2024 **Published:** 13-05-2024

Editor: PhD. Prof. Estela Morales Peralta

Corresponding Author: Sujayaraj Samuel Jayakumar

ABSTRACT

The fast growth of digital health tools has changed the way healthcare is provided, making it easier for both people and healthcare workers to get the care they need and more efficient. On the other side, digitising health data seriously compromises patient privacy and data security. The various hazards resulting from violations of data privacy in digital health records are discussed in this article. It emphasises the larger picture for healthcare systems and how these breaches can compromise patient privacy. Patient data is saved and distributed across many platforms as Electronic Health Records (EHRs), cloud computing, and telemedicine become more and more common. This article discusses typical hazards that could lead to unauthorised sharing of private medical records. These cover technological problems in healthcare information systems, insiders, and hackers. The General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA) among other laws, norms, and ethics aimed to safeguard patient data are discussed as well. Making ensuring health data is kept, shared, and accessed securely remains difficult even with current initiatives. Furthermore discussed in this study are many approaches to safeguard patient data including encryption, multi-factor login, and very strong safety measures. Finally, it emphasises how crucial it is for healthcare institutions to have a thorough data security strategy in place so as to establish patient confidence and guarantee adherence to all policies. Keeping data privacy current as digital health technologies evolve helps to safeguard patient privacy and maintain seamless operations of healthcare systems.

Keywords: Data Privacy; Digital Health Records; Patient Confidentiality; Cybersecurity; Electronic Health Records (EHR); Healthcare Regulations.

RESUMEN

El rápido crecimiento de las herramientas sanitarias digitales ha cambiado la forma de prestar asistencia sanitaria, facilitando tanto a las personas como al personal sanitario la obtención de la atención que necesitan y haciéndola más eficiente. Por otro lado, la digitalización de los datos sanitarios compromete seriamente

la privacidad del paciente y la seguridad de los datos. En este artículo se analizan los diversos peligros derivados de la violación de la privacidad de los datos en los historiales médicos digitales. Se hace hincapié en el panorama general de los sistemas sanitarios y en cómo estas violaciones pueden comprometer la privacidad del paciente. Los datos de los pacientes se guardan y distribuyen a través de muchas plataformas a medida que las historias clínicas electrónicas (HCE), la computación en la nube y la telemedicina se hacen cada vez más comunes. En este artículo se analizan los peligros típicos que pueden llevar a compartir sin autorización historiales médicos privados. Se trata de problemas tecnológicos en los sistemas de información sanitaria, información privilegiada y piratas informáticos. También se analizan el Reglamento General de Protección de Datos (RGPD) y la Ley de Portabilidad y Responsabilidad de los Seguros Sanitarios (HIPAA), entre otras leyes, normas y principios éticos destinados a salvaguardar los datos de los pacientes. Garantizar que los datos sanitarios se conservan, comparten y acceden de forma segura sigue siendo difícil incluso con las iniciativas actuales. Además, en este estudio se analizan muchos enfoques para salvaguardar los datos de los pacientes, como el cifrado, el inicio de sesión multifactorial y medidas de seguridad muy estrictas. Por último, se hace hincapié en lo crucial que es para las instituciones sanitarias contar con una estrategia de seguridad de datos exhaustiva para establecer la confianza de los pacientes y garantizar el cumplimiento de todas las políticas. Mantener actualizada la privacidad de los datos a medida que evolucionan las tecnologías sanitarias digitales ayuda a salvaguardar la intimidad del paciente y a mantener un funcionamiento sin fisuras de los sistemas sanitarios.

Palabras clave: Privacidad de Datos; Historias Clínicas Digitales; Confidencialidad del Paciente; Ciberseguridad; Historias Clínicas Electrónicas (HCE); Normativa Sanitaria.

INTRODUCTION

Since digital technologies were adopted into healthcare, patient information is managed, processed, and shared in rather different ways. Good for patients and healthcare professionals alike, moving medical information from paper to digital formats like Electronic Health information (EHRs) has greatly improved patient data efficiency and accessibility. As digital health records gain popularity, more people, meantime, worry about data privacy concerns and patient security. Since healthcare institutions depend more and more on digital platforms, unauthorised access to private patient data has grown to be a significant challenge. This compromises patient confidence in the authorities meant to look after them as well as the security of healthcare systems. Digital health records enable physicians and nurses to rapidly access patient information, therefore facilitating their better coordination of treatment and decision-making process. Additionally enabling physicians to interact with patients from distances and enable workers in various healthcare environments to collaborate better are cloud-based technologies and video services. Digital storage and distribution of patient data puts health information vulnerable to breaches, hackers, and usage even with these benefits.[1] Those who violate data privacy laws might be allowed to see or distribute private information about patients including medical records, ailments, and treatment plans without authorisation. Not only do these types of violations compromise patient privacy, but they also erode the confidence patients have in their healthcare providers qualities required for effective healthcare delivery. Digital health data is susceptible in many different ways. First, a lot of healthcare organisations store and manage health data with the help of outside companies, like cloud service providers. This makes it possible for data to be stolen while it's being sent from one site to another, especially if the third-party service doesn't have enough security measures in place.[2]

Second, the risk of data breaches has grown even more because hackers are getting smarter and healthcare institutions are being hit with ransomware attacks more often. Hackers could take advantage of flaws in healthcare IT systems to get to patient data without permission, which would be very bad for both patients and healthcare organisations. Telemedicine and mobile health (mHealth) apps are also becoming more popular very quickly, which means that more digital patient data is being gathered and sent. There are many good things about these new technologies, but they also make it harder to keep health information private and safe. For example, using personal health devices and smartphone apps for online tracking can put patient data at risk if the data is not properly protected or if the devices do not follow privacy rules.[3] Healthcare providers, even those who mean well, may unintentionally violate data privacy by not putting in place strong data security measures or by not fully understanding the technical risks of storing data digitally. Figure 1 shows a risk study of data privacy violations in digital health records. It looks at possible threats and how they might affect patient privacy.

