ResolutionOne™ Platform

Cybersecurity Regulatory Brief

Healthcare

Accelerate your Information Security Improvement Initiatives

Understand the regulations that impact the financials services sector and streamline improvements in your information security program

AccessData®

OVERVIEW

The nature of data resident in the health care industry presents one of the most challenging information security landscapes when it to comes to achieving regulatory compliance and mitigating risks. Aside from just the sheer size of this industry (healthcare represents roughly 18% of US GDP today and will grow to nearly 20% of GDP by 2021), there are three important issues to consider in the context of managing healthcare and related organizations:

- The number of regulations focused on healthcare organizations, as well as the severity of failing to comply with them, are increasing.
- The number of organizations that must comply with healthcare-related laws is expanding and now encompasses organizations that formerly were never subject to them.
- The growing volume of healthcare-related information – and the sometimes-lax protection of this data – reveals an enormous need for improved cybersecurity protections.

KEY REGULATIONS TO CONSIDER

There are a variety of healthcare-related regulations with which a growing number of organizations must comply. Not only are hospitals, clinics and medical practitioners subject to these laws, but also are organizations as diverse as Certified Public Accounts, benefits administrators, attorneys and cloud-service providers.

HIPAA AND HITECH

The healthcare industry has faced a variety of regulations for many years. In 1996, the Health Insurance Portability and Accountability Act (HIPAA) went into effect, which included obligations for electronic records, communications and a number of other aspects of healthcare management. HIPAA is one of the most important issues faced by healthcare-related organizations because of its impacts on a wide variety of organizations, particularly as HIPAA was expanded in 2009, as discussed below.

HIPAA deals with a number of different focus areas, with one of its main objectives to reduce the administrative costs and burdens in the healthcare industry, as well as the costs of government reimbursement programs like Medicare. Congress included provisions in HIPAA that specify the use of standard electronic formats for transmission, as well as for the exchange and processing of data regarding healthcare transactions.

KEY REGULATIONS TO CONSIDER

The types of organizations are subject to HIPAA compliance has been expanded. As just one example, a cloud provider that is used for purposes of storing PHI is now considered a "Business Associate" and must adhere to a variety of HIPAA requirements.

Must receive "satisfactory assurances" from all of their Business Associates that PHI under their control is being protected.

Moreover, HIPAA establishes standard electronic data interchange (EDI) formats for transactions and records, such as medical claims and reimbursements, benefit enrollment forms and health plan premium payments. It also establishes standard code sets (to replace proprietary and ambiguous codes) for medical diagnoses and procedures as they are coded for claims and billing. HIPAA also established standards for the protection of patient privacy rights, including controls on how personal data (Protected Health Information, or PHI) is stored and access inside or outside of an organization.

The Health Information Technology for Economic and Clinical Health (HITECH) Act, followed by the HIPAA Omnibus Rule that became effective in late March 2013, significantly increased both the scope of HIPAA and the consequences for its violating it. Some of the key provisions of HITECH include:

- The definition of which types of organizations are subject to HIPAA compliance has been expanded. As just one example, a cloud provider that is used for purposes of storing PHI is now considered a "Business Associate" and must adhere to a variety of HIPAA requirements.

- Any subcontractor that "creates, receives, maintains or transmits PHI on behalf of a Business Associate, is a HIPAA Business Associate" and so must comply with the HIPAA Privacy Rule, Breach Notification Rule, Security Rule and other requirements. This would include CPAs, cloud providers, attorneys and any other entity that receives or manages PHI.

- The HIPAA Security Rule Section 164.306(c) has been clarified with respect to Covered Entities' and Business Associates' requirements to provide "reasonable and appropriate" protection of electronic PHI.

- Covered entities – i.e., those covered by HIPAA – must receive "satisfactory assurances" from all of their Business Associates that PHI under their control is being protected. Business Associates must also receive this from their subcontractors, creating a cascading impact of compliance obligations. A Covered Entity is any organization – such as a hospital, insurance company, clinic, clearinghouse, doctor's office, etc. – that handles either Personal Health Records (PHR) or PHI. The impact of HIPAA on Covered Entities is that they are required to follow all HIPAA and HITECH requirements for protecting this content from accidental disclosure and other violations.

KEY REGULATIONS TO CONSIDER

Omnibus rule allows HHS to impose fines ranging from $100 for an accidental, "Did Not Know" breach of PHI to $50,000 for a single, uncorrected and willful violation. Fines can reach $1.5 million per year or more.

