The Essentials for Healthcare Data Security

Author – **DEEPAK MATHAM**

CISM, CEH

AVP – IT Security, Inovaare Corporation

Overview

Today, practices and services offered by healthcare providers help to improve quality of care at a decreased cost. However, this opens up access to large amounts of healthcare data, a popular target for attackers and hackers, as they contain confidential information such as:

- Demographics
- Social Security numbers
- Credit card information

As such, the healthcare sector is suffering from many data breaches.

According to hipaajournal.com, 707 breaches were reported in 2022, resulting in compromise of a staggering 51,000,000 healthcare records. In 2021, there were 715 breaches and 54 million healthcare records compromised. These are scary numbers to look at.

Of the 707 breaches reported in 2022:

- 555 breaches are the result of hacking or an IT incident
- 113 are the result of unauthorized access or disclosure
- 35 are the result of loss or theft
- 4 are the result of improper disposal

In 2022, more than 43 million records were compromised due to hacking or an IT incident. The major portion of these breaches happened at network servers and through emails. The numbers are even greater when you factor in business associates and healthcare providers, who handle most of the healthcare data. Settlements and penalties accounted for $2,127,140 in 2022, alone.

Importance of Data Protection in Healthcare

Healthcare entities — including, but not limited to health plans, healthcare providers, and business associates — need to store protected health information (PHI) such as demographic data, medical history, and treatment information. This type of information falling into wrong hands could lead to many consequences, including malicious intent to conduct fraudulent activities. Such incidents could lead to reputational loss, defamation and adverse effect on the organization's brand. Additionally, such breaches could lead to penalties and lawsuits, as PHI is protected by laws such as HIPAA & HITECH.

There are various cyber threats which result in breaches, such as:

Malware Attacks

Malicious programs in the form of a virus and trojans targeting endpoints, which can spread onto servers.

Ransomware Attacks

Data or drives get encrypted, and a ransom amount (typically in crypto currency) is demanded for decryption.

Social Engineering (phishing/vishing/whaling)

Social accounts are used to gather required information followed by the spoofing of identity to send phishing emails, manipulation of devices, theft of equipment, etc.

Protective Measures

Some protective measures to safeguard healthcare data include:

- Application control to protect from malware
- Education
- Training
- Awareness enhancement
- Multifactor Authentication (MFA)
- Endpoint Detection and Response (EDR) software,
- IDS/IPS
- Web Application Firewall (WAF)

It is always recommended to implement a Zero Trust approach, which is the principle of Never Trust, Always Verify. This approach treats all assets, services, and users equally and distrusts them.

In an era where BYOD (bring your own device) and work from anywhere is allowed, the Zero Trust approach works better compared to traditional approach. This way, all the devices, services, and users are verified before being allowed and authorized.

Malware attacks can be controlled by using a strong endpoint protection software as well as implementing tamper protection. Additionally, the use of EDR applications will help to enable real-time visibility and control over endpoints.

Use of network and host-based IDS/IPS will help in detecting and blocking any intrusion attempts. Using WAFs on web applications will help in blocking any vulnerabilities including Open Web Application Security Project (OWASP) top 10 at the application layer.

Best Practices

The following best practices will help the healthcare industry to protect their data.

Perform risk assessments: Security best-practice begins with risk assessments. Yet, many organizations in healthcare sector are not conducting them. Risk assessments help organizations to maintain a balance between access and security. This will, in turn, help to maintain a balance among CIA (confidentiality, integrity, and availability).

Secure endpoints: Securing endpoints is a critical area that protects endpoints like desktops, laptops, mobile devices, databases and other servers. This best-practice includes usage and restrictions of USB storage devices, CDs/DVDs and other peripheral devices.

One of the most important aspects of this protection is being proactive. Traditional antivirus, antispyware and signature-based protections, which are reactive, were perfect solutions until a few years ago. Fortunately, current endpoint protection and EDR software are proactive, which will help us from zero-day vulnerabilities, as well.

(Note: Typical endpoint protection and EDR software comes equipped with antivirus, antispyware, firewall, IPS and device controls, which are recommended for enhanced security.)

Minimize data leakage: It is recommended to enable and implement DLP (data loss prevention/protection) on endpoints as well as at email gateways.

Encrypt: Encryption plays a key role in protecting healthcare data. Encryption of data is recommended at all stages and places — at rest, in transit and while in use. Since encrypted data will be in unreadable format, even if such data is compromised, it will not lead to data breach.

Mobile security: Today's mobile devices are more usable and advanced than many sophisticated computers, which means they contain a vast amount of sensitive data. The theft of mobile device poses a serious threat.