Many laws and rules have been put in place to protect patient privacy and make sure that health data is handled safely in order to deal with these risks. The Health Insurance Portability and Accountability Act, HIPAA, guarantees American patient health information is maintained secure. HIPAA mandates that organisations and healthcare providers use certain safeguards to maintain accurate, confidential, and easily available health data.

https://doi.org/10.56294/mw2024498

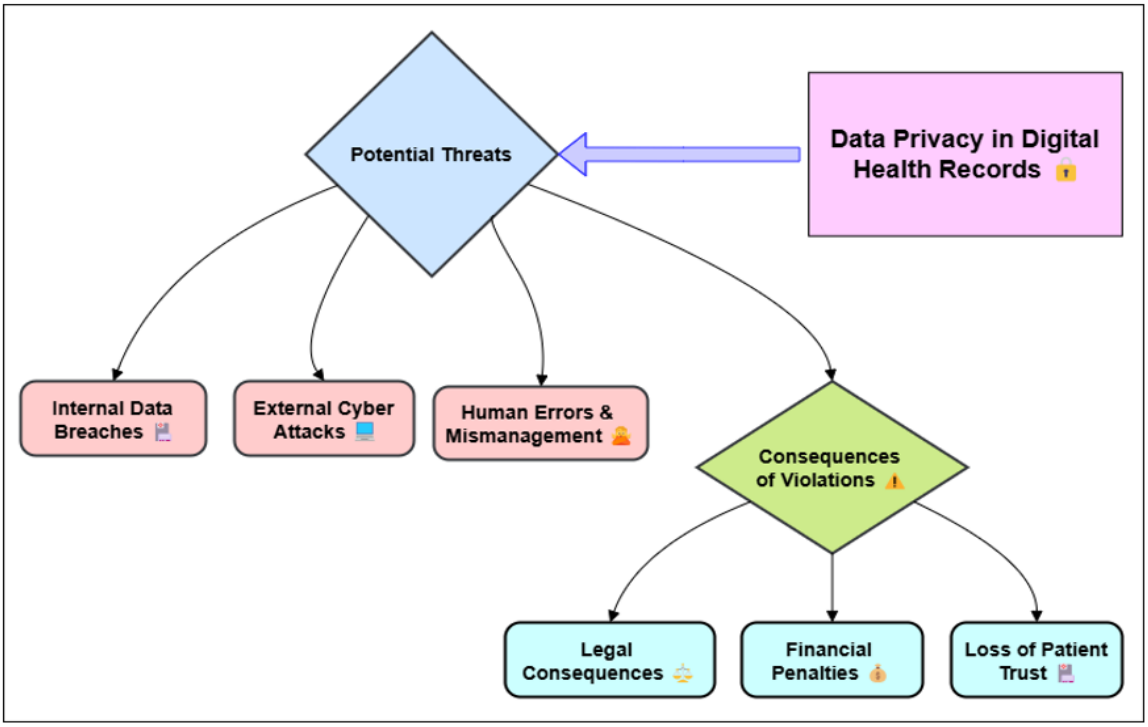

Figure 1. Risk Analysis of Data Privacy Violations in Digital Health Records

Likewise, the European Union's General Data Protection Regulation (GDPR) offers several safeguards for data, including the need of specific patient approval prior to processing medical information. These rules are very important for making sure that data privacy is at least met, but they can be hard to police, especially in the digital health environment, which is changing so quickly.[4] Even with these efforts by regulators, the healthcare sector is still not uniform in how it enforces data privacy rules and uses good security measures. A lot of healthcare organisations, especially smaller practices, might not have the money or time to get the newest hacking tools or teach their staff the best ways to keep data safe. At the same time that digital health tools change, so do the ways that hackers use them. Cyberattacks on healthcare organisations like hacking, ransomware, and malware are getting smarter, which shows that data security needs to keep getting better and healthcare information systems need to be checked on a regular basis.

Literature Review

Overview of Data Privacy in Healthcare

As digital health records spread around the world, data protection in healthcare is becoming more and more important. Healthcare organisations are in charge of keeping private patient data safe. This includes medical reports, treatment records, personal identification information, and diagnosis data. When these records are kept online, they are easier to reach, allow people to work together, and make patient care more efficient. Still, this shift to virtual implies that preserving patient privacy is greater difficult as ever. Healthcare personnel, insurers, and different involved events secure hold this non-public information covered.[5] That is the reason numerous legal guidelines and policies were advanced to shield affected person information and hold public self-assurance in healthcare institutions. Two legal guidelines that virtually define guidelines for healthcare information privateness within the United States and the european Union are the overall facts privateness law (GDPR) and the health insurance Portability and accountability Act (HIPAA). Affected person data needs to be securely saved by using organizations encrypting it and proscribing access to it. Patients also have to be allowed to see, alter, and delete their health information in accordance those recommendations. Records privacy is still an issue despite those guidelines as healthcare institutions cope with complex hazards like inner breaches, hackers, and inadequate safety structure. As virtual technologies like synthetic intelligence (AI), cloud computing, and telemedicine proliferate in healthcare, increasingly more capability dangers to health statistics security floor.[6] These technological developments call for up to date security protocols and additional knowledge about how they might damage patient privateness.

Current Challenges in Protecting Health Data

The growing connection between more and more healthcare systems presents another issue. Patient data is continuously being sent across multiple devices, platforms, and healthcare firms as telemedicine and mobile health applications proliferate.[7] While these instruments simplify patient access to health care, they

potentially compromise data security and privacy. Cybercriminals can get access to private health information on mobile apps or smart health gadgets that don't have enough protection and security features. Also, there is a chronic lack of skilled computer experts working in healthcare. Many healthcare organisations, especially smaller clinics and practices, don't have the money or staff to put in place advanced security measures or teach their staff the best ways to keep patient data safe. This makes healthcare professionals more likely to be hit by scams, malware, and blackmail.[8] Also, people often think that hackers won't be as interested in healthcare as they would be in finance or other businesses. This makes people underestimate how important strong data security really is. The growing number of data breaches and violations shows how important it is to keep improving data protection strategies, spending money on technology, and teaching staff on a regular basis to lower these risks.

