Data Protection and Security in the Healthcare Industry:

CHALLENGES AND SOLUTIONS

US SIGNAL®

TABLE OF CONTENTS

AN INDUSTRY AT RISK

Between a pandemic, evolving government regulations, rising costs, payment reform, and other issues, the healthcare industry has its metaphorical hands full. One challenge, in particular, that seems to never abate is the threat of data breaches.

A 2020 data breach report noted that the past year was the worst ever in terms of healthcare data breaches. There were 572 data breaches of 500 or more records reported to the Department of Health and Human Services' (HHS) Office for Civil Rights and other sources in 2019 — up 48.6% from 2018. The number of compromised or exposed records is known for 481 of them and totals 41,404,022 patient records that were breached.

Things aren't looking good for 2020. Between January and May 2020, well over a million individuals have been affected by healthcare data breaches, according to the HHS.

When these incidents occur, they aren't cheap. A 2020 IBM report notes that healthcare is the most expensive industry for a data breach at $6.45 million.

THE HIGH VALUE OF HEALTHCARE DATA

Why are hospital systems, clinics, physician groups, insurance providers, medical device manufacturers, and other types of organizations in the healthcare industry so vulnerable to cyber-attacks? And, why are the attacks so costly? Three words: protected health information (PHI).

PHI is information in a medical record that can be used to identify an individual. It's created, used, or disclosed in the course of providing a healthcare service. Even more so than credit card numbers, PHI is a hot commodity on the black market.

It's valuable because it tends to include specific details such as an individual's date of birth, full name, and Social Security number. Cybercriminals can use that information to commit identify theft and access individuals' bank accounts, obtain prescriptions for controlled medications, open credit card accounts, and more.

When PHI is stolen, time-to-report and time-to-discover periods are often long, giving cybercriminals time to collect and sell stolen records before vulnerabilities are detected and patched. For example, in 2019 a data breach exposed patient data at Munson Healthcare Group from July 31 to October 22 but went undetected until January 16, 2020.

NO TIME FOR DOWNTIME

Stolen data isn't the only repercussion of cyber-attacks. They can also result in business-disrupting downtime.

In July 2018, the electronic health records (EHR) system at Blount Memorial Hospital in Tennessee was offline for three days. During that time, 90 doctors were unable to access patient records. Appointments were canceled. People didn't receive care.

Downtime is expensive. In a 2019 survey conducted by Statista, 25% of respondents worldwide reported the average hourly downtime cost of their servers as being between $301,000 and $400,000. That takes into consideration metrics such as business disruption, lost revenue, end-user and IT productivity, detection, recovery, equipment and third parties.

In the healthcare industry, however, financial costs are the least of organizations' concerns — particularly if they're involved in patient care delivery. Downtime — whether due to a cyberattack, a natural disaster, or another cause — poses a threat to patient safety and patient care continuity.

Learn how Baystate Health gained near continuous block-level replication for proven RPOs of seconds and RTOs of minutes

READ CUSTOMER STORY

WHERE THE RISKS ARE

In terms of the threats to IT systems in the healthcare industry, ransomware seems to be the most prevalent. According to Verizon's 2020 Data Breach Investigations Report, ransomware attacks represented over 70% of all malware incidents in healthcare.

Distributed denial of service (DDoS) attacks also pose serious threats. A DDoS attack bombards a server with access requests. The server processes each request to determine its identity, origin, and credentials. But cyber-attackers don't care if access is granted. Their goal is to tie up the server's processing capabilities so that the overworked server eventually crashes.

The growing use of connected medical devices and other IoT devices also translates into more targets, risks, and endpoints to manage, protect, and continually monitor. Internet of Medical Things (IoMT) devices, in particular, have inherent risk factors that increase the chances of a data breach. They have largely unquestioned access to much of the data stored on a healthcare organization's network. Security features often aren't embedded, increasing the risk of human error.

THE REALITY OF HUMAN ERROR AND INSIDER THREATS

It's not just cybercriminals behind security incidents in the healthcare industry. Employees, vendors, and other insiders are often to blame. These insider threats are also are among of the most difficult to detect and mitigate.

The 2020 Data Breach Investigation Report (DBIR) points out that in healthcare, more often than in other industries, security breaches take the form of privilege misuse, lost or stolen assets, and web application attacks. The report also noted that insider incidents, both malicious and accidental, are more common than external attacks.