Because the US Department of Health and Human Services (HHS) has expanded the requirements for protection of confidential and sensitive information and expanded the number of organizations that are subject to HIPAA, it can be expected to levy fines and penalties more frequently than it has in the past. For example, the Omnibus rule allows HHS to impose fines ranging from $100 for an accidental, "Did Not Know" breach of PHI to $50,000 for a single, uncorrected and willful violation. Fines can reach $1.5 million per year or more.

IMPORTANT ISSUES TO CONSIDER FOR HIPAA COMPLIANCE

The following rules and obligations are important to understand in the context of managing the impact of HIPAA compliance:

- HIPAA Security Rule [CFR Part 160 (a)(c), Part 164]
  HHS implemented the HIPAA Security Rule "to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity. The Security Rule requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information."

- HIPAA Privacy Rule [CFR Part 160(a)(e), Part 164]
  The Privacy Rule is a federal mandate designed to protect medical records and other sensitive information about individuals. Much of the focus of this rule is on the management and protection of information in electronic form.

- Business Associates
  A Business Associate is an organization like a benefits administrator, CPA or cloud provider with which a Covered Entity interacts in the context of sharing patient records or PHI. The HIPAA Privacy Rule allows a Covered Entity to share this information with a Business Associate as long as the latter can provide proper assurances that sensitive patient information will be protected, and that it will help the Covered Entity to maintain compliance with the Privacy Rule.

- Business Associate Agreements
  A Business Associate Agreement (BAA) is a contract between a Covered Entity and a Business Associate focused on protecting PHI. BAAs went into effect in February 2010 and obligate Business Associates to comply with the HIPPA Privacy and Security Rules for protection of PHI.

KEY REGULATIONS TO CONSIDER

A key component of a BAA is the process that the BAA will use to address and remediate a data breach, including data breaches that are caused by subcontractors used by the Business Associate.

RISKS AND COSTS

According to the Ponemon Institute's 2014 Cost of Data Breach Study, the average financial cost for each stolen record rose from $188 to $201, and the total average cost paid by an organization recovering from a breach rose from $5.4 to $5.9million. This is before HIPPA fines and penalties.

Covered entities and BAAs that fail to comply with the various healthcare-related obligations noted above can face a variety of consequences. For example, violations of HIPAA used to carry with them some serious penalties, but HITECH has significantly increased them and expanded the scope of the issues that IT and others need to address. For example:

- Before the implementation of HITECH, there was not an obligation to report data breaches other than those required under various state notification laws. Under HITECH, however, a public notification is required if a data breach results in the records of more than 500 individuals being exposed in an unauthorized manner. This notification consists of both informing HHS about the breach, as well as informing local media about the incident(s).

- Fines for data breaches under HIPAA could reach a maximum of $25,000 with a minimum penalty of $100 per violation. Under HITECH, however, each violation can be docked between $100 and $50,000, and yearly maximums can reach as high as $1.5 million.

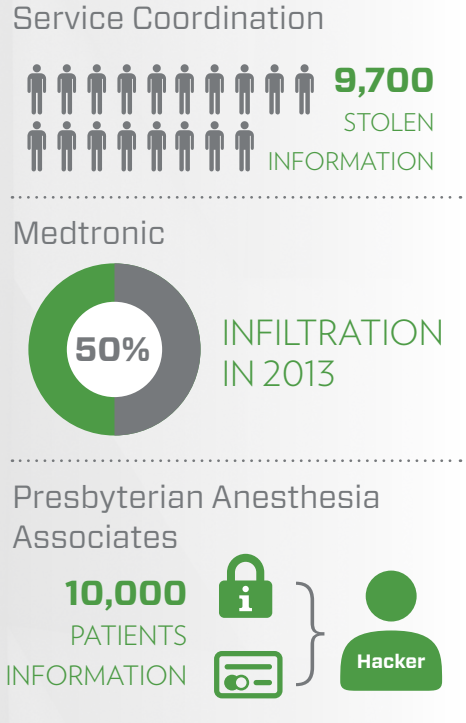
CYBERSECURITY IS A KEY ISSUE TO ADDRESS IN HEALTHCARE

Email remains a primary threat vector for cybercriminals focused on the healthcare industry. Email-based exploits can result from employees divulging login credentials as the result of a phishing attack, or it can result from a direct exploit from hackers through a firewall, an advanced persistent threat or malware. All of these threats are increasingly common and, because of the large number of susceptibility points in a healthcare network, there are likely to be even more serious exploits in the future.

