HEALTH DATA BREACHES AND RANSOMWARE IMPACTS

University of Pittsburgh- School of Health and Rehabilitation Sciences

## **2251 HI 2450 SEC1000 SECURITY, PRIVACY, LGL & ETHCL**

BY:

Sree Gayatri Anusha Mylavarapu

Guided By : **Yong Choi, PhD, MPH**

**Executive Summary -**

This is a summary of my project, and this project is mainly focused on the data breaches and ransomware attacks, and my major focus for this project focuses on Electronic Health Records (EHR) systems. With technology growth in the healthcare industry, these organizations have become a significant target for cyberattacks because of the valuable and sensitive nature of the data held. The project aims to explore the technologies and strategies used to protect against ransomware attacks and data breaches in healthcare settings.

This project mainly focuses on the critical issues of healthcare data breaches and ransomware attacks particularly focusing on the impact of Electronic Health Records and these store sensitive information of patients and support critical healthcare operations. My analysis highlights the key vulnerabilities of EHR systems and risks. I have discussed some case studies like Universal Health Services ransomware attack 2020, and Accellion data breach 2021, which showed severe operational, financial, and patient safety consequences of these attacks. An interdisciplinary approach is emphasized within this paper, whereby the technical development such as advanced encryption and audit trails are combined with the organizational approach of training for staff and incident response.

Many new technologies promise to better secure health care data, with blockchain and AI being in the fore, while simultaneously improving threat detection. These recommendations will aim at privacy and security concerns to ensure compliance with the relevant regulatory frameworks, including those issues that impact the continuity of care. Such in-depth analysis of these critical issues thus outlines the roadmap for the creation of robust cybersecurity defenses among healthcare organizations against emerging threats.

Key Findings -

Lack of Encryption - Most of the EHR systems lack proper encryption of data. As such, during transfers, data is highly vulnerable.

Poor Password Policies - Poor passwords and poor password management policy allow unauthorized access to information and data breaches.

Integration of insecure third-party applications and telehealth platforms -The integration of insecure third-party systems contributes to new vectors of vulnerability introduced into your infrastructure.

Insufficient User Training - Poor user training will amount to poor handling of data, as well as to the highest probability of susceptibilities regarding phishing attacks.

Impact of Ransomware Attacks: Attack via Ransomware in the EHR systems leads to grave after-effects.

Disruption of Healthcare Services - Ransomware attacks disrupt healthcare services and affect patient care, causing delays. For instance, the 2020 Universal Health Services ransomware attack caused huge disruptions to healthcare services. Financial Losses: These kinds of attacks result in huge financial losses. The 2021 Accellion data breach underlined how serious the financial consequences are, such as reduced hospital volume, increased in-hospital mortality, and substantial financial losses.

Cybersecurity Threats Some of the recent studies estimated that ransomware attacks resulted in a hospital volume reduction of 17 to 25%, increases in in-hospital mortality, and huge financial losses. The average cost per incident of a data breach in healthcare is around $9.23 million.

Privacy and Security Aspects in EHR

EHR systems have a number of features that enable and support healthcare delivery in the following ways.

Comprehensive Digital Medical Records - The EHR systems retain comprehensive digital medical records about the patient's history that includes demographic resources, medical history, diagnoses, treatment plans, medications, laboratory test results, vaccination details, allergies, and radiology studies.

Real-time access - The system provides real-time access to the user for patient records, securely, in order to make timely and informed clinical decisions. Clinical documentation: EHR enhances the quality of clinical documentation by offering features that include progress notes, customizable templates, or voice and handwriting recognition options that allow for correct data entry.

e-Prescribing and Order Management- It enables providers to prescribe electronically to pharmacies, checks interactions, and maintains the entire record of medications. Providers also place orders and track their results for tests, procedures, and referrals from associated risks with data breach incidents to ransomware attacks, the following are some recommendations to mitigate the possibility of such risks.

Encryption Standards -Advanced encryption standards and Transport Layer Security (TLS) are to be implemented for data at rest and in transit. This ensures that even when data is intercepted, access to it cannot be gained without the decryption key.

Role-Based Access Controls - Role-based access controls with multi-factor authentication should be implemented. In this way, only the authorized personnel will be able to gain access to the patient records, reducing the chances of unauthorized access.

Security Audits - Periodic security audits, including vulnerability testing, help identify and fix potential vulnerabilities. This is a proactive way of trying to mitigate the risk before it becomes an opening that a cybercriminal could exploit. Staff Training: Engage in regular training programs regarding cybersecurity awareness and best practices. The nature of healthcare requires such training in order to keep cybersecurity cultures in all healthcare organizations.

Incident Response Planning - Incident response planning involves establishing and keeping incident response plans updated regularly that will ensure immediate action the moment a security breach takes place. Such plans make sure that during and after the cyber incident, continuity of care and data integrity is taken into consideration.

Emerging Technologies - Equally, there is an encouraging study of how, among the emerging technologies, blockchain and AI could improve the cybersecurity landscape for healthcare. The technology of blockchain can allow management of health records transparently and securely, while AI may enable more effective real-time detection and response towards cyber threats.

Evaluation of the Privacy and Security Checklist

User Authentication and Access Control - EHR systems are usually installed with strong mechanisms for user authentication, like two-factor or three-factor authentications, and role-based access controls. However, the precision of the latter accesses tends to vary from system to system

Data Encryption - Modern EHR systems use data encryption both at rest and in transit, which is important in terms of compliance with HIPAA and securing sensitive patient data.

Audit Trails - EHR systems continuously log all activities of users concerning patient record access, changes, and other manipulations within their audit logs. This is crucial for security oversight and regulatory compliance.

Secure Backup and Disaster Recovery -While backup and disaster recovery options are part of most EHR systems, the strength of such backup strategies may vary. For instance, the loss of data resulting from the ransomware attack in Desert Wells Family Medicine shows the requirement of sound backup solutions

HIPAA Compliance and EHR Systems

Consequently, HIPAA has provided several national standards for protecting identifiable patient information. Some of the main requirements for EHR systems include:

Mediated Access to Information: The EHR systems should provide mechanisms enabling healthcare providers to access just that amount of information about the patients that is essentially required to do their work by facilitating role-based access control supported with multi-factor authentication.