Case Studies of Data Breaches and Violations

A lot of well-known examples of data breaches and violations show how badly healthcare needs to improve its data protection measures. In 2015, hackers got into the records of 78,8 million patients at Anthem Inc., one of the biggest health insurers in the US. This was one of the biggest breaches ever. Names, birthdates, Social Security numbers, medical IDs, and job details of patients were made public because of the breach. Because health insurance companies keep a lot of private information, this breach made their weaknesses even clearer. It also showed how hard it is to keep personal health information safe in the digital age, especially when third-party providers are involved. The 2017 hack of the UK's National Health Service (NHS), which was caused by ransomware called WannaCry, was another well-known case.[9] Several NHS hospitals had to cancel appointments and treatments because of the attack, which messed up their services. The breach caused problems with operations right away, but the real risk was that patient information could be seen by anyone. Attacks like this one show how weak public healthcare systems are when they use old technology and don't have good protection. Also, Universal Health Services (UHS), a big U.S. healthcare company, had problems with its electronic health data system after the 2020 hack. UHS had to go back to using paper methods, which made care for patients take longer. Ransomware was responsible for this breach, which showed how threats to healthcare organisations are changing. These case studies show how data breaches can affect many people and stress how important it is to keep strict security rules and take proactive hacking steps to protect patient data.[10]

Table 1. Summary of Literature Review

Method	Challenges	Scope	Impact
Risk Management Framework (RMF)	Implementation complexity	Comprehensive risk management across all assets	Improved risk mitigation and reduced data breaches
Failure Mode and Effects Analysis	Identification of all potential failure points	Analysis of failure modes in healthcare systems	Identification of critical failure points to prevent data exposure
Bowtie Model	Limited visibility of risk causes	Risk visualization for decision-making	Clear visualization of risk management for decision-makers
Encryption[11]	Key management, performance overhead	Data confidentiality during transmission and storage	Secure transmission of sensitive data
Blockchain	Scalability, integration with existing systems	Decentralized secure data storage and sharing	Enhanced data security and integrity in shared environments
Multi-Factor Authentication	User adoption, implementation cost	Secure user authentication	Stronger system protection from unauthorized access
Cloud Computing Security	Ensuring adequate protection across multiple platforms	Data protection in cloud environments	Reduced risk of cloud-related data breaches
Data Access Control[12]	Balancing user accessibility with strict access control	Ensuring least privileged access for users	Prevention of unauthorized access to confidential data
Regular Security Audits	Regular updates and comprehensive coverage	Continuous monitoring and proactive measures	Early detection and remediation of security vulnerabilities
Penetration Testing	High costs, skilled resources required	Simulation of real-world attacks to identify vulnerabilities	Identification of gaps in security measures
Employee Training	Human error, lack of awareness	Educating workforce on data security	Reduced risk of data leakage due to human negligence
Incident Response Planning[13]	Timely and accurate response, resource allocation	Defining clear protocols and processes for breach events	Minimized impact and recovery time during breaches
Compliance with HIPAA and GDPR	Varying enforcement, compliance audits	Ensuring patient data protection through legal standards	Stronger legal and regulatory compliance
Third-Party Vendor Risk Management	Coordinating across multiple external vendors	Ensuring compliance through contract agreements with vendors	Minimized risk from external vendor partnerships

https://doi.org/10.56294/mw2024498

Table 1 summarizes the method, challenges, scope, and impact of studies reviewed, highlighting key issues and potential areas for future research. They also stress how important it is for businesses to use a complete risk management strategy to spot, stop, and deal with new threats to data privacy.

METHOD

Research Design

This study uses a mixed-methods approach, which means that it collects data from both qualitative and quantitative sources. This gives a full picture of how data privacy is broken in digital health records. In-depth case studies of recent data breaches and violations in the healthcare business will be used for the qualitative part. These case studies will help you figure out the main reasons why data privacy is broken, the effects those breaches have, and the steps healthcare organisations take to stop them. We will learn more about the situations that lead to breaches in patient privacy by looking at records that are open to the public, reviews by regulatory bodies, and conversations with healthcare workers and computer experts. As part of the quantitative part of the study, poll data will be gathered from healthcare workers and data security experts to find out how common and useful different data protection methods are in the healthcare sector right now.[14] Using both case study analysis and poll data together makes it possible to "triangulate" the results, which gives us a fuller picture of the risks and difficulties of keeping patient data safe. A study of current literature, legal standards, and security measures in healthcare is also part of the research plan. This gives a theoretical structure for looking at breaches of data protection. The research will be done in stages. First, secondary data will be gathered.[15] Then, poll tools will be made and main data will be gathered. The final goal of this method is to find important patterns in breaches of data privacy, evaluate the efficacy of current risk reduction efforts, and come up with doable suggestions for making healthcare systems safer for data.

