Healthcare

Cybersecurity Regulatory Brief

Understand the regulations that impact the healthcare industry and accelerate information security initiatives.

AccessData®

Contents

Overview

The nature of data resident in the healthcare industry presents one of the most challenging information security landscapes when it comes to achieving regulatory compliance and mitigating risks. Aside from the sheer size of this industry (healthcare represents roughly 18% of US GDP today and will grow to nearly 20% of GDP by 2021[1]), there are three important issues to consider:

- The number of regulations focused on information security are on the rise, as well as the penalties for failing to comply.
- The number of organizations that must comply with healthcare-related laws is expanding and now includes 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.

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 organizations as diverse as Certified Public Accountants, Benefits Administrators, Attorneys and Cloud-service Providers.

The number of regulations focused on information security are on the rise, as well as the penalties for failing to comply.

HIPAA and HITECH

The healthcare industry is not new to regulations. 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 impact 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 the transmission, exchange and processing of data relating to healthcare transactions.

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

The types of organizations subject to HIPAA compliance have risen dramatically. For 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.

1. Executive Office of The President Council Of Economic Advisers. *The Economic Case for Health Care Reform*, June 2012.

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 accessed 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 March 2013, significantly increased both the scope of HIPAA and the consequences for violating it.

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.

HIPAA covered entities must receive "satisfactory assurances" from all of their Business Associates that PHI under their control is being protected.

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"

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.

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 individuals' medical records and other sensitive information.

Business Associates
A Business Associate is an organization such as 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.

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

A key component of a Business Associate Agreement 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.

Fines and Other Consequences

Covered Entities and BAAs that fail to comply with the various healthcare-related obligations noted above can face a variety of consequences. For example, HIPAA violations traditionally carried

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.

serious penalties, the addition of HITECH has significantly increased those and expanded the scope of the issues IT and other must 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, each violation can result in fines ranging from $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 (the APT) or malware. All of these threats are increasingly common and, because of the large number of susceptible 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 put at major risk from things as simple as staff members 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 impact to patients. Given the size of the healthcare industry, there will be increasing attention paid to attacking healthcare organizations by hackers and other cybercriminals.

The Unique Aspect of Cybersecurity in Healthcare

Every industry faces some level of risk from malware, replace advanced persistent threats with the APT, direct hacking to their corporate networks, laptop computers, mobile devices and other computing platforms. However, the healthcare industry presents a unique cybersecurity problem due to 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 a significant cybersecurity threat in healthcare that does not exist in other industries.

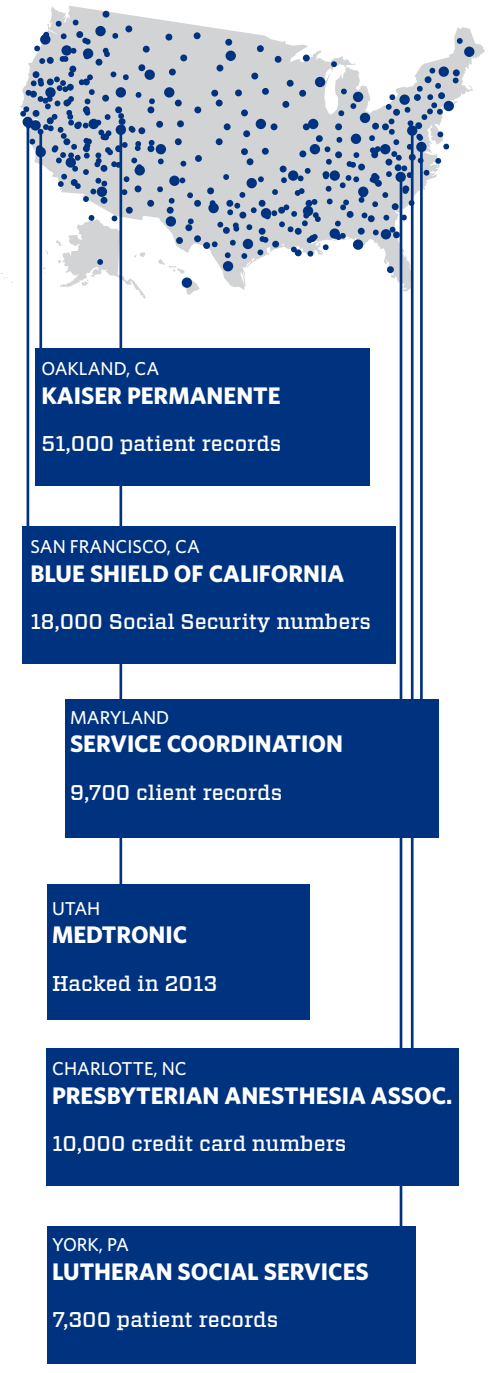
For example, in late 2012 there were 664 different pieces of medical hardware at Boston's Beth Israel Deaconess Hospital that ran on older versions of Windows—their respective vendors would not permit security or other upgrades to the equipment because of concerns about potentially violating FDA rules. Researchers found that medical equipment as diverse as drug pumps, surgical robots and defibrillators can be remotely hacked. And unlike other industries, 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 resulting in loss of sensitive data, including:

- 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.
- In July of 2014 Blue Shield of California and the state Department of Managed Health Care reports the Social Security numbers of about 18,000 California physicians were accidentally released with other data. The incident occurred after Blue Shield of California included doctors' Social Security numbers in required monthly filings to the state Department of Managed Health Care. The filings also included doctors':
    - Business addresses
    - Business phone numbers
    - Medical group names
    - Names
    - Practice areas
- 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.

Cyberattacks in the Healthcare Industry



- 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 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.

Statutory Fines for HIPAA Violations

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 Attorney 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

How AccessData Can Help

AccessData's ResolutionOne™ Platform integrates network, endpoint and malware analysis, threat intelligence, large-scale data auditing and remediation capabilities into a single solution that doesn't just deliver rapid detection and response; it delivers Continuous Automated Incident Resolution.

ResolutionOne enables your organization to:

- Immediately identify when a sensitive data leak is occurring so you can quickly resolve the issue.

- Fully integrate with existing security infrastructure—such as SIEMs, next-generation firewalls, alerting tools, monitoring solutions—to reduce the time it takes to identify critical security incidents and get the most out of your existing investments.
- Automate manual processes to free up valuable resources and focus on more business critical tasks.
- Cull through the noise in order to quickly confirm and prioritize true threats.

Benefits to Healthcare Organizations

In addition to the incident resolution benefits offered by ResolutionOne, its integration of 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 security teams have more threat data available to them and the ability to respond to incidents more quickly.

Problems with cybersecurity in the healthcare industry are exacerbated by the growing number of ingress points for malware, hacking, advanced persistent threats and other potential infiltrations; and the growing number of egress points for PHI and other sensitive data.

ResolutionOne Platform

The ResolutionOne™ Platform from AccessData, as well as AccessData's solutions portfolio, can help healthcare-related organizations to understand how information flows within an organization and across its network of Business Associates.

Automate the process of malware triage. Identify, isolate and remediate cyberattacks, malware incursions and other threats more efficiently than contemporary manual processes with the ResolutionOne Platform.

Healthcare

Cybersecurity Regulatory Brief

Accelerate Information Security Initiatives

Learn more about how AccessData can help accelerate information security initiatives at http://accessdata.com

AccessData Group makes the world's most advanced and intuitive incident resolution solutions. AccessData technology delivers real-time insight, analysis, response and resolution of data incidents, including cyber threats, insider threats, mobile and BYOD risk, GRC (Governance Risk and Compliance) and eDiscovery events. Over 130,000 users in law enforcement, government agencies, corporations and law firms around the world rely on AccessData software to protect them against the risks present in today's environment of continuous compromise.

AccessData®

GLOBAL HEADQUARTERS
+1 801 377 5410
1100 Alma Street
Menlo Park, CA 94025
USA

NORTH AMERICAN SALES
+1 800 574 5199
Fax: +1 801 765 4370
sales@accessdata.com

INTERNATIONAL SALES
+44 20 7010 7800