Encryption - patient information security through the process of data encryption at transit and rest. Different data security techniques, including encryption, ensure that although an unauthorized entity acquires the data, he will not be able to comprehend any information.

Audit Trails: Records of user access have to be maintained in the system, wherein every access, every attempt to modify, or attempt to interact with the record can be logged. The record will help prevent unauthorized access or change.

Incident Response and Contingency Planning: There should be formal incident response and contingency plans in case of security breaches like data compromise or ransomware infections. The interventions to be covered include storage backup, testing, and recovery, and the procedures for system continuity.

Future Trends and Considerations - Regulatory mechanisms need to be upgraded in order to answer current cybersecurity threats. Further research is needed to test the adequacy of existing regulations, such as HIPAA, and to provide evidence-based policy updates. It also requires regulatory evolution to meet new technologies and threat landscapes.

Intersection of Cybersecurity and Public Health - The paper needs to establish the interaction of cybersecurity and public health preparedness in terms of the protection of health data in case of emergencies and widespread outbreaks. As the COVID-19 pandemic has shown, one of the most important components of the response of public health is represented by health information systems that need to be assured about security. Further research is needed to show how cybersecurity measures can be embedded within the response plans for emergencies within public health.

Ethical Dimensions – Thus, ethical discussions on patient privacy, ownership of data, and the trade-off between security and accessibility are warranted. These ethical issues need to be debated in future research, and guidelines on responsible cybersecurity practices in healthcare should be outlined. Ethical frameworks must consider the balance between robust security measures and the need for patient access and privacy.

The project has emphasized the importance of strong cybersecurity in healthcare to protect sensitive patient information and maintain EHR system integrity. Advanced encryption, periodic audits, staff training, and incident response plans are some of the ways in which healthcare organizations can reduce risks from data breaches and ransomware attacks. The recommendations given stand a chance to shape future decisions in healthcare technology so that care can be continuum and patient data secure against the ever-rising tide of cyber threats.

For health organizations, it is high time that holistic approaches are resorted to with regard to technical solutions, organizational policies, and education of employees in matters related to cybersecurity. Auditing and updating of security protocols are necessary in order to maintain resiliency in the landscape of cybersecurity threats to health care. These emerging technologies would assist in leveraging these, thereby adhering to a wide range of regulatory frameworks such as HIPAA to ensure data protection of patients and integrity within EHR systems.

**Project Reflection -**

This project has discussed in detail the critical issue of health data breaches and ransomware attacks, including those related to EHR systems such as those provided by Epic Systems.

Vulnerabilities in EHR Systems: Most EHR systems use weak encryption therefore data becomes susceptible during transit.

Poor Password Policies: Poor passwords and poor password management could result in unauthorized access and data breaches.

Integration of systems with insecure third-party applications and telehealth platforms: These also introduce other vulnerabilities, provided the third-party systems are not secure.

Poor User Training: Poor user training will lead to poor handling of data and increased vulnerability to phishing attacks.

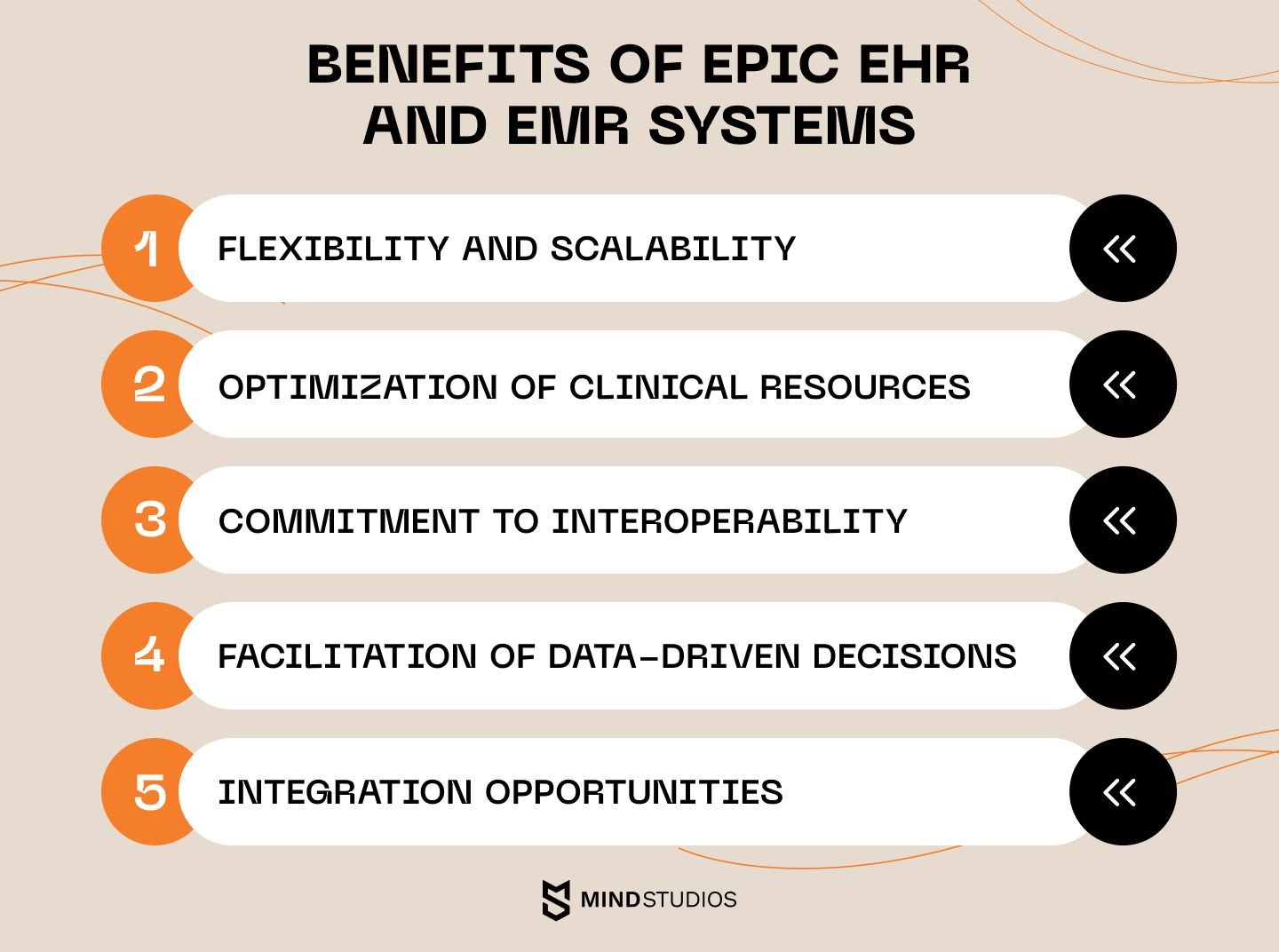
To mitigate risks for data breaches and ransomware attacks, a number of recommendations are made.

