Data Protection for the Healthcare Industry
Executive Summary

The nature of the healthcare industry has changed dramatically over the past decade, as those who provide health-related services have begun moving from paper-based processes to electronic methods. Today, it is not uncommon to have a doctor enter an exam room with a laptop in hand instead of a paper medical chart. The healthcare business generates massive amounts of data and those in the field recognize the benefits to be gained from incorporating more digital processes into their daily operations – cost savings, increased efficiency, and improved communications, to name a few. However, those are not the only incentives.

In the U.S., the federal government has recognized the advantages of health information technology (HIT). The Health Information Technology for Economic and Clinical Health Act (HITECH) of 2009 requires the U.S. government to take a leadership role in developing standards by 2014 that “allow for the nationwide exchange and use of health information to improve quality and coordination of care.” Under the Act, $20 billion dollars has been allocated for investment in the HIT infrastructure to encourage doctors and hospitals to electronically exchange patient health information. While the Act vigorously promotes the move to an electronically interconnected healthcare environment, it also mandates the strengthening of federal privacy and security laws to protect identifiable health information from misuse, expanding upon the regulations already in place through the Health Insurance Portability and Accountability Act (HIPAA). The U.S. Congressional Budget Office estimates that, as a result of the HITECH legislation, approximately 90 percent of doctors and 70 percent of hospitals will be using electronic health records (EHRs) within the next decade.

From medical records to insurance forms to prescription services, the healthcare business is becoming a networked environment that allows patient information to be shared and managed by a variety of resources and from a number of endpoints, each with their own level of security for protecting that information. Not only are healthcare organizations often times mandated to protect this information from data breaches and fraud, it is imperative for the health of their business that patients have confidence that their personal information remains private and secure.

Introduction

Identity thieves have expanded their target list to include not only financial records but medical information. Cyber criminals see medical records as particularly valuable as they include not only names and addresses, but also employer and bank account/credit card information. By stealing a patient’s personal data and health insurance information, thieves are able to illegally obtain medical goods and services. The victim is then left to deal with the doctors, hospitals, insurance companies, and creditors to resolve the ensuing financial fallout. In some cases, the victim can even lose their medical coverage, resulting in costly out-of-pocket payments to have their insurance reinstated. There is also the concern of the legitimate patient’s medical record having altered or incorrect information, which may prevent them from obtaining proper medical treatment and insurance benefits.

According to a recent study by The Ponemon Institute, nearly 5.8% of American adults have been victims of medical identity theft, with an average cost per victim of $20,160. In the study, victims reported that they were sent collection notices for hundreds of thousands of dollars for medical procedures and surgeries performed under their names. The study estimates the total cost of this type of crime in the U.S. at $28.6 billion.

In a 2010 report by the Healthcare Information and Management Systems Society, since 2008, more than 110 healthcare organizations reported the loss of sensitive patient data affecting over 5.3 million individuals. In addition, according to the Federal Trade Commission, more than 300,000 Americans were victims of medical identity theft in 2009. The following examples serve to illustrate the growing issue of securing electronic healthcare information:
May 2009 – In Virginia, a hacker stole over 500,000 patient records from a state-run database that tracks drug prescriptions, and then demanded a ransom to return the information.

October 2009 – BlueCross BlueShield of Tennessee reported the theft of 57 computer hard drives from a training facility. BCBS initially reported that the drives did not contain personal information and that they were encrypted, but they later rescinded both statements. To date, they have spent more than $7 million recovering from the breach, including credit monitoring services for the 220,000 people affected and 700 employees working to identify the details of the breach.

January 2010 – The Methodist Hospital in Houston, Texas reported the theft of a laptop from a medical office in the Texas Medical Center. The laptop was attached to a medical device that test pulmonary function, and contained private health information and Social Security Numbers of 689 people. The hospital has offered one year free subscription for credit monitoring and identity theft protection to those affected.

February 2010 – The Connecticut Attorney General has sued Health Net, claiming the insurance company failed to adequately protect the medical records of 446,000 patients whose private data was stored on a missing disk drive, and waited six months to notify customers of the breach. The missing disk contained health information, Social Security Numbers, and bank account numbers.

Protecting data is much like dodging a barrage of arrows. With no shortage of insiders and outsiders attempting to compromise valuable patient information, increasing global collaboration between doctors, hospitals, insurance companies, partners, and suppliers, and a growing list of industry and government privacy/disclosure regulations, those in the healthcare industry are under mounting pressure to focus intently on information security.

Threats to sensitive data have reached a critical point, with the sophistication and frequency of attacks escalating over the last several years. It is imperative that healthcare organizations implement security solutions that will not only protect important data assets but also satisfy the compliance mandates to which they are held accountable. Reaching the appropriate balance between ease of communication and strong protection of sensitive information is one of the most significant challenges faced by today's business network and security teams.