Data Collection Techniques

Multiple methods will be used to collect data for this study to make sure that both depth and range of important information are captured. A close study of case studies and stories on data breaches in the healthcare sector will be the main way that data is gathered. Some of the sources for these case studies are public records, government probes, and scholarly papers. The study looks at well-known breaches, like the ones that happened with Anthem Inc. and the NHS, to find similar risk factors, weak spots in data security, and the effects of breaches on patient privacy. Along with the case study analysis, polls will be sent to healthcare workers (such as medical staff, managers, and computer experts) to get their first-hand reports of how data protection is currently handled.[16] People who fill out the poll will be asked to rate how common different types of security measures are, like encryption, multi-factor identification, and access control protocols, and to say how well they work at stopping data leaks. Experts in hacking and healthcare IT systems will also be interviewed in a semi-structured way. These talks will help us learn more about the technical and organisational problems that healthcare organisations have when they try to keep patient data safe. We will also get secondary data from government studies, business white papers, and regulatory groups to give us more background and a bigger picture of the laws that affect data privacy in healthcare.[17]

Risk Assessment Models for Data Privacy Violations

This research will determine the likelihood of healthcare data privacy being compromised using many risk assessment techniques widely used in cybersecurity and data protection. Among the primary tools to be used is the Risk Management Framework (RMF). Many healthcare institutions assess and lower information security threats using it. This approach entails identifying hazards, estimating their possible severity and frequency of occurrence, and then implementing the appropriate responses. Using digital health data, the RMF will be used for this research considering hazards from both within and outside the business like hacking, human error, and technological defects. Still another model available is Failure Mode and Effects Analysis (FMEA). It helps identify and investigate potential failure sites in medical data systems as well as determines how they can compromise patient privacy. This approach will concentrate on identifying the most critical locations such as software flaws, inadequate security, and insufficient access control where healthcare IT systems could fail. Additionally seen and assessed will be the causes behind violations of data privacy as well as the measures in place to minimise these risks using the Bowtie Model. Whether the risk event such as a data breach occurs or not, this model provides a picture of the link between the risk event (like a data breach), what causes it like inadequate security protocols and the actions done to avert it like encryption, staff training either way. Combining these risk assessment models will enable the research to provide a whole approach for evaluating the effectiveness of data privacy policies and identifying areas for improvement to prevent data breaches.

Criteria for Evaluating Patient Confidentiality

Patient privacy has to be assessed using a multifarious approach including the ethical, technological, and legal aspects of healthcare data handling. Judging how successfully patient privacy is preserved will mostly

depend on following the guidelines established by organisations such as the General Data Protection Regulation (GDPR) in the EU and the Health Insurance Portability and Accountability Act (HIPAA) in the United States.

1. Step 1: Identify Data Classification and Sensitivity Levels
    - Objective: Classify data based on sensitivity and criticality to patient confidentiality.
    - Action: Determine whether the data is public, internal, or confidential.

$$C = \{c1, c2, \ldots, cn\}$$

2. Step 2: Assess Data Access Control
    - Objective: Evaluate the effectiveness of access control mechanisms, ensuring only authorized users can access patient data.
    - Action: Use Role-Based Access Control (RBAC) or least-privilege model to evaluate access control.
    - Mathematical Equation:

$$A = \Sigma(ui * ri)$$

3. Step 3: Evaluate Data Encryption
    - Objective: Assess whether sensitive data is encrypted during transmission and storage.
    - Action: Verify if encryption algorithms are applied (e.g., AES-256).

$$E = \left(\frac{Data\ encrypted}{Total\ data}\right) * 100$$

4. Step 4: Analyze Audit Logs for Access Tracking
    - Objective: Ensure all access and modification of patient data is logged and reviewed.
    - Action: Review the frequency and accuracy of audit logs.

$$L = \Sigma(ai * ti)$$

5. Step 5: Assess Compliance with Legal and Regulatory Frameworks
    - Objective: Check if patient data handling adheres to regulations like HIPAA or GDPR.
    - Action: Compare data handling practices against compliance requirements.

$$P = \left(\frac{Compliance\ Criteria\ Met}{Total\ Compliance\ Criteria}\right) * 100$$

6. Step 6: Evaluate Incident Response and Breach Management
    - Objective: Assess the effectiveness of response mechanisms in case of data breaches.
    - Action: Evaluate the time to detect, report, and mitigate breaches.

$$R = \left(\frac{1}{Tb}\right) * \left(\frac{Breaches\ detected}{Total\ breaches}\right)$$

Risk analysis of data privacy violations

Identifying Threats to Digital Health Records

To keep patient information private and safe, it is very important to keep digital health data safe from different threats. Digital health records are mostly at risk from hacks from outside sources, threats from inside sources, and mistakes made by people. Safety of health data is highly compromised by cyberattacks from outside sources like hacking, ransomware, and frauds. Since the data kept in digital health records is confidential, cybercrime targets healthcare companies. Ransomware attacks, for instance, might prevent access to critical healthcare records and demand money to release it. These forms of strikes may also substantially disrupt healthcare services, therefore influencing general operation of healthcare facilities as well as patient treatment. A second major concern is insider hazards. This is the situation when partners or employees with access to confidential health records either intentionally or unintentionally abuse it. Employees who are not supposed to, for example, search medical records for personal benefit or leak private information—which might be used for evil intent. One more major cause of data leaks is human error. Usually, this results from negligent behaviour among medical professionals failing to follow correct security protocols. Simple errors like sending emails with patient information to the incorrect location or neglecting to log out of a system let those who shouldn't be seeing health data access them.

https://doi.org/10.56294/mw2024498

Vulnerabilities in Digital Health Systems

Because the technology is antiquated, there aren't adequate security controls, and data access isn't effectively controlled, digital health systems are often fractured. One major flaw is the antiquated or incompatible nature of the software tools healthcare institutions use. Many healthcare institutions still rely on antiquated systems that lack updates, which leaves them vulnerable to attacks using well-known weaknesses. Hackers will likely target these old systems because they may not have the most up-to-date encryption methods or security fixes. Healthcare organisations may also find it hard to make sure that all of their security methods are the same in different buildings or areas. Smaller clinics, bigger hospitals, and third-party service providers may have different security systems, which can leave holes that attackers can use. Managing who has access to data is another major weakness. Without strict entry rules, people who aren't supposed to be there could get to private patient information. Role-based access control (RBAC) is important to make sure that only people who are allowed to see, change, or share patient data can do so. Figure 2 shows places where digital health systems are weak, showing possible dangers like data breaches, unauthorized access, and not enough security protocols in healthcare technology.