• The key deliverable is to understand a design to develop a customized security and privacy checklist and integrate all the required measures to be taken for keeping healthcare data secure and avoiding ransomware.

• Then, this checklist will be provided to real-world implementation to EHR systems and test its resiliency against cybersecurity threats.

A checklist or criteria containing all the detailed information needed can be prepared that would act as a primary tool to conduct a review of the selected technology for its measures in ensuring the privacy and security of healthcare information. The checklist would assure the components missed by earlier research and identify the industrial standards that can help safeguard data protection in health care.

I will start compiling all the critical elements of privacy and security, considering regulatory frameworks like HIPAA and best practices in healthcare cybersecurity. I want the checklist to address various security domains, such as data encryption, access management, and user authentication.



ADVANCED ENCRYPTION AND ACCESS CONTROLS

|  |  |  |
| --- | --- | --- |
| **Criteria** | **Adherence** | **Notes** |
| Data backups (Regular) | YES | Weekly checks are done, and backups are performed. |
| Backup Storage (offline) | YES | Critical data is backed up separate from the main network and is stored offline on storage devices. |
| Network Segmentation | Partially YES | Critical systems are isolated, but some legacy systems remain on the main network. |
| Multi-Factor Authentication | YES | It is required for all accounts and users |
| Email Filtering | YES | Advanced email gateway solution implemented, scanning all incoming emails for malicious content. |
| Endpoint Protection | YES | Next-gen antivirus and EDR solutions deployed on all endpoints. |
| Patch Management | Partially YES | Critical systems are patched promptly, but some non-critical systems experience delays. |
| User Training | YES | Monthly security awareness training conducted, including simulated phishing exercises. |
| Incident Response Plan | YES | Detailed ransomware-specific incident response plan in place, with regular tabletop exercises. |
| Third-Party Risk Management | Needs Improvement | While assessments are conducted, monitoring of third-party access is limited. |
| Compliance with Regulations | YES | Regular audits ensure compliance with relevant data protection regulations. |

**Reasons for Concern and Possible Influences of Recommendations on Innovations in Medical Technology**

Sensitive Data Protection

* Advanced encryption standards and multi-factor authentication provide broadened layers of security to patient information against cyberattacks and data breaches.
* Incident response plans updated periodically guarantee timely action at the time of breaches for maintaining continuity in care and data integrity, which becomes specially crucial in ransomware attacks.
* Training programs for staff and regular security audits reduce financial losses by preventing breaches; the estimated average cost per incident is $9.23 million in healthcare.

Regulatory Compliance

* Conformity to HIPAA, FIPS 140-2, and HITECH reduces the risks of litigation and financial penalties.
* Grudging audits and resolute standards of compliance support organization accountability and resilience.
* Recommendations have the potential to push changes in regulatory frameworks towards becoming more adaptive and stringent in tackling current cybersecurity threats, coupled with emerging technologies.

Ethical Issues

* The privacy of the patients and ownership of the data thus generated will be adequately addressed for ethical treatment of such sensitive information.
* Emphasis on balance between security measures and accessibility to patients will be laid for future ethical and policy frameworks.
* These considerations ensure that research and decision-making are directed toward technological innovations that do not compromise either security or patients rights.

Broader Implications

* This can encourage a more proactive approach to cybersecurity in healthcare, extending to influence future decision-making and the adoption of technology.
* This would lay a path for integrating ethical, secure, and cost-effective practices toward meeting the evolving challenges of innovation in the healthcare industry.
* The recommendations provided in this project are crucial for several reasons, and they have the potential to significantly influence future decisions in healthcare technology.

Data Protection

* Advanced encryption standards along with role-based access controls, including multi-factor authentication, can go a long way in protecting sensitive patient data from unauthorized accesses and breaches. This assumes greater significance considering the value of healthcare data and the increasing frequency of cyberattacks.
* Incident response plans established and regularly updated will provide an immediate course of action after a security breach, ensuring care continuity and data integrity. This will be important because ransomware attacks can disrupt healthcare services, impacting patient care and causing delays.
* Regular security audits and vulnerability assessment, coupled with regular training programs for healthcare staff, can reduce financial losses due to data breaches and ransomware attacks.
* These recommendations have the potential to shape future regulatory updates, focusing on the development of more robust and adaptive cybersecurity regulations capable of responding to modern cybersecurity threats while keeping pace with emerging technologies and new threat landscapes.
* The recommendations stress that ethical issues relating to patient privacy, ownership of data, and the balance between security and accessibility need to be addressed. These will help in guiding further research and policy-making as ethical frameworks balance the need for robust security measures with the need for patient access and privacy.

**Integration of Milestone 1, 2 and 3**

The main component I discussed in this review is ransomware attack on EHRs - Electronic Health Record Systems.

● EHRs are usually digital versions of patients' paper charts and have all the patients information like case history, medical history, diagnosis , imaging records, scans , treatment plans, lab results , immunization records etc.