Ecosystem

Data protection is comprised of many elements, including where the data resides, how it is used, and who has access to it. Risk comes from both inside and outside the organization – from employees to third-party vendors and cyber criminals looking for financial gain or to intentionally or unintentionally inflict damage to an organization's reputation.

In October 2009, the Ponemon Institute published a report entitled Electronic Health Information at Risk: A Study of IT Practitioners. The report surveyed IT practitioners from healthcare organizations that collect patient health information in both paper and electronic format - 61 percent of respondents are employed by healthcare providers, plans or insurance companies (HIPAA covered entities), while the remaining 39 percent are employed by HIPAA business associates or hybrid organizations.

The majority of IT practitioners in the study believe that their organizations do not have adequate resources to protect patients' sensitive or confidential information, citing that “a lack of resources and support from senior management is putting electronic health information at risk.”

According to the study, the top three emerging threats to EHRs are virus or malware infections, data breaches, and malicious employee attacks. The top ranking security measures employed to combat these threats are policies and procedures, anti-virus and anti-malware systems, training and awareness programs, and perimeter controls, such as multi-layered firewalls.

Perhaps the most startling statistic in the report is that 90 percent of respondents reported that their organization had one or more data breaches that involved the loss of patient health information, with the most vulnerable locations being hospitals, clinics, and insurance companies.

Data protection is more challenging when information is shared among multiple resources, devices, and locations. Since each endpoint can have their own level of security practices and procedures, there is an increased opportunity for a breach to occur. Many organizations use various point solutions to protect different areas of their infrastructure. While each solution may be strong on its own, a lack of cohesiveness between disparate products can result in gaps in security that can be easily exploited. Any type of disjointed, inconsistent approach will leave areas of weakness and vulnerability.
Fingers on the Pulse

The healthcare industry is held to exacting rules regarding the confidentiality of patient records. Regulations such as HIPAA, HITECH, and the EU’s Data Protection Directive define guidelines around the world that the healthcare industry must adhere to in order to be compliant and protect patient privacy. In the U.S., forty-seven states plus the District of Columbia, New York City, and Puerto Rico have their own varying laws regarding how public and private organizations should handle breaches of sensitive information.

HIPAA, the Health Insurance Portability and Accountability Act, is a far-reaching standard that provides federal protections for personal health information held by covered entities (healthcare providers, health plan administrators, healthcare clearinghouses, schools, and universities) and provides patients with various rights related to that information. HIPAA’s Privacy Rule applies to all forms of an individuals’ protected health information (electronic, written, and oral), and regulates who can look at and receive this information, while the Security Rule requires covered entities to ensure that electronic protected health information is secure.

Building on the scope of HIPAA requirements, the Health Information Technology for Economic and Clinical Health Act (HITECH), Title IV of the America Recovery and Reinvestment Act of 2009 (ARRA), stipulates mandatory data breach notifications, heightened enforcement, increased penalties, and expanded patient rights. HITECH also requires the U.S. government to take a leadership role in developing standards by 2014 that “allow for the nationwide exchange and use of health information to improve quality and coordination of care.”

Under the Act, $20 billion dollars has been allocated for investment in the health information technology (HIT) infrastructure to encourage doctors and hospitals to electronically exchange patient health information. Doctors and hospitals can qualify for the funds upon certification that their implemented technology conforms to mandated standards for data security. The U.S. Congressional Budget Office estimates that, as a result of the HITECH legislation, approximately 90 percent of doctors and 70 percent of hospitals will be using EHRs within the next decade. While the Act vigorously promotes the move to an electronically interconnected healthcare environment, it also mandates the strengthening of federal privacy and security laws to protect identifiable health information from misuse.

The Data Protection Directive is a European Union (EU) edict implemented in 1995 that regulates the processing of personal data within EU member states, including healthcare data. While each member state must transform the directive into internal law, it serves as an important component of EU privacy and human rights regulations. European Union countries spend upwards of €1 trillion Euros a year providing nationalized healthcare for their citizens. A report by the European Healthcare Fraud and Corruption Network concludes that “€56 billion Euros of these healthcare budgets are lost to fraud in Europe annually and €180 billion Euros globally.”

Healthcare consumers expect their medical information to be properly protected. The myriad of regulations in existence throughout the world place direct and irrefutable responsibility upon those in the health industry to implement that protection or face legal and financial repercussions.

Considerations

All standards for protecting electronic health records revolve around access and audit controls, data integrity, person or entity authentication, and transmission security. Access controls must be implemented to manage the users and applications that are allowed access to systems containing EHRs. Audit control processes must record and analyze activity involving systems that store or process EHRs. Policies and procedures regarding the integrity of data must be implemented that protect EHRs from improper modification or deletion. Authentication policies and procedures must be implemented to verify persons or entities attempting to access files and systems that contain EHRs. Policies and procedures must be implemented to prevent unauthorized access to EHRs that are transmitted over public networks, such as the Internet.