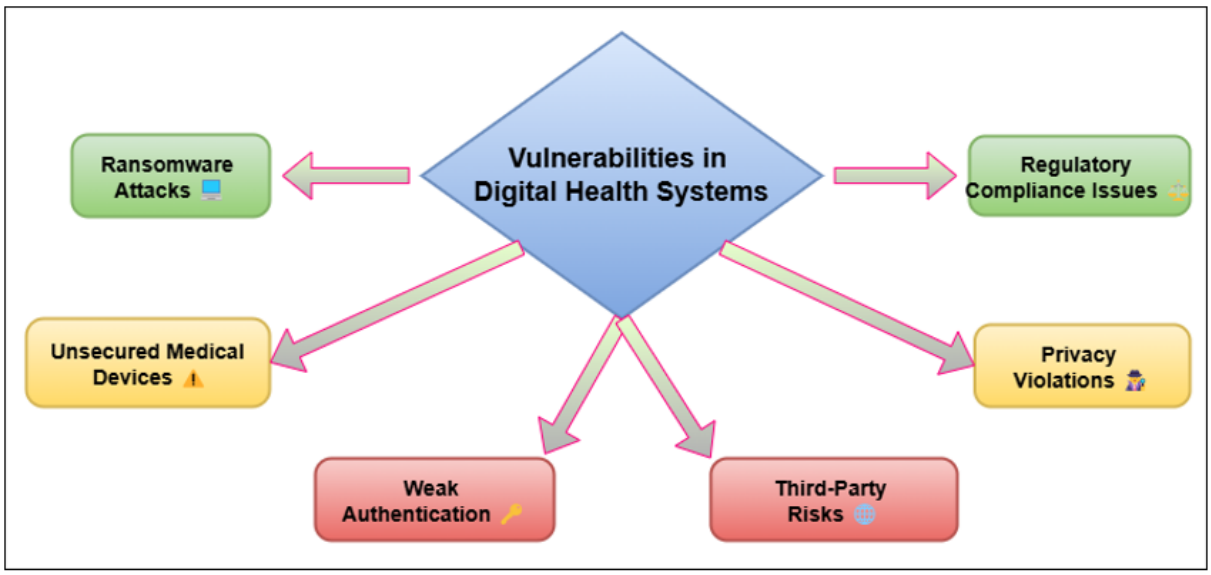

Figure 2. Illustrating vulnerabilities in digital health systems

Impact of Data Breaches on Patient Trust and Healthcare Providers

In addition to making patient data less secure, data breaches in healthcare damage people' faith in healthcare professionals and tarnish their names. It greatly influences the level of patient trust you inspire. If patients believe their confidential medical records may be hacked or shared, they could not trust healthcare facilities as much. The doctor-patient relationship depends on trust, hence when it is damaged; patients may not want to provide crucial medical information. People's communication suffers from this lack of transparency, which might reduce the efficacy of examination and therapy. Health management and treatment outcomes are more challenging in the worst of circumstances when patients may choose not to seek alternative physicians or get treatment at all. Data leaks in a mental sense may also impact patients, particularly if they discover that their personal medical records such as those containing genetic information, diseases, or treatment notes have been stolen or leaked. Those whose privacy has been violated might be judged, vulnerable, and concerned, particularly if the pilfers of information are utilised for evil purposes like discrimination or identity theft. For healthcare organisations, the consequences of a data breach may be just as detrimental. A breach can hurt the institution's image, which can cause patients to stop coming to the institution and lose faith in its ability to keep private data safe. Healthcare providers could be fined by regulators, sued, and have to pay a lot of money to fix the breach, which could include recovering data, telling patients who were affected, and paying for credit tracking services. Additionally, a breach can make regulatory bodies look at the healthcare provider more closely, which could lead to more frequent audits and stricter compliance rules.

Case studies and real-world examples

High-Profile Data Breaches in Healthcare

Publicised data breaches in the healthcare sector have exposed the shortcomings of digital health records and the extent of the consequences these sorts of occurrences may cause. Major US health insurance business Anthem Inc. was hacked in 2015, exposing personal data of 78,8 million individuals at danger. Among the

largest hacks ever was this one. Private information like Social Security numbers, medical IDs, birthdates, and employment details fell into hands of hackers. Although some of the information was encrypted, the hack revealed that security policies of large healthcare companies are not always robust. It also demonstrated how urgently data protection must be safeguarded by insurance companies and medical practitioners. 2017 saw a major hack at the National Health Service (NHS) in the United Kingdom. Problems resulted from the WannaCry ransomware outbreak. The malware afflicted about 200 000 computers worldwide, including NHS institutions. Many patients lacked the required care due to the assault because physicians had to reschedule appointments, postpone treatments, and return to paper records. This hack exposed the risks of using outdated programs as well as the reality that state healthcare institutions lack total security protocols in place. Among the largest healthcare firms in the United States, Universal Health Services (UHS) also suffered ransomware in 2020 and had to close its IT systems. At UHS, patient services were seriously lacking, and for a while the medical team had to rely on written notes. These tips compromised operations and cost money in addition to endangering patient data. The breaches highlight how crucial it is to be vigilant in safeguarding data privacy and safety as they reveal how more open healthcare systems are becoming to hacking.

Lessons Learned from Previous Violations

The well-known data leaks in the healthcare industry have given us a lot of knowledge on how to better guard patient information and simplify company handling of security concerns. One of the most crucial lessons acquired is the need of routinely updating and fixing software to prevent use of defects. The NHS hack demonstrated the risk involved in using outdate operating systems and software devoid of significant security modifications. Given many of healthcare facilities still rely on antiquated technology, cyberattacks are very likely to occur there. Regular software update and handling vulnerabilities before they become an issue help to reduce security concerns. Learning is the need of having thorough backup procedures for your data. Ransomware froze a lot of data in both the Anthem and UHS intrusions, hence the businesses either had to cope with a lot of downtime or pay big sums of money. Regular, efficient backups of data and storage in secure, off-site locations help to guarantee company survival in the case of a cyberattack. Also very crucial is teaching staff members how to identify potential security flaws. Part of the Anthem hack included phishing emails, which sought employees to provide confidential information. Although human error is a major issue in healthcare systems, frequent training and awareness campaigns may assist to prevent it. These stories also highlight the value of crisis response strategies. If discovered and controlled fast, data leaks may cause less harm. Institutions should establish open channels of discovery for violations, notify patients of them, and forward the matter to the appropriate regulatory authorities. Finally, the disclosures have proven the need of maintaining third-party interactions safe. Like Anthem, many hacks originate from third-party vendors or partners with access to sensitive data. Healthcare firms must ensure that their outside partners do thorough risk analyses on them and adhere to their identical data security policies.