● EHRs are generally used to provide real time access to patients about their records and improve the quality of care. These EHRs can be modified anytime by the healthcare providers to update the health status of the patient and streamline the workflow.

● EHRs enable better clinical decision making and reduce human errors.

● Interoperability is present in EHR and Patient engagement is more allowing access to information like scheduling appointments and communicating with healthcare providers.

Vulnerability of EHR systems

● Many EHR systems have a lack of encryption system making the data vulnerable during transfers

● Poor password policies can also affect data breach and unauthorized access.These health records often engage with third party applications and telehealth platforms which can cause additional vulnerabilities if they are not secure.

● The users need to have adequate training to use the application or it might lead to poor data handling and phishing attacks.

Ransomware attacks -

Cybercriminals target EHRs and encrypt the patient data and ransom money or certain form of payments to restore patient access and these attacks may cause dispute in healthcare services and cause delay in patient care.

● Data breaches in cybercrime occur through hacking, threats, stolen devices and it compromises sensitive patient information.The cybercriminals target the attackers through phishing scams and emails and provide credentials or download malicious software. Examples of EHR- related data breaches

● This is a data breach case that happened in 2020 with universal health services which is a large healthcare provider and had a ransomware attack that disrupted the EHR systems and impacted patient care and caused a substantial financial loss.

● This is another example of an accellion data breach that happened in 2021 an incident that happened was its file sharing service led to data breaches affecting several healthcare organizations exposing sensitive information stored in EHR systems

Some Key Components of healthcare cybersecurity -

● Advanced encryption standard and Transport Layer Security are some encryption technologies. Biometric authentication systems .VLANs and log analysis

● Security awareness programs Literature Review This review of mine talks about some recent healthcare data breaches and ransomware attacks in the healthcare sector.

● There are many ransomware attacks happening on hospitals and a study conducted in 2024 reveals that finding these attacks have decreased the volume of the hospital by 17-25% and these attacks reduced the revenue of the hospital but also increased the in hospital mortality admitted at the time of attack and this study highlights the importance of safety impacts.

There has been a massive ransomware attack in feb 2024 on change healthcare shows the losses and costs of incidents and UnitedHealth group has reported $2 - 2.45 billion dollar loss and this has affected millions of patients and disrupted operations across the healthcare sector.

● The american hospital association has shown more that 380 cyber attacks in this year alone indicating that the threat remains same compared to previous years and much more emphasizing is needed.

● LogRhythm shows that ransomware puts patient data and its confidentiality at risk. This breach could also expose data to unauthorized parties, and as shown in this article, the average cost per incident of a data breach is $9.23 million, thus affecting financial incentives of the organization.

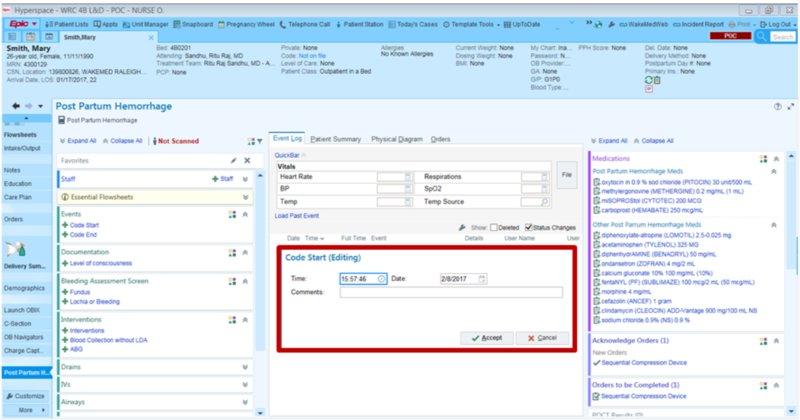
● Kruse et al. (2023) conducted a systematic review of 110 articles related to cybersecurity in healthcare, after which they established the evolving threat landscape of modern times. The top three threats identified are: phishing, insider threats, and IoT vulnerabilities. Researchers squarely stress that it involves many-level security: technical solutions, organizational policies, and education among employees.

● Drawing on the work of McGlave et al. (2024), Chen and Li explore indirect impacts on quality of care for patients following ransomware attacks. The investigators found that in the months after an attack, medication errors increased 12% in targeted hospitals, while hospital-acquired infections rose 9%. This present study highlights the impact of cybersecurity breaches on patient safety and healthcare outcomes.

● An exhaustive economic study conducted by the Ponstan Institute pegs the average cost of a healthcare data breach at $10.1 million in 2024, which is 9.4% higher than the previous year. "This is because attacks are getting increasingly sophisticated and the attack surface is expanding due to the adoption of digital health technologies," the study said. Indeed, organizations that have mature security practices and incident response plans in place tend to realize considerably lower costs per breach.

● In the paper, "The Primacy of Cyber - Issues and Challenges of Creating a Robust Cyber Security Environment for Healthcare," Rahman et al. (2023) address the unique challenges which the healthcare institutions face in implementing robust cyber security. The investigator considers how to balance stringent security protocols against the needfor clinical staff in emergencies to access patient information immediately. They suggest that one of the most imperative components of successful cybersecurity strategy within healthcare is training and awareness programs for clinicians and staff

. ● While regulatory frameworks, such as HIPAA, are essential to comply with numerous studies suggest meeting compliance is not enough to provide complete cyber security protection. There is increasing literature asserting that healthcare institutions need to move from basic compliance to establish more sophisticated and proactive security measures. ● Several works exist that explore some emerging technologies, such as blockchain and AI, that can bolster cybersecurity in healthcare. Yet these technologies can introduce new issues of privacy and security that need to be carefully considered.



**Privacy and security aspects in EHR:**

EHR systems possess functionalities that enhance and facilitate healthcare delivery at large. At the center of the EHR system is its capability in keeping comprehensive digital medical records of a patient's history. This covers demographic resources, medical history, diagnoses, treatment plans, medications, laboratory test results, vaccination details, allergies, and radiology studies. By integrating these information bits, EHRs create a complete picture of a patient's health status, which many providers and settings can share to have more coordinated care. Additionally, EHRs enable authorized users to access patient records in real-time, securely, which is very essential to make timely and informed clinical decisions.