The confidential and sensitive nature of healthcare data means that providers are often at major risk from things as simple as staff member browsing a web site. A data breach caused by a single piece of malware could put an entire healthcare network in danger and result in the loss of PHR or PHI, possibly resulting in major fines and negative publicity, not to mention negative impacts on patients. Given the size of the healthcare industry, there will be increasing attention paid to attacking healthcare organizations by hackers and other cybercriminals.

Beth Israel Deaconess Medical Center in Boston complained about running 664 pieces of medical equipment with old versions of Windows — however, manufacturers won't allow the software to be updated or even for antivirus software to be installed because of fears that modifying those devices would run afoul of FDA rules.

CYBERATTACKS IN THE HEALTHCARE INDUSTRY



THE UNIQUE ASPECT OF CYBERSECURITY IN HEALTHCARE

Every industry faces some level of risk from malware, advanced persistent threats, direct hacking and the like to their corporate networks, laptop computers, mobile devices and other computing platforms. However, the healthcare industry presents a unique cybersecurity problem because of the many non-traditional platforms that are targeted by cybercriminals.

For example, there is an enormous amount of computer-controlled medical equipment that presents a unique opportunity for cybercriminals. Because much of this equipment runs on older versions of Windows or other operating systems, and because regulatory considerations often prevent this equipment from being protected against threats easily or quickly, there is an enormous cybersecurity threat in healthcare that does not exist in other industries.

For example, in late 2012 there were 664 different pieces of medical hardware at Boston's Beth Israel Deaconess Hospital that ran on older versions of Windows – their respective vendors would not permit security or other upgrades to the equipment because of concerns about potentially violating FDA rules . Researchers have found that medical equipment as diverse as drug pumps, surgical robots and defibrillators can be remotely hacked . Unlike the case in virtually every other industry, cybersecurity failures in the healthcare industry can result in loss of life.

EXAMPLES OF CYBERATTACKS IN THE HEALTHCARE INDUSTRY

There have been numerous instances of cyberattacks in the healthcare industry, among which are:

- Kaiser Permanente reported in April 2014 that a malware infiltration had permitted unauthorized access to sensitive information for 5,100 patients involved in research studies.
- Service Coordination, a State of Maryland-licensed service provider for special needs individuals, was hacked and sensitive information on 9,700 clients was stolen in October 2013.
- During the first half of 2013, hackers infiltrated Medtronic's internal network for purposes that are as yet unknown. The company was not aware of the infiltration until US federal authorities informed them of the breach.

RISKS AND COSTS

- The credit card numbers, identities, contact information and other data for nearly 10,000 patients of Presbyterian Anesthesia Associates in Charlotte, NC were breached when a hacker exploited a security flaw on the company Web site.

- Lutheran Social Services of South Central Pennsylvania in York, PA was the victim of a malware infiltration that might have exposed sensitive data on 7,300 patients.

There are many other examples of HIPAA and HITECH violations that have resulted in significant penalties.

KEY BENEFITS

AccessData solutions can be used in the healthcare industry to conduct digital investigations and related types of processing, indexing, filtering and searching of critical data. Consequently, AccessData solutions can be useful in helping Covered Entities and their extended network of Business Associates to unearth potential violations before they rise to the level of an actual data breach.

HIPAA Violation	Minimum Penalty	Maximum Penalty
Individual did not know (and by exercising reasonable diligence would not have known) that he/she violated HIPAA	$100 per violation, with an annual maximum of $25,000 for repeat violations (Note: maximum that can be imposed by State Attorneys General regardless of the type of violation)	$50,000 per violation, with an annual maximum of $1.5 million
HIPAA violation due to reasonable cause and not due to willful neglect	$1,000 per violation, with an annual maximum of $100,000 for repeat violations	$50,000 per violation, with an annual maximum of $1.5 million
HIPAA violation due to willful neglect but violation is corrected within the required time period	$10,000 per violation, with an annual maximum of $250,000 for repeat violations	$50,000 per violation, with an annual maximum of $1.5 million
HIPAA violation is due to willful neglect and is not corrected	$50,000 per violation, with an annual maximum of $1.5 million	$50,000 per violation, with an annual maximum of $1.5 million

KEY BENEFITS

The problems associated with cybersecurity in the healthcare industry are being exacerbated by the growing number of ingress points for malware, hacking, advanced persistent threats and other potential infiltrations (including medical equipment); and the growing number of egress points for PHI and other sensitive data. The problem is made worse by the fact that many healthcare providers, such as hospitals and clinics, permit patients to gain access to corporate networks through "guest" Wi-Fi access, further increasing the potential of a cybersecurity attack. As a result, cybersecurity must become a top priority for any organization that manages healthcare-related information.