Effective Mitigation Measures Implemented

Data breaches have led healthcare institutions to implement some sensible measures to increase data security and prevent next crimes. One of the most often used techniques is implementing multi-factor authentication (MFA) all across hospital systems. MFA asks users to verify who they are using more than one means, such as a password, biometric data, or a one-time security code, thus far less likely someone would enter without permission. Particularly in cases of worker login data theft, multiple factor authentications (MFA) has proved very beneficial in preventing confidential patient data from finding incorrect hands. Healthcare professionals have also resorted to encryption as a fundamental safety precaution to protect sensitive patient data. Many locations nowadays ensure that, both while they are not in use and during transmission, all medical records are safeguarded using robust cryptographic techniques. Although they can access a system, cybercriminals will find it difficult to get or use patient data with this security. Blockchain technology has also begun to be used by healthcare companies to enhance data accuracy and security. Blockchain generates a decentralised, immutable log that may be securely used to store health information and monitor any data modification activity. This guarantees open and responsibility for access. For instance, many healthcare companies restrict who may see patient data depending on their employment within the company using role-based access control (RBAC). Making ensuring only approved staff members have access to confidential data helps healthcare facilities reduce internal breach risk.

RESULTS AND DISCUSSION

A look at well-known data breaches like those at Anthem, NHS, and UHS shows that healthcare organisations are still at risk, even though they follow rules like HIPAA and GDPR. Technology options like encryption, bitcoin, and multi-factor identification were found to lower risks by a large amount. But problems still exist because of old systems, poor training for employees, and uneven adherence to security rules.

https://doi.org/10.56294/mw2024498

Table 2. Risk Analysis of Data Privacy Violations			
Evaluation Parameter	**Low Risk (%)**	**Medium Risk (%)**	**High Risk (%)**
Risk of Cyberattacks	10	30	60
Risk of Insider Threats	5	35	60
Human Error	20	40	40
Regulatory Compliance	15	50	35
Technology Integration	30	40	30

Table 2 shows the different levels of risk that come with breaches of data protection in digital health records. The risk is broken down into low, medium, and high amounts based on a number of review criteria. Figure 3 displays the average risk level over all evaluation criteria, revealing changes and possible weak spots.

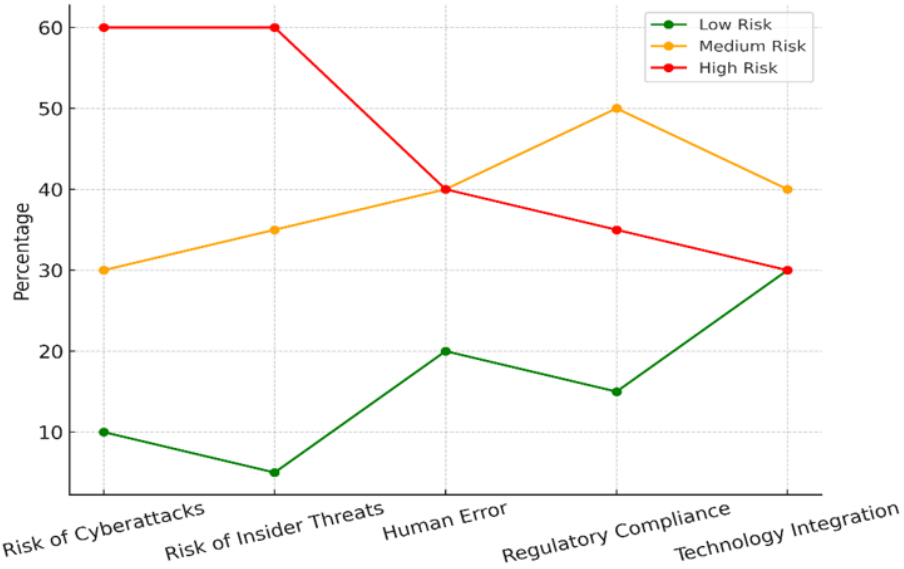

Figure 3. Trend of Risk Levels Across Evaluation Parameters

The rate of high risk in Cyberattacks is 60 %, while the percentages of low risk (10 %) and middle risk (30 %) are not very different. This means that healthcare organisations are probably very vulnerable to cyber dangers. Figure 4 shows what happens when the risk level is high across all groups. It shows how weak digital health systems are and what could go wrong.