* EHRs also enhance the quality of clinical documentation, allowing the clinician to digitally document patient interactions through capabilities such as progress notes, customizable templates, or voice or handwriting recognition options that support accurate data entry. These functionalities allow the clinician to create clinical documents, including care plans and protocols. E-prescribing is another key capability: providers can transmit prescriptions directly to pharmacies, check for drug interactions, and keep a complete medication history. It also supports order management: providers could order and track tests, procedures, and referrals. In terms of results management, one has easy access and can manage lab results, radiology reports, and other diagnostic tests in a very organized manner in the interest of effective communication of patient data.

**Prevalence and Impact -**

The great value of medical data has made the health sector a potential target for cybercriminals. Indeed, according to HHS, there were a record number of 725 breaches of healthcare data reported in 2023, affecting over 133 million records of patients. This increase underlines the ever-evolving threat surface. Some striking statistics, in the face of a 239% growth in hacking-related data breaches and a 278% growth in ransomware attacks from 2018 to 2023, show that in 2019, hacking represented 49% of all reported breaches-a mark truly showing how vulnerable this sector is getting.

Common Attack Vectors: Threats against cybersecurity in healthcare predominantly include phishing and ransomware attacks. Cyberattacks need only send very sophisticated phishing emails that trick employees into divulging their login credentials or need to install malware. Once attackers break through, they can execute ransomware programs that may encrypt critical EHR data and hold it for ransom. It has also been determined through research that phishing and ransomware together contribute to 40.7% of all non-malicious breaches in health care and, when severe, can have devastating effects, as it was with the case of the Desert Wells Family Medicine in Arizona, whose EHR system was lost permanently when both primary and backup data were encrypted in a ransomware attack.

Prevention and Mitigation Strategies: The following are the ways a multilayered cybersecurity approach should be engaged to protect EHR systems from ransomware and data breaches:

• Employees should be enlightened regarding how phishing emails come to them and how they can maintain good security practices.

• EHR data should be safely stored in offline backups that could assure restoration in case of ransomware attack.

• Inquiring whether vendors of third-party service providers are adhering to the highest measures of security.

• Develop and rehearse the incident response plan regularly to rapidly handle cybersecurity incidents of varied types.

User Authentication and Access Control - Mostly Adheres

Evidence - EHR systems commonly employ robust user authentication measures, including multi-factor authentication, role-based access controls, and user-specific customization for roles and permissions. However, the precision of these access controls can vary among systems.

Data Encryption - Fully Adheres

Evidence - Modern EHR systems incorporate data encryption for both data at rest and in transit, which is essential for HIPAA compliance and safeguarding sensitive patient information.

Audit Trails - Fully Adheres

Evidence - EHR systems consistently maintain comprehensive audit logs of user activities, including patient record access, modifications, and other interactions. This is critical for security oversight and regulatory compliance.

Secure Backup and Disaster Recovery - Mostly Adheres

Evidence - While most EHR systems include backup and disaster recovery features, the robustness of these strategies can vary. For instance, Desert Wells Family Medicine’s loss of data in a ransomware attack underscores the need for reliable backup solutions.

Interoperability and Data Sharing - Partially Adheres

Evidence - Many EHRs offer data-sharing capabilities with labs and pharmacies and support connections with national health information exchanges. However, interoperability remains challenging across different EHR platforms, with inconsistent implementation levels.

Patient Portal Security - Mostly Adheres

Evidence - EHR systems generally provide secure patient portals that include secure login options, encrypted communication, and the capability for patients to securely upload data.

Mobile Access Security - Partially Adheres

Evidence - Although numerous EHRs offer mobile access, the associated security standards can vary, making it essential to ensure that mobile access aligns with the security of desktop versions.

Third-Party Integration Security - Partially Adheres

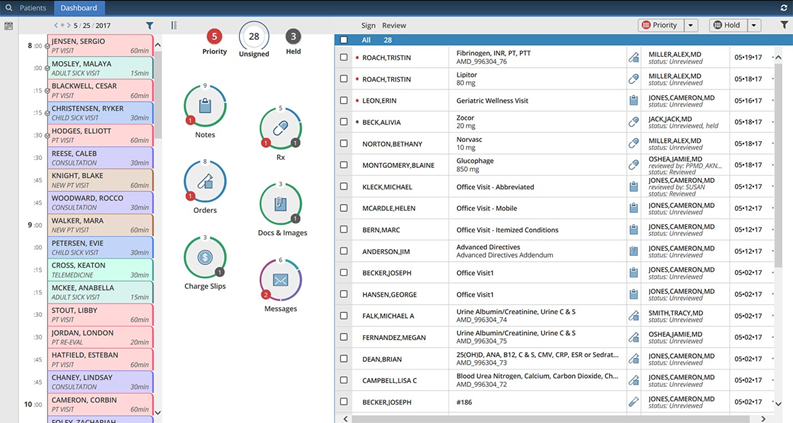
Evidence - Third-party integrations often present security risks, as seen in incidents like the Blackbaud ransomware attack, which impacted Trinity Health’s donor database. EHR vendors must carefully vet and monitor these integrations.

Compliance with Regulations - Mostly Adheres

Evidence - EHR systems are generally designed to comply with healthcare regulations, such as HIPAA, and often adhere to standards like FIPS 140-2 and HITECH.

Regular Security Updates - Mostly Adheres

Evidence - Most reputable EHR vendors provide regular security updates to address new threats and vulnerabilities, though the frequency and thoroughness of these updates can vary by vendor.



· **HIPAA compliance**

HIPAA has set national standards for the protection of identifiable patient information. The rule requires healthcare organizations and their business associates to implement core protections focused on the privacy and security of EHRs. Against the backdrop of the growing ransomware attacks on healthcare systems, this is a critical period in HIPAA compliance as it raises the stakes in protecting patient data and system resilience against cyber threats.

