solarwinds

SIMPLIFYING HIPAA COMPLIANCE FOR IT PROFESSIONALS

SOLARWINDS
WHITEPAPER

SIMPLIFYING HIPAA COMPLIANCE FOR IT PROFESSIONALS

All modern healthcare organizations rely on information technology. From sophisticated purpose-built surgical equipment to the back-office billing, IT keeps the healthcare provider running. So why should an IT or security professional care about compliance? The answer is that a well-designed compliance program can improve overall IT and security efficiency while saving time and energy otherwise spent remediating audit failures/gaps. Electronic records are a cornerstone of modern healthcare delivery, and IT and security professionals need to be aware of how those records are managed and secured. This paper provides information about the Health Insurance Portability and Accountability Act (HIPAA) and offers guidance on how to work with an existing program or how to start your own.

A BRIEF BACKGROUND

WHAT IS HIPAA?

If you are not a full-time compliance professional based in the United States, you may not know that HIPAA began as legislation in 1996. Originally drafted to solve problems related to health information portability, privacy, security, and fraud, HIPAA is now entering its twentieth year. The benefits of health information portability include not only efficiency, but also truly life-saving practices. In 1999, for example, the estimated number of accidental, but preventable, deaths due to medical errors was 98,000[1]. Improving the way health information was exchanged, including Electronic Health Records (EHR), was thought to reduce the risk of these errors.

Despite that fact, it took a while for EHR to gain adoption. An additional law, the Health Information Technology for Economic and Clinical Health Act (HITECH Ac[2]), which was passed in February 2009, was needed first. With HITECH came the characterization of “meaningful use” for electronic health information that defined specific health and safety improvement goals to be achieved by the use of electronic records. HITECH created economic incentives that prompted healthcare providers to move to electronic records. Between 2009 and 2012, EHR adoption rates doubled[3].

[1] https://iom.nationalacademies.org/~/media/Files/Report%20Files/1999/To-Err-is-Human/To%20 Err%20is%20Human%201999%20%20report%20brief.pdf

[2] Health Information Technology for Economic and Clinical Health

[3] http://www.hhs.gov/asl/testify/2013/07/t20130717b.html

HIPAA SECURITY RULE

The first Security Rule (SR) was promulgated under HIPAA in February 2003. The final HITECH Security Rule was not promulgated until ten years later. Under HIPAA, information security is to provide protection of the privacy of electronic records at rest and in transit based on the principles of "comprehensiveness, scalability, and technology neutrality."

PRIVACY RULE

The other record-handling guidance within HIPAA is the Privacy Rule. Under the Privacy Rule, organizations are instructed to apply the "appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." The Privacy Rule is also where you find the data breach notification obligations, which are:

1. Any entity must notify any individual whose protected health information (PHI) has been disclosed in an unauthorized way.
2. If the breach consists of more than 500 residents within a single state, "prominent media" outlets must be notified.
3. If 10 or more individuals have out-of-date contact information, a notice must be placed conspicuously on the entity's website.
4. The Secretary of the U.S. Department of Health and Human Services (HHS) must be notified immediately in the case of breaches that involve 500 people or more. If a breach affects fewer than 500 individuals annually, the Secretary must be notified within 60 days of the end of the calendar year in which the breach was discovered[4].

These rules are designed to work together, however the Privacy Rule applies to both physical and electronic records, whereas the Security Rule only applies to electronic records.

[4] http://www.hipaasurvivalguide.com/hitech-act-13402.php

GETTING STARTED WITH HIPAA/HITECH

STEP 1: ARE YOU A COVERED ENTITY OR A BUSINESS ASSOCIATE?

If you work for a covered entity, you probably know it. If you are a business associate, or a subcontractor to a business associate, you may not know you are subject to the Security and Privacy Rules. But the inquiry is simple. Do you ever view, analyze, handle, transfer, store, forward, or transform any health data that has not been de-identified? If yes, read on.