Addressing the threats caused by highly focused and highly skilled attackers, such as those that are responsible for sophisticated malware incursions, advanced persistent threats and similar types of sophisticated incursions, requires a very robust and integrated set of capabilities that many vendors do not offer.

HOW ACCESSDATA CAN HELP

The AccessData ResolutionOne™ platform and solutions portfolio can help healthcare-related organizations to understand how information flows within an organization and across its network of Business Associates. Their solutions can also detect potential cybercriminal activity quickly and remediate problems before content is stolen. For example:

- ResolutionOne can be useful in helping organizations to understand where unencrypted content is being sent in violation of HIPAA and HITECH requirements so that remediation can take place before violations become too large or too serious. The ability to detect data leaks is absolutely critical in the healthcare industry, since leaks of as few as 500 patient records can result in extraordinarily expensive consequences.

- ResolutionOne capabilities can identify suspicious binary files based on their unusual behavior even when there are no signatures that have been designed to detect previously identified malware. Suspicious code can be isolated and examined without the use of sandboxing, dynamic analysis or traditional heuristic analysis.

KEY BENEFITS

If malware, hacking or other cybercriminal activities are detected, AccessData's automated solutions can be used to identify suspicious binaries quickly, analyze them, and conduct remediation activities (e.g., reimaging affected machines, or isolate the endpoints) much more quickly than if manual processes were used. This permits infected machines to be brought back online much more quickly.

- ResolutionOne can help owners of PHI and PHR to understand who has access to what content, how long they are storing it, where they are storing it, and whether or not they even need to be in possession of it.

- ResolutionOne can be used to identify the most vulnerable parts of an extended healthcare network so that the most serious potential violations can be addressed with the highest priority.

- Finally, the AccessData solutions portfolio can help healthcare organizations to conduct the forensic examination necessary to determine how and why breaches occurred, and what can be done to prevent them in the future.

The ResolutionOne platform features Continuous Automated Incident Resolution (CAIR™) which provides key benefits for those charged with protecting healthcare organizations and others in the extended network that manage healthcare data and systems:

AccessData solutions automate the process of malware triage and identifies, isolates and remediates cyberattacks, malware incursions and other threats more efficiently than contemporary manual processes. The ResolutionOne platform features Continuous Automated Incident Resolution (CAIR™) which provides key benefits for those charged with protecting healthcare organizations and others in the extended network that manage healthcare data and systems:

- CAIR integrates analysis of endpoints, networks and malware into a single tool that employs a centralized database. This allows security teams to rely less on signature-based tools and other solutions that do an inadequate job at detecting zero-day and other sophisticated threats, and to eliminate the "noise" of excessive alert information.

- The result of this integration and comprehensive toolset enables all relevant parties to a security investigation – compliance, legal and security – to work together on a single platform.

KEY BENEFITS

Faster detection and remediation because of this collaborative capability can bring critical systems back online more quickly, limiting system downtime and the potential data loss – and potentially prevent loss of life – that can occur.

- Members from various groups addressing security breaches or other problems have access to the same data presented on one platform, permitting them to automate a variety of tasks and to collaborate in real time, thus speeding the time to resolving the problem and minimizing the impact of security incidents.

- Faster detection and remediation because of this collaborative capability can bring critical systems back online more quickly, limiting system downtime and the potential data loss – and potentially prevent loss of life – that can occur.

BENEFITS TO HEALTHCARE ORGANIZATIONS

In addition to the technical benefits offered by ResolutionOne, its integration of multiple capabilities and integration with existing security investments into a single, collaborative platform permits healthcare organizations to eliminate the use of separate point solutions, eliminating much of the complexity and delay that plagues most security infrastructures. This not only permits better performance, but lower cost and easier management of a healthcare organization's security capabilities. The savings can be dramatic because the costs associated with procuring and configuring multiple solutions, training staff members on various platforms, and managing several vendor relationships is significantly reduced.

Moreover, CAIR allows organizations to optimize their use of Security Information and Event Management (SIEM) tools, next-generation firewalls, alerting tools, monitoring solutions and the like by integrating their output with threat intelligence feeds to provide more robust protection. The result is the ability for security teams to have available to them more threat data and the ability to respond to incidents more quickly.

FOR MORE INFORMATION

For more information about AccessData, please visit
http://www.accessdata.com/resolutionone-platform

CONTACT US

Sales@accessdata.com
US: 801.377.5410
International: +44.0207.010.7800