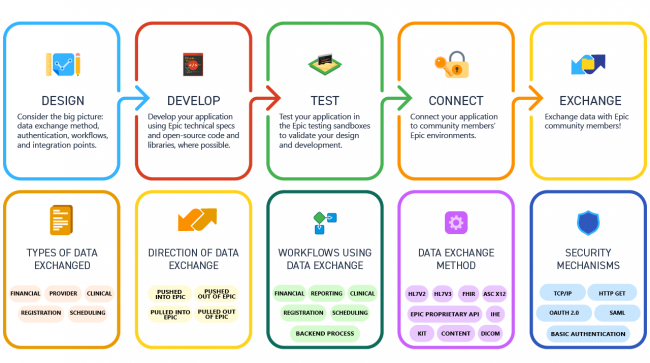
The use of EHR systems must adhere to the laid down HIPPA laws, more specifically the Health Insurance Portability and Accountability Act (HIPAA). This act includes several laws including those applicable in the medical field like safety, transmission and integrity of all data available from the EHR systems. Specifically, the requirements for HIPPA compliance for EHRs.

These include - Mediated access to information: Under HIPAA it is expected that every medical facility should have means in place that allows a healthcare provider to view only the amount of patient addiction the users function positively speaks of. In other words, electronic health record systems should always observe role-based access, which is mainly made. And it may also involve multi factor authentication and specifying per user authorizations.

The Safeguarding of Health Information with Encryption: Achieving the levels of efficiency that we intend include protecting patient information by encrypting the data while it is on the move (transmission over networks), and while it is at rest (stored in EHR databases). Ideally, techniques of data security such as encryption are such that if someone does obtain the data, it is impossible to understand its contents.

Audits: The enforcement unit of the code of strong surveillance to prevent and guard the EHR data against unauthorized access at all times and after any access intervention in internal controls it helps to avoid the potential of unauthorized accesses or changes being made to records. For instance, the EHR systems are required to provide the user access log from where every access, every attempt to modify or interact with the system can be logged.

Incident response and Contingency Planning: In accordance with HIPAA there must be formal incident response and contingency strategies for any security breaches such as data compromise or ransomware infections. Such interventions will encompass storage back up, testing and recovery procedures and lastly system continuity measures.



**Compliance with Privacy and Security Regulations (HIPAA/HITECH)**

Epic EHR is designed with features to support compliance with critical privacy and security regulations. This is my analysis of how effectively Epic aligns with HIPAA and HITECH standards, including potential gaps.

User Authentication and Access Control

Compliance Status: Epic incorporates robust user authentication mechanisms and access control protocols to ensure that only authorized personnel can access patient information. This includes multi-factor authentication (MFA), which adds an extra layer of verification requiring users to confirm their identity through multiple methods. The system also employs role-based access controls, restricting access based on a user's specific role within the healthcare organization and ensuring adherence to HIPAA's principle of minimum necessary access.

Potential Gaps: While Epic's authentication framework is inherently strong, the practical implementation may vary across healthcare facilities. Administrative oversight or insufficient customization could inadvertently allow users broader access than necessary, potentially leading to the exposure of sensitive patient data.

Data Encryption

Compliance Status: Epic employs advanced data encryption protocols for both data at rest and data in transit, aligning with HIPAA standards. This ensures that patient information remains protected against unauthorized access during transmission over networks and while stored within the system.

Potential Gaps: Despite Epic's adherence to high encryption standards, challenges can arise when integrating with third-party systems. Inconsistent encryption practices among these external systems could present vulnerabilities, potentially undermining the robust encryption provided by epic software itself.

Secure Backup and Disaster Recovery

Compliance Status: Epic includes robust backup and disaster recovery functionalities designed to maintain system operations during failures or cyber incidents. These measures align with HIPAA requirements for safeguarding data and ensuring system availability, as healthcare organizations must have processes to quickly restore access to electronic protected health information (ePHI).

Potential Gaps: Although Epic’s built-in backup capabilities are comprehensive, their effectiveness can vary in practice. The data loss experienced by Desert Wells Family Medicine due to substandard backup protocols underscores the necessity of regularly testing and validating these systems. Organizations utilizing Epic should conduct routine backup drills and audits to verify data integrity and reliability.

Compliance with HIPAA’s Security Rule Safeguards

Administrative Safeguards: Epic offers various tools that support compliance with HIPAA's administrative requirements, including risk management, workforce training, and planning for security incident response. It also facilitates the creation and management of data access policies and monitoring of user activity.

Technical Safeguards: Epic’s platform meets HIPAA’s technical safeguard standards through the implementation of encryption, authentication, and audit controls. This includes features such as automatic log-off, data encryption, and data integrity checks.

Physical Safeguards: While Epic supports physical security measures, such as remote access monitoring, responsibility for securing physical infrastructure (e.g., data centers and user endpoint devices) rests with the healthcare organization implementing Epic.

Third-Party Integration Security

Compliance Status: Epic accommodates a range of third-party integrations that enhance functionality, including lab data exchange, billing systems, and patient engagement tools, supporting HITECH’s objectives of improved healthcare communication and interoperability.

Potential Gaps: Integrating third-party systems can introduce security risks if not carefully vetted and managed. The Blackbaud ransomware incident demonstrated how vulnerabilities in third-party systems can impact even well-secured platforms like Epic. Ensuring that all external integrations meet Epic’s stringent security requirements is essential for maintaining overall system integrity.

Patient Portal Security

Compliance Status: Epic’s patient portal, MyChart, enables secure patient access to medical records and provider communication. It employs secure login methods, data encryption, and user authentication to protect patient information, aligning with HIPAA requirements for secure data transmission.

Potential Gaps: Despite the comprehensive security of MyChart, risks related to credential theft and user-side vulnerabilities, such as weak passwords and unsecure devices, persist. Healthcare facilities should provide patient education on secure access practices to mitigate these risks.