Negligence is often the issue, such as leaving a personal laptop or mobile device at a coffee shop or inserting an infected USB into a device. Also high on the list of causes — using weak passwords on devices, sharing information about a patient's treatment or prognosis with someone who doesn't have a legal right to it, and giving inappropriate system access to someone to get a job done quickly.

Insider security breaches may also result from malicious attacks and grudges, especially in the case of disgruntled employees. In one case, an employee at a facility in Maryland used his privileged network access to steal patient data. He then used the data to fraudulently obtain credit cards over a two-year period before being caught.

MAKE DATA PROTECTION AND SECURITY BUSINESS IMPERATIVES

As is the case in many industries, healthcare organizations tend to base their data protection and security plans on short-term cost-benefit analyses: do what's cheaper now and hope for the best later.

When the best doesn't happen but breaches or data losses do, the end results can be costly. Investing in data protection and data security approaches that deliver both short- and long-term benefits will be far more cost effective in the long run.

That requires making data protection and data security a business priority, so build your business case. Identify your proof points. Seek out executive support.

The specifics of a comprehensive strategy will vary based on the nature of your organization, the type of data and applications you handle, your stakeholders, and other factors. However, the information that follows provides some important elements to consider.

Business Continuity and Disaster Recovery in Healthcare

CLICK TO READ 3 USE CASES IN THIS WHITEPAPER

KNOW YOUR DATA

Start with a data inventory. You can't protect data if you don't know what it is or where it is.

Data can take many forms, from patient insurance/payment information to digital images to physician peer reviews. There's also the enormous flux of data generated by electronic health records (EHRs), medical devices, and other technologies.

+ Identify where your data exists. It can reside in patient registration systems and accounting systems, electronic patient charts, monitoring devices, telemetry systems, and even on employee laptop computers.
+ Map where your data goes, including when it's accessed, stored, or transmitted outside of the physical premises of your healthcare organization. For example, a physician may need to access an ePrescription application from a smartphone while out of the office to respond to a patient request for a prescription refill.
+ Determine how data travels throughout and beyond your organization. Identify who handles it or has the opportunity to handle it along the way. Factor in mobile devices and the various scenarios in which staff or vendors may interact with patient data.

It's a good idea to pull in representatives from various departments throughout your organization to make sure you are covering everything.

REVIEW YOUR DATA SECURITY STRATEGY

Assess your current data security and privacy strategies. Map the various tactics within your data security strategy to your data inventory and the various routes your data takes.

Are tactics in place at every touch point? How effective are they? How often are they reviewed and updated? Do they account for potential attacks by cyber criminals or the loss of data due to employee negligence?

Think of all potential ways data could be compromised. Document potential "holes" in your security plan.

Test all aspects of your data security approach. For example, assess how effective your employee security training programs are and how well employees abide by the security protocols. Periodically "attack" employees at all levels in your organization with phishing and other social engineering campaigns.

Fill in the gaps with US Signal's Managed Security

CLICK TO LEARN MORE

ESTABLISH AN INCIDENT RESPONSE PLAN

Knowing the risks to your data is one thing. Knowing how to respond if data is compromised is another. Develop a data breach response plan and have an incident response team ready to enact it.

Each team member should be thoroughly trained in the steps to take to stop data leakage or prevent additional data from being compromised, as well as to determine the source of the breach. Make sure to test the plan frequently and update it as needed.

The Office of the National Coordinator for Health Information Technology (ONC), U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR), and other HHS agencies have developed a number of resources for you. These tools, guidance documents, and educational materials are intended to help you better integrate HIPAA and other federal health information privacy and security into your practice.

While not specific to the healthcare sector, the following resources can help as well:
+ Data Breach Response: A Guide for Business (Federal Trade Commission)
+ Data Breach Response Guide (Experian)

MEET YOUR COMPLIANCE REQUIREMENTS

If you're classified as a "covered entity" by the HHS, are you in compliance with the requirements stipulated by HIPAA and HITECH? If you're an eligible provider under the Center for Medicare and Medicaid Electronic Health Care Record (EHR) Incentive Program, can you "attest" to meeting the HIPAA and HITECH requirements it requires? If your data is handled by third parties classified as "business associates," are they in compliance?