With new federal rules and incentives focused on increased interoperability among healthcare service providers, it will be increasingly important that the healthcare ecosystem be comprised of security solutions that work together to address the constantly evolving challenges that face the industry, and satisfy the stringent requirements for end-to-end data protection and privacy to which the industry is held.

It will also be imperative for these types of covered entities to implement encryption to protect not only the transmission of electronic patient information, but in databases as well. Encryption, combined with strong access control, provides the highest level of protection for data in all circumstances, ensuring that it is protected should it fall into the wrong hands. By placing a defined
set of controls around each user’s access to files and applications, the healthcare organization creates an environment of non-repudiation. So even if an authorized person should decide to do something illicit with the data they’ve been granted access to, there will be an auditable trail leading directly to who, what, when, and where.

To ensure patient privacy, secure patient records, medical images, and applications, and reduce the cost and complexity of compliance, SafeNet recommends a solution comprised multi-factor authentication technologies, hardware security modules (HSMs), high-speed encryptors (HSEs), and data encryption and control solutions. With complete information lifecycle data protection, healthcare organizations will be able to secure EHRs and easily transfer it among doctors, insurance providers, and other healthcare entities. Sophisticated encryption, access, and policy management solutions provide end-to-end data security to satisfy even the most exacting government and industry requirements.

As the healthcare industry moves toward a true EHR system, the validation and authenticity of documents must be ensured. Digital signature solutions provide in-network and out-of-network healthcare providers with complete confidence that electronic files are valid, and enable trust in the security of their patient data management system. Pharmaceutical organizations, as well as universities, are moving towards digital signatures for providing security and trust in pharmaceutical and clinical trials. With a trusted solution for paper-to-digital transmissions, confidence in data transfers can be ensured, and can result in expedited time to market for both pharmaceuticals and breakthrough medical procedures.

By securing healthcare information from the data center to the endpoints, and even into the cloud, healthcare organizations can protect databases, applications, networks, identities, transactions, and individual files. This approach allows healthcare entities to align IT goals and business growth strategies with a comprehensive, intelligent, persistent and extensible solution that easily integrates into their current architecture.

Usernames and passwords are no longer enough to protect access to patient records, and regulatory mandates, such as HIPAA and HITECH, now require heightened login credentials that will provide audit trails. By implementing authentication technology that adapts as your organization changes, such as hybrid tokens and OTP, you can construct an authentication solution to fit your healthcare network. With granular policy management, patient medical records and information are accessed only by authorized parties. With the proper procedures in place, patient medical records, lab results, DICOM images, and hospital and pharmaceutical information are all kept in an encrypted state, only viewed in the clear by authorized parties as dictated by policy.

Conclusion

The healthcare industry is under pressure to transition to an electronic environment in which patient information can be exchanged quickly and easily among healthcare stakeholders. Not only are paper-based processes becoming antiquated and inefficient in today’s fast-paced medical settings, doctors and hospitals are being presented with financial incentives to implement technology into their practices and join a growing system for the electronic use and exchange of health information.

While the impact of electronic health records (EHRs) will be broad and profound in terms of the effect on the operation and management of healthcare organizations, the inherent risks associated with the transmission and storage of electronic data of any type also need to be considered and addressed—not by choice, but by law.

Reports have shown that medical identity theft is on the rise, and the ramifications can be acute and far-reaching to all involved—from the patient whose medical and financial records are directly impacted to the doctors, hospitals, and insurance companies, who spend countless resources pursuing payments, assisting victims, and perhaps even defending themselves against lawsuits. Though different in terms of damage, this type of crime inflicts pain to both the patient and the provider.

Protecting electronic patient information from malicious employees and a variety of external threats is a requirement, as well as a challenge, for many healthcare organizations. Piecemeal protection schemes are ineffective on several levels—they do not provide optimal, comprehensive security, are not cost-effective, and, in the long run, do not effectively address the secure interoperability that is required for the HIT infrastructure.
SafeNet believes an effective implementation must consist of security solutions that work together to address the constantly evolving challenges facing healthcare organizations. With a flexible, centralized solution that provides complete information lifecycle protection, healthcare entities can align IT strategies with future business growth through an approach that is comprehensive, intelligent, persistent, and extensible. With a single, comprehensive platform, healthcare organizations can achieve end-to-end protection for identities, transactions, and applications, ensure regulatory compliance, and secure local, as well as remote, access to critical applications and EHRs.

---


3 National Study on Medical Identity Theft, Ponemon Institute