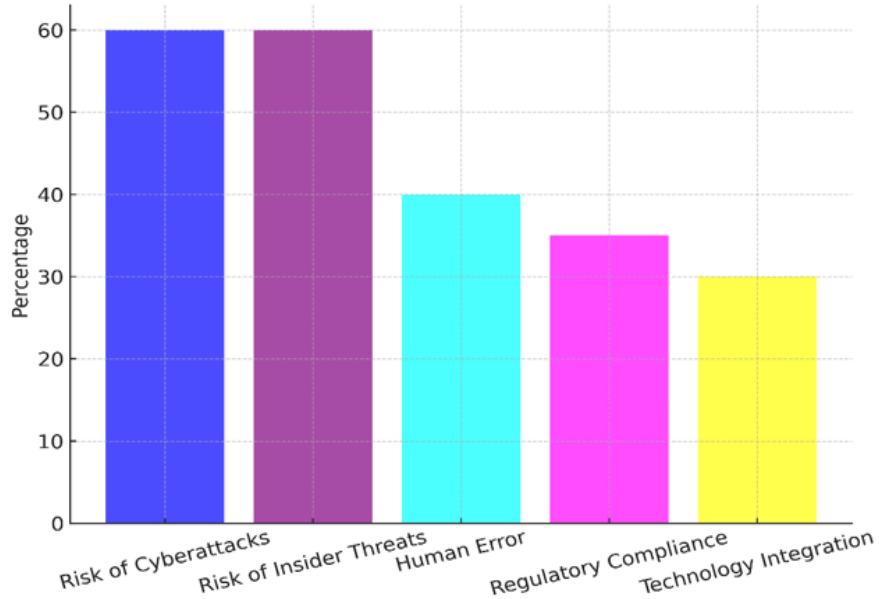

Figure 4. Impact of High Risk Across Categories

https://doi.org/10.56294/mw2024498

This is probably because hackers want to steal health data, which is very valuable. In the same way, the Risk of Insider Threats shows a high risk (60 %), a low risk (5 %), and a medium risk (35 %). This means that internal players, whether they are evil or careless, pose a big threat to the privacy of patient data. Human error makes up 40 % of the medium risk, and the low risk group (20 %) stands out. This means that human error is still a part, but it's not as common as the other risks. Regulatory Compliance is mostly seen as medium risk (50 %), which means that while rules are mostly followed, there are still some areas where they aren't fully followed. Lastly, Technology Integration has a more even risk distribution, with 30 % in each of the low, medium, and high risk groups. This shows how difficult and complicated it is to safely add new technologies to healthcare systems that are already in place.

Table 3. Mitigation Measures Effectiveness

Evaluation Parameter	Very Effective (%)	Effective (%)	Ineffective (%)
Encryption Effectiveness	50	40	10
Blockchain Adoption	60	30	10
Multi-Factor Authentication	70	25	5
Data Access Control	40	50	10
Security Audits	55	35	10

The information in table 3 shows how well different security methods protect patient data privacy in healthcare. Encryption Effectiveness is thought to be very effective by 50 % of those who answered, effective by 40 %, and useless by only 10 %. Figure 5 shows how the efficiency of security measures varies across digital health systems, showing how well they work to lower risks.

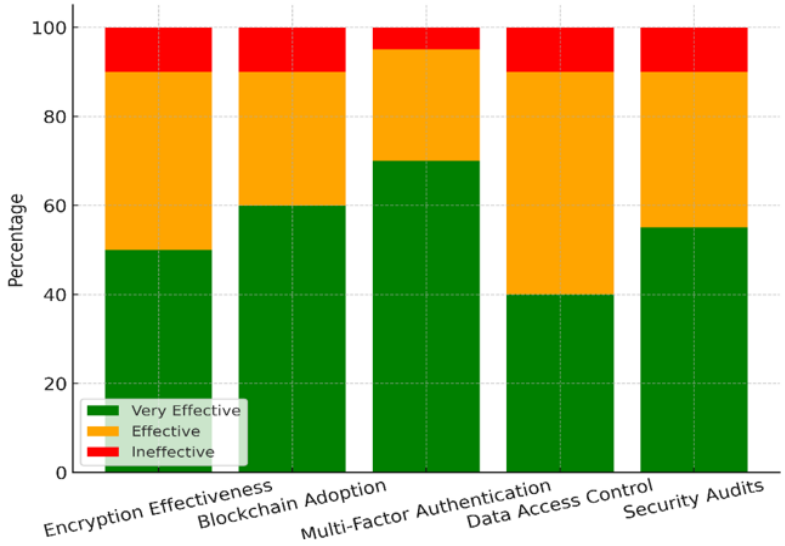

Figure 5. Distribution of Security Measure Effectiveness

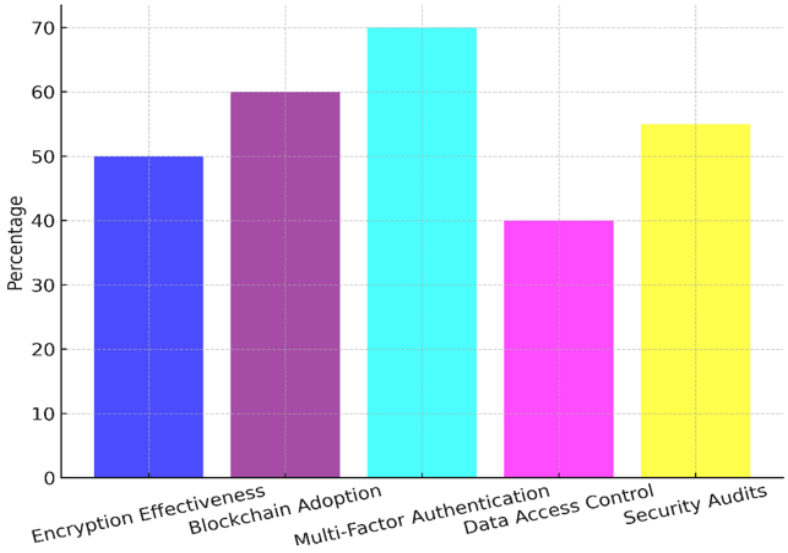

Figure 6. Impact of Very Effective Security Measures

https://doi.org/10.56294/mw2024498

This shows that encryption is an important and well-known way to keep private patient information safe, especially when it's being sent and stored, though its use could be better in some areas. Sixty percent of those who answered the survey said that blockchain adoption was very effective, which shows that it is becoming more important for keeping data safe and secure. But 30 % think it works and 10 % think it doesn't, which suggests problems with how it fits into and grows with current healthcare systems. Figure 6 shows what happens when you use very strong security methods to make digital health systems safer by lowering weaknesses.

Multi-Factor Authentication is thought to be the best measure; 70 % of respondents said it was very successful, and only 5 % said it wasn't. This strong recommendation shows that it can keep people from getting in without permission by giving an extra layer of security on top of passwords.