Identify weaknesses, potential threats, and possible compliance violations. Don't assume that because you work with vendors or systems that are "HIPAA-compliant" that you're off the hook for compliance. Ultimately, the responsibility for compliance with regulatory requirements such as HIPAA rests with your organization.

Insist on seeing documentation from any vendor you work with that claims to be HIPAA compliant. Hold business associates accountable by reserving and exercising your right to audit them.

In addition, entities defined as "business associates" are required to sign a business associate agreement (BAA). Don't do business with a vendor that refuses do so. For information on who is considered a business associate and what is required in a BAA, refer to the information at http://www.hhs.gov.

US Signal is audited for HIPAA compliance annually by an independent third-party auditor, and will sign a Business Associate Agreement (BAA).

Know the right questions to ask when considering vendors

READ "PARTNERING FOR COMPLIANCE IN THE CLOUD"

IMPLEMENT/REVIEW MOBILE AND BYOD POLICIES

Establish a mobile device/Bring Your Own Device (BYOD) policy that includes employee and management procedures as well as technical controls. If you already have a policy in place, review it to ensure that it includes the components that follow.

+ Limit access from mobile devices to critical systems that contain or connect to PHI and other healthcare data. Review and evaluate who absolutely needs access to these systems, and require special log in procedures.
+ Educate employees about possible data breaches, viruses and insider threats and the role they each play in preventing them.
+ Outline instructions for protecting devices from possible theft or hacking and how to report a suspected data breach.

Make this information available to all employees as well as to any third-party companies you work with that handle your protected health information and are considered “business associates” by the Department of Health and Human Services (HHS).

PRIORITIZE DISASTER RECOVERY

It’s not enough for organizations in the healthcare industry to ensure the security and privacy of their data. They also must be able to recover it — and for most, never to lose access to it. Failure could result in severe financial penalties and, worse-case scenario, impact lives.

Here are some key points related to disaster recovery and business continuity in the HIPAA Security Final Rule:

+ All hospitals and health systems, including medical practices, must securely back up “retrievable exact copies of electronic protected health information.”
+ Health systems must back up their data regularly. Many organizations do this nightly to comply with regulations.
+ Health systems must be able to recover their data, and be able to fully “restore any loss of data.” The process is to failover the information to a target site where there is standby equipment. A disaster recovery process must then be executed to build the applications with the associated data so that the system is fully usable to deliver patient care.
+ Once in recovery mode, health systems must still maintain safeguards.
+ Both the 2009 HITECH Act and the HIPAA Security Rule require health systems to encrypt or destroy data.
+ Health systems must have written documentation of policies and procedures for data recovery plans.
+ Recovery testing is mandatory.

CLICK TO SEE ALL DR OPTIONS FROM US SIGNAL

THE RIGHT TOOLS. THE RIGHT PARTNERS.

Data protection and data security are complex, complicated issues. There are numerous challenges and, not surprisingly, no one-size-fits-all solution.

However, there are many good data protection and data security tools out there. There are also companies that can partner with you to determine the right ones for building effective, well-rounded data protection and data security plans.

US Signal is one of them. While we favor cloud-based options because of the many benefits offered, we know that organizations in the healthcare sector often must deal with legacy IT systems and applications. By taking the time to understand your organization’s unique systems, needs, challenges, and plans, we can devise a hybrid solution that meets its specific needs.

Get insights into how US Signal can work with your specific needs. Read the customer story, “**Pine Rest Receives a Customized IT Infrastructure to House Its EHR System**.”

THE US SIGNAL STRATEGY FOR HEALTHCARE ORGANIZATIONS

US Signal understands the IT needs of the healthcare industry and offers strategies and solutions to meet even the most complex of them. Its industry experience, ability to customize IT solutions and its investment in HIPAA-compliant, audited IT infrastructure are among the factors that uniquely position it to help healthcare IT professionals manage and implement the technology that is transforming the healthcare industry.

US Signal is a leading data center provider, offering connectivity, cloud hosting, data protection, and disaster recovery services — all powered by its wholly owned and operated, robust fiber network. US Signal also helps customers optimize their IT resources through the provision of managed and professional services.

Contact US Signal at **866.274.4625** or **info@ussignal.com** and speak to a solution architect.

OUR COMPLIANCE

GDPR

HIPAA COMPLIANT

PCI

AICPA SOC

AICPA SOC 2

2020 CJIS READY

US SIGNAL®