Mobile Access Security

Compliance Status: Epic’s mobile app and web-based solutions adhere to the same stringent security protocols as its desktop counterparts, incorporating encryption and user authentication to ensure HIPAA compliance.

Potential Gaps: The effectiveness of mobile access security largely depends on the policies enforced by the implementing organization. Gaps can arise from inconsistent use of mobile device management (MDM) solutions and variations in user training, potentially leading to security vulnerabilities.

**Visual Representation**

EHR System Security Evaluation -

The evaluated EHR system demonstrates strong adherence to many critical security and privacy measures, but there are areas that require improvement:

Strengths:

* Robust user authentication with multi-factor authentication
* Comprehensive data encryption for information at rest and in transit
* Detailed audit trails for user activities
* Regular data backups, with offline storage for critical data
* Compliance with HIPAA regulations

Areas for Improvement:

* Network segmentation is only partially implemented
* Patch management delays for non-critical systems
* Limited monitoring of third-party access
* Inconsistent mobile access security measures

|  |  |  |
| --- | --- | --- |
| **Security Measure** | **Status** | **Notes** |
| Data Backups | ✅ | Weekly checks and backups performed |
| Offline Backup Storage | ✅ | Critical data stored offline |
| Network Segmentation | 🟨 | Critical systems isolated, legacy systems remain on main network |
| Multi-Factor Authentication | ✅ | Required for all accounts |
| Email Filtering | ✅ | Advanced gateway solution implemented |
| Endpoint Protection | ✅ | Next-gen antivirus and EDR solutions deployed |
| Patch Management | 🟨 | Delays in non-critical system updates |
| User Training | ✅ | Monthly security awareness training conducted |
| Incident Response Plan | ✅ | Ransomware-specific plan with regular exercises |
| Third-Party Risk Management | 🟥 | Limited monitoring of third-party access |
| Regulatory Compliance | ✅ | Regular audits ensure HIPAA compliance |

✅ Fully Implemented 🟨 Partially Implemented 🟥 Needs Improvement

Health Care Providers

* Network Segmentation: This would completely segregate critical systems from the main network to avoid breach extension and proliferation.
* Enhanced Patch Management: Create a much more aggressive cadence of patching throughout systems-even non-critical-for reducing vulnerability.
* Third-Party Risk Management: Institute a full lifecycle program in monitoring and managing third-party access to EHR systems.
* Expand User Training: Increase the frequency of security awareness training, including modules on emerging threats such as ransomware and phishing.

EHR Technology Developers

* Enhance Mobile Security: Enhance the security of mobile access to EHRs at least to the same standard when compared to desktop access.
* Improve Interoperability: Continue to emphasize development of standardized APIs that allow for secure sharing between different EHR platforms without sacrificing strong security.
* Threat Detection by AI: Utilize machine learning algorithms to reveal unusual activity that could indicate a potential breach or unauthorized access.

Policy Makers

* Refresh HIPAA Guidelines: Update the guidelines of HIPAA in accordance with recent technologies and newly emerging threats, particularly in mobile health and AI-powered healthcare solutions.
* Create Minimum Standards of Cybersecurity: Establish minimum standards of cybersecurity for health organizations, with particular specification to EHR systems.
* Motivate Security Investments: Incentivize, through financial means, health care providers to invest in cybersecurity infrastructure and better practices.

End-User - Patients

* Password Hygiene Promotion: Educate patients to create strong unique passwords for patient portals and the risks of password reuse.
* Regular Reviewing of Data: Patients are encouraged to review their personal health information on the EHR system periodically and report disparities.

Public Policy Implications

* Regulate and update existing regulations in line with the rapidly evolving cybersecurity challenges within the health sector.
* Needless to say, this is just an update of HIPAA for new technologies and emerging threat landscapes; it is, however, one of the urgent needs for strict standards in cybersecurity that apply universally within the health industry and are regularly updated in order to adapt to technological changes and emerging threats.
* Incident Reporting: Include policies that require or incentivize timely reporting of cybersecurity incidents so as to ensure quicker response times and enhanced preparedness across the industry.
* Patient Rights: As EHR systems advance, policies need to strike a balance between access to patient data while providing security. It is required to definitely specify the ownership and control over patient data.
* Security and Interoperability: Policies should support the development of secure, standardized approaches for sharing data between EHR systems, considering interoperability and security.
* Adhering to such recommendations taken into policy will leave healthcare organizations well on their way towards better enhancement in security and privacy of EHR systems, protecting patient data from emerging threats.

Based on the analysis of EHR systems and their security measures, here are specific actions healthcare providers can take to enhance privacy and security:

Network Segmentation Strengthening

* Healthcare providers should start implementing comprehensive network segmentation to isolate critical EHR systems from the main network.
* Creating distinct network zones for various types of data and applications.
* Utilizing microsegmentation to establish secure zones within the EHR environment.
* Regularly reviewing and updating network segmentation policies to ensure effectiveness.

Improve Patch Management

* To strengthen patch management processes, providers should
* Adopt a more rigorous patching schedule for all systems, including non-essential ones.
* Deploy automated patch management tools for timely updates of the EHR system and associated infrastructure.
* Prioritize critical security patches and develop procedures for rapid implementation.

Enhance Third-Party Risk Management

* To address gaps in managing third-party risks, providers should
* Develop a comprehensive program to oversee and manage third-party access to the EHR system.
* Utilize continuous monitoring tools for third-party integrations.
* Perform regular security assessments for all vendors with EHR access.

Expand User Training

* To enhance the current monthly security awareness training, providers should
* Increase the frequency of training sessions.
* Include specialized modules on new and emerging threats such as ransomware and phishing, tailored to EHR-related scenarios.
* Conduct regular simulated phishing exercises to gauge and improve staff awareness.

Strengthen Backup and Recovery Processes

* Regular testing and backup
* This ensures data integrity and accessibility
* Develop and maintain a recovery plan for this system

Enhance Mobile Security

* Deploy advanced mobile device management (MDM) solutions specifically designed for healthcare settings.
* Ensure that mobile access to EHR systems adheres to the same stringent security standards as desktop access.
* Conduct regular audits and updates of mobile security policies and practices.