CONCLUSIONS

As more and more health records are digitised, protecting patient privacy offers both possibilities and difficulties. Healthcare organisations still face a big risk when their data protection is violated, which has effects on both patients and workers. According to a comprehensive risk study, human errors, insider breaches, and hacking are quite frequent hazards. This emphasises the need of having solid cybersecurity systems. Though they provide guidelines for data protection, legislative systems such HIPAA and GDPR are not always implemented. Healthcare companies have to act more aggressively if they are to keep ahead of new dangers. New technologies that might help to safeguard patient data include encryption, Bitcoin, and multi-factor authentication. Data encrypted is secure both in storage and during transit. Patient data is therefore protected even in cases of access without authorisation. Blockchain's irreversible, distributed record guarantees patient data can be securely monitored and seen and helps to make things more transparent and responsible. Multi-factor authentication greatly increases access control; hence unauthorised people cannot enter systems using stolen passwords. Technology by itself, meanwhile, cannot guarantee patient data security. According to the studies, companies should have explicit policies and equip their employees to lower risks by means of training. Strong data access policies must be established by healthcare institutions to guarantee that only approved personnel may see confidential patient records. Regular security audits, penetration testing, and incident response strategies help one to identify flaws and manage breaches. Healthcare professionals must constantly learning about the best methods to keep data private in order to reduce the danger of human error which is still a major factor driving data breaches.

BIBLIOGRAPHIC REFERENCES

1. Kiania, K.; Jameeii, S.M.; Rahmani, A.M. Blockchain-based privacy and security preserving in electronic health: A systematic review. Multimed. Tools Appl. 2023, 82, 28493–28519.

2. Nowrozy, R.; Ahmed, K.; Wang, H.; Mcintosh, T. Towards a universal privacy model for electronic health record system: An ontology and machine learning approach. Informatics 2023, 10, 60.

3. Basil, N.N.; Ambe, S.; Ekhator, C.; Fonkem, E. Health records database and inherent security concerns: A review of the literature. Cureus 2022, 14, e30168.

4. Bani Issa, W.; Al Akour, I.; Ibrahim, A.; Almarzouqi, A.; Abbas, S.; Hisham, F.; Griffiths, J. Privacy, confidentiality, security and patient safety concerns about electronic health records. Int. Nurs. Rev. 2020, 67, 218–230.

5. Abunadi, I.; Kumar, R.L. BSF-EHR: Blockchain security framework for electric health records of patients. Sensors 2021, 21, 2865.

6. Adamu, J.; Hamzah, R.; Rosli, M.M. Security issues and framework of electronic medical record: A review. Bull. Electr. Eng. Inform. 2020, 9, 565–572.

7. Aladwani, S.O.; Almotairi, M.A. Security & privacy of electronic health records. J. Med. Sci. Clin. Res. 2023, 11, 88–93.

8. Pooja Das, Smrutihara Biswal. (2015). "Sustainable HR": A Need For A Sustainable Enterprise. International Journal on Research and Development - A Management Review, 4(1), 114 - 124.

9. Gariépy-Saper, K.; Decarie, N. Privacy of electronic health records: A review of the literature. J. Can. Health Libr. Assoc. 2021, 42, 74–84.

https://doi.org/10.56294/mw2024498

10. Chen, H.; Wu, Z.; Chen, T.; Huang, Y.; Liu, C. Security privacy and policy for cryptographic based electronic medical information system. Sensors 2021, 21, 713.

11. Li, Q.; Yu, H.; Li, W. Information sharing and privacy protection of electronic nursing record management system. Sci. Program. 2022, 2022, 4169340.

12. Nair, J.; Alshaikh, M.; Culnane, C. A comparative study of security and privacy in electronic health records. J. e-Health Manag. 2020, 2020, 557564.

13. Sharma, D.; Prabha, C. Security and privacy aspect of electronic health records: A review. In Proceedings of the 2023 International Conference on Advancement in Computation & Computer Technologies (InCACCT), Gharuan, India, 5–6 May 2023.

14. Abdulhameed, I.S.; Al-Mejibli, I.; Neif, J.R. The security and privacy of electronic health records in healthcare systems: A systematic review. Turk. J. Comput. Math. Educ. 2021, 12, 1979–1992.

15. Tsai, C.H.; Eghdam, A.; Davoody, N.; Wright, G.; Flowerday, S.; Koch, S. Effects of electronic health record implementation and barriers to adoption and use: A scoping review and qualitative analysis of the content. Life 2020, 10, 327.

16. Tertulino, R.; Antunes, N.; Morais, H. Privacy in electronic health records: A systematic mapping study. J. Public Health 2023, 32, 435–454.

17. Keshta, I.; Odeh, A. Security and privacy of electronic health records: Concerns and challenges. Egypt. Inform. J. 2021, 22, 177–183.

FINANCING

No financing.

CONFLICT OF INTEREST

The authors declare that there is no conflict of interest.

AUTHORSHIP CONTRIBUTION

Data curation: Sujayaraj Samuel Jayakumar, Kunal Meher, Udaybhanu Rout, Gujjala Srinath, Shivam Khurana, Sukhman Ghumman, Shilpi Singh.

Methodology: Sujayaraj Samuel Jayakumar, Kunal Meher, Udaybhanu Rout, Gujjala Srinath, Shivam Khurana, Sukhman Ghumman, Shilpi Singh.

Software: Sujayaraj Samuel Jayakumar, Kunal Meher, Udaybhanu Rout, Gujjala Srinath, Shivam Khurana, Sukhman Ghumman, Shilpi Singh.

Drafting - original draft: Sujayaraj Samuel Jayakumar, Kunal Meher, Udaybhanu Rout, Gujjala Srinath, Shivam Khurana, Sukhman Ghumman, Shilpi Singh.

Writing - proofreading and editing: Sujayaraj Samuel Jayakumar, Kunal Meher, Udaybhanu Rout, Gujjala Srinath, Shivam Khurana, Sukhman Ghumman, Shilpi Singh.