HIPAA specifies two types of entities: Covered Entities (CEs) and Business Associates (BAs). Originally, HIPAA Security and Privacy rules only directly applied to CEs. Per the legislative definitions, CEs are (1) a healthcare provider, like a doctor, pharmacist, or clinic; (2) a healthcare plan, like an insurance company or Medicare; or (3) a healthcare-clearing house, such as a billing company. Organizations that work with CEs on protected health information are considered business associates. BAs are other entities in the health care ecosystem that support CEs and need access to protected data. Examples of BAs include 3rd-party administrators, ancillary support services, such as CPAs and attorneys, and SaaS providers, that process or transit protected health information. For example, Dropbox, if it is being used to share X-ray images, is a BA. BAs are brought under the Security and Privacy Rule through Business Associate Agreements (BAAs). CEs are responsible for the BAAs as CEs are required to obtain “reasonable assurances” that BAs will safeguard the privacy and security of health information they process.

The rules applying to CEs and BAs have changed a bit over time, but the Net/Net is since the final rules have been passed, if you are in IT or IT security and have anything to do with electronic health records, you probably need to follow the Security and Privacy Rules. If you don’t, you are subject to penalties delivered by the Office for Civil Rights (OCR).[5]

[5] Summary of final rule changes:

1. Expanded the definition of BAs to include subcontractors
2. Apllied the Security Rule and most of the Privacy Rule directly to BAs
3. Created direct liability for BAs to the office of Civil Rights (“OCR”). FYI the OCR has the statutory authority to investigate and assess civil penalties for violations of the Security and Privacy rules.
4. Clarified that CEs can be held liable for BA violations under an agency legal doctrine.

STEP 2: WHO HAS ACCESS, AND WHERE IS EPHI ANALYZED OR STORED?

It is important to train and manage electronic protected health information (ePHI) access. The core of the Privacy Rule goes to who is accessing data and when. This can be quite challenging because of the many different roles and authorizations needed to effectively manage healthcare data and provide services. Basic security involves confidentiality, integrity, and availability. In most businesses, one of these three will be the most important, but in healthcare, depending on the activity, the priority changes. For example, in the emergency room, availability is the most important, in keeping with the so-called "break the glass" rule. In pharmacy or testing data transfer, integrity is most important, largely due to the potential for harmful drug interactions. Finally, in data at rest, confidentiality is the most important, as the Anthem[6] and Community Health breaches taught us. So, as an IT or security professional, you have to adapt your controls to each different data use case.

TIP: You have to start with a data inventory. To build your access use cases, even if this is just a spreadsheet, you need to start with a list. If your IT colleagues are not sure, finance usually has a list of all the application software the company uses.

Privacy notices and violations

Privacy notices must provide information about where to file a complaint, and in healthcare, we see a high rate of complaints. At the end of 2015, the OCR had received over 125,000 complaints since the department started receiving complaints in 2003[7]. The OCR most common violations of the Privacy Rule include the following:

1. Impermissible uses and disclosures of protected health information.
2. Lack of safeguards of protected health information.
3. Lack of patient access to their protected health information.
4. Lack of administrative safeguards of electronic protected health information.
5. Use or disclosure of more than the minimum necessary uses or disclosures of protected health information.[8]

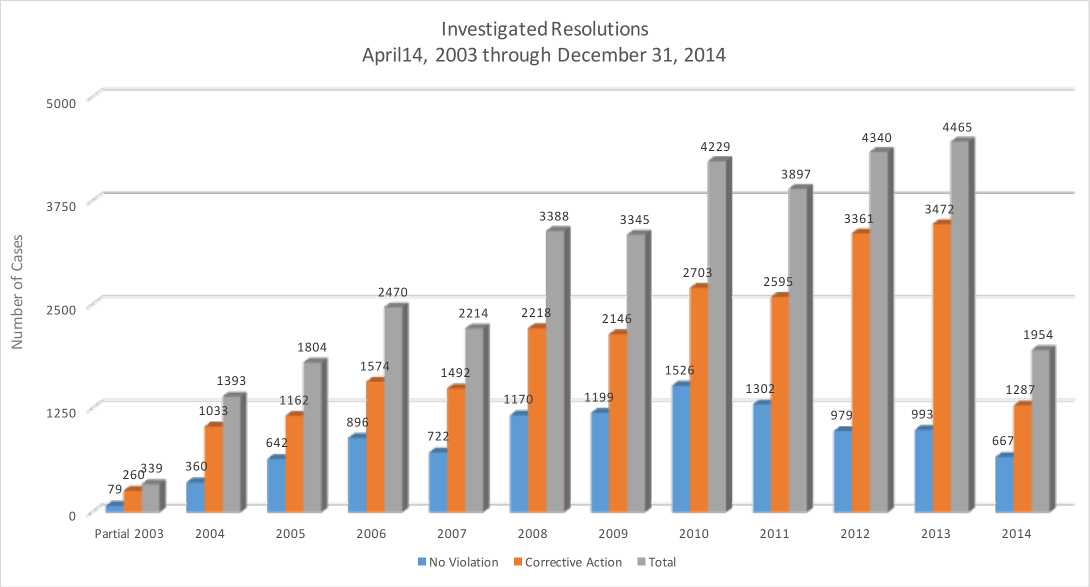
TIP: You can use the above list of common privacy violations to prioritize your control implementations.