To protect from such threats, it is recommended to implement stringent mobile device security policies and implementation of MDM solutions. MDM solutions leverage services like:

- Rolling out installation packages
- Segregation of sensitive and enterprise data from other data on the mobile device
- Log capturing
- Remote wiping

Ensure regulatory compliance, and adopt frameworks and mapping controls: As part of risk assessments, it is recommended to list the regulatory and compliance requirements, and adopt a framework accordingly. Beyond this, mapping a control against each of the regulatory and compliance requirements will help organizations to:

- Automate and actively measure compliance
- Report gaps
- Enforce policies

Such policies include, but are not limited to, minimizing threats identified, bringing residual risk scores within the risk appetite and reducing the impact of security incidents etc.

Regular reviews: It is recommended to periodically review policies, procedures, new threats, risks and their treatments, data mapping etc., and present them to the stakeholders. Such reviews will help to address critical issues on priority, thus minimizing data compromise.

Inovaare's Practices on Data Security and Privacy

Inovaare is committed towards safeguarding information through rigorous high-standards information security and compliance processes. The Information Security Team is comprised of highly qualified professionals who focus on appropriate risk-management and other requirements including:

- Business continuity
- Information security
- Compliance with privacy regulations, standards and frameworks

Our security programs include the implementation of a proactive and robust Information Security Plan to protect information assets. Inovaare's facilities and platform are HITRUST and ISO 27001 certified, which confirms our commitment towards the security and privacy of customer data.

Inovaare considers Information Security Management to be a key domain, and invests appropriately in implementing a strong Information Security Management system and controls. The Information Security Program at Inovaare is led by the Information Security Officer (ISO), who is assisted by a dedicated team of security professionals.

To ensure a minimum baseline standard for information security across the organization, Inovaare has adopted an ISO 27001 framework and is certified by qualified external, independent assessors. Our internal information security audits cover information and pertaining assets; cloud and infrastructure security; personnel security; physical and environmental security; SSDLC, business continuity; change management; and incident management. These audits are compliant with contractual as well as regulatory (e.g., HIPAA, HITECH) obligations.

The following are some of the highlights of our information security practices:

- Regular and detailed vulnerability assessments and penetration tests
- Malware protection, intrusion prevention or detection systems
- Hosting partners are chosen for infrastructure and data hosting based on certifications and compliance standards including, but not limited to, ISO 27001, HITRUST and SOC2
- Enforcement of requirements and guidelines from HIPAA/HITECH, ISO 27001, HITRUST, NIST, etc. into our solutions, services, processes, policies, and procedures

Data security is essential in healthcare and Inovaare has its clients covered. Its qualified and certified IT security experts manage data security to keep current on the latest global threats and risks. Inovaare performs internal and external assessments to ensure all necessary elements are checked — from an information security perspective — as well as to make sure data is always secured.

Inovaare's information security objectives are amalgamated into cross-cloud platforms where its software-as-a-service (SaaS) solutions reside. This way, Inovaare ensures it delivers consistently reliable solutions with high uptime, uninterrupted availability and ironclad data security.

Recognizing the importance of protecting the privacy and integrity of PHI, Inovaare has developed organizational security policies and procedures in compliance with HIPAA requirements. Inovaare's information security team — led by its ISO — coordinates, monitors and maintains the compliance plan.

Conclusion

The following are the best practices that are recommended to ensure healthcare data is secured:

- Application of risk management approach
- Protection of endpoints
- Minimizing data leakage by enforcing encryption of data at rest, in transit, and while in use
- Implementing MDM and EDR solutions
- Identification of regulatory and compliance requirements, adoption of standards and mapping of controls
- Regular reviews of policies, procedures, assets, risks, etc.

About Inovaare

Inovaare simplifies complex compliance processes by designing configurable solutions so healthcare organizations can collect real-time data across internal and external departments, creating one centralized management system. A comprehensive suite of HIPAA-compliant software solutions features best-practice regulatory processes to help healthcare organizations efficiently meet their unique business requirements, sustain audit readiness, reduce noncompliance risks and lower overall operating costs.

Far from being a one and done software vendor, Inovaare has been serving health plans and healthcare providers since 2008, offering over 125 years of combined compliance experience to consult and guide clients through each step of every process within an ever-changing regulatory environment. Since each organization's compliance demands are as complex as the regulations they need to comply with, Inovaare tracks every shift in the regulatory landscape so its automated applications consistently satisfy evolving reporting requirements.

Inovaare's unparalleled responsiveness and agility ensure healthcare organizations won't get caught off guard or unprepared for regulatory audits. Inovaare studies its clients' unique needs and objectives to deliver solutions based on current regulatory requirements and protocols so health plans and providers remain in compliance, avoid fines and improve their bottom line.

If you would like to explore how Inovaare can help you sustain audit readiness, please contact us at info@inovaare.com or 408-850-2235.

Request a Demo