Improve Incident Response Capabilities

* Conduct regular tabletop exercises focused on EHR-related security incidents.
* Create a detailed incident response playbook specific to EHR security.
* Establish clear communication protocols for reporting and managing security incidents.

By implementing these measures, healthcare providers can significantly bolster the privacy and security of their EHR systems, address existing gaps, and enhance their overall cybersecurity posture.

**Conclusion**

This project has provided a comprehensive analysis of healthcare data breaches and ransomware impacts, with a specific focus on Electronic Health Record (EHR) systems like Epic. The findings revealed significant vulnerabilities in EHR systems, including insufficient encryption, weak password policies, and insecure third-party integrations, which make patient data and healthcare operations highly susceptible to cyberattacks. The project also highlighted the devastating effects of ransomware, such as operational disruptions, financial losses, and compromised patient safety, as demonstrated by case studies like the Universal Health Services attack in 2020 and the Accellion breach in 2021.

To mitigate these risks, the project proposed a multi-layered approach emphasizing technical measures like advanced encryption, organizational strategies including user training and regular audits, and the adoption of emerging technologies like blockchain and AI. These recommendations are not only vital for safeguarding sensitive patient information but also for ensuring the resilience and continuity of healthcare operations. By addressing the identified gaps, these strategies can influence future decision-making in healthcare technology, paving the way for a secure, patient-centric digital healthcare landscape.

REFERENCES -

* *A look at 2024’s health care cybersecurity challenges | AHA News*. (2024, October 7). American Hospital Association | AHA News. <https://www.aha.org/news/aha-cyber-intel/2024-10-07-look-2024s-health-care-cybersecurity-challenges>
* Alanazi, A. T. (2023). Clinicians’ perspectives on healthcare cybersecurity and cyber threats. *Cureus*. <https://doi.org/10.7759/cureus.47026>
* *Assessment*. (n.d.). <https://www.who.int/teams/health-product-policy-and-standards/assistive-and-medical-technology/medical-devices/assessment>
* Basil, N. N., Ambe, S., Ekhator, C., & Fonkem, E. (2022). Health Records Database and Inherent Security Concerns: A Review of the literature. *Cureus*. <https://doi.org/10.7759/cureus.30168>
* Coker, J. (2024, December 7). 14 million patients impacted by US healthcare data breaches in 2024. *Infosecurity Magazine*. <https://www.infosecurity-magazine.com/news/patients-us-healthcare-data/>
* *EHR/EMR Evaluation Checklist*. (n.d.). Mentalyc. <https://www.mentalyc.com/blog/ehr-evaluation-checklist>
* *Health Technology assessment*. (2008, January 4). ISPOR.org. <https://www.ispor.org/heor-resources/heor-by-topic-new/health-technology-assessment>
* *Manage Third-Party Risks with Mastercard Cybersecurity*. (n.d.). <https://info.riskrecon.com/free-trial-healthcare-ga?cmp=2024.q4.us.nam.all.dir-res.prod.others.healthcare.3.sep.txt.googles&utm_term=cybersecurity%20threats%20healthcare&utm_campaign=Healthcare+US+Search&utm_source=adwords&utm_medium=ppc&hsa_acc=6347508364&hsa_cam=21993760246&hsa_grp=172673800698&hsa_ad=724323778239&hsa_src=g&hsa_tgt=kwd-2380515430026&hsa_kw=cybersecurity%20threats%20healthcare&hsa_mt=p&hsa_net=adwords&hsa_ver=3&gad_source=1&gclid=Cj0KCQiApNW6BhD5ARIsACmEbkX6SwxuVNMIkJjcdCmYTNW25fEL2CXxkmzioBdvAK76J8Z0G48s_wAaAsexEALw_wcB>
* *Ransomware Protection Solution | Lepide*. (n.d.). <https://www.lepide.com/page/ransomware-protection-demo/?utm_term=ransomware%20protection%20solution&utm_campaign=Ransomware-USA&utm_source=adwords&utm_medium=ppc&hsa_acc=8546785528&hsa_cam=21256103462&hsa_grp=161281994345&hsa_ad=702565327094&hsa_src=g&hsa_tgt=kwd-352698322766&hsa_kw=ransomware%20protection%20solution&hsa_mt=p&hsa_net=adwords&hsa_ver=3&gad_source=1&gclid=Cj0KCQiAx9q6BhCDARIsACwUxu6E6heVP8_bBVsC9_v7Fg1oP8gGAhGZ9TKbHbE-31svg7_ESwhvTw4aAuW8EALw_wcB>
* Schutz, M. (2024a, November 13). Arizona Medical Practice Completely Loses EHR System in Ransomware Attack. *Arizona*. <https://pktech.net/blog/2021/10/arizona-medical-practice-completely-loses-ehr-system-in-ransomware-attack>
* Schutz, M. (2024b, November 13). Arizona Medical Practice Completely Loses EHR System in Ransomware Attack. *Arizona*. <https://pktech.net/blog/2021/10/arizona-medical-practice-completely-loses-ehr-system-in-ransomware-attack>
* Yeo, L. H., & Banfield, J. (2022a, March 15). *Human Factors in Electronic Health Records Cybersecurity Breach: An Exploratory analysis*. <https://pmc.ncbi.nlm.nih.gov/articles/PMC9123525/>
* Yeo, L. H., & Banfield, J. (2022b, March 15). *Human Factors in Electronic Health Records Cybersecurity Breach: An Exploratory analysis*. <https://pmc.ncbi.nlm.nih.gov/articles/PMC9123525/>
* <https://www.selecthub.com/medical-software/ehr/ehr-security/>
* <https://pmc.ncbi.nlm.nih.gov/articles/PMC9123525/>
* <https://www.mentalyc.com/blog/ehr-evaluation-checklist>
* <https://www.hipaajournal.com/change-healthcare-responding-to-cyberattack/>