[6] http://money.cnn.com/2015/02/04/technology/anthem-insurance-hack-data-security/

[7] http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/numbers-glance/index.html

[8] http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/enforcement-highlights/index.html

The chart below summarizes the findings from investigated complaints (~35,000) for the period 2003-2014. You can see the spike in corrective action after the final Security Rule was released. While monetary penalties are not high in HIPAA violations (3-4 million dollars is a big fine), investigations that disrupt business and potential corrective actions can be much more costly than maintaining a proper program from the beginning.



STEP 3: WHAT ARE YOUR CRITICAL CONTROLS?

The critical controls you need to understand and implement are:

Identity Access Management - This is the cornerstone for authorization for both physical and electronic data access. Temporary authorization for both visiting doctors and interim staffing create some of the biggest challenges in this area.

Encryption (at rest and in transit) – This is essential to mitigating the risk of data breaches, but it's difficult to find a single solution that meets all encryption needs. Be sure and negotiate for best of breed for each use case from your vendors.

Automated Logging and Monitoring – This is your go-to platform for (i) assurance (Is everything operating within expected norms?), (ii) risk management (Have we seen unusual activity?), and (iii) forensics (Where did this unauthorized access originate?). Logging and monitoring needs to be connected to all critical systems (physical access is often overlooked), and data-at-rest sources.

Reliable, Accessible Backups – One of the worst scenarios in IT is to have a catastrophic failure and then discover your backups haven't been running for the last however many weeks. Backup success or failure needs to be integrated with logging and monitoring. Also, even if your backups are running, that doesn't mean you can effectively restore. Work with your disaster recovery, emergency planning, or business continuity team and randomly test your backups.

Also, keep in mind that seemingly unrelated IT changes can impact compliance. For example, if you move from an on-prem calendaring system to a cloud-based system (such as Google®), the access models of these new cloud-based systems may not easily fit into your security policies. See the Phoenix Cardiac Surgery case, in which the healthcare provider was fined for using a publicly accessible Internet calendar for patient appointments.[9] The ability to share outside the organization in cloud-based storage solutions (accidentally sharing a box folder, for example), may cause a data breach.

Balancing flexibility and ease of access to improve information-sharing between CEs and BAs while understanding the associated risks is a critical responsibility shared among IT, security and risk management teams.

TIP: Take your counterpart in risk, security, or IT to lunch and have a frank conversation at least once a quarter.

STEP 4: MANAGING THREATS

Every IT and security professional knows that threats are constantly changing, and when patterns emerge, the damage is already done. 2014 was the year of the big health information data breach (Anthem, Community Health Systems)[10]. 2016 looks to be the year of ransomware. Hospitals in California, Kentucky, Canada, and Germany have been hit so far. Unfortunately, there is no advance alerting system for what the latest malicious attack mechanism will be. Often your best options are the basics:

- Maintain patches.
- Manage change.
- Monitor everything.
- Backup, backup, backup.

[9] http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/examples/phoenix-cardiac-surgery/index.html

[10] http://www.modernhealthcare.com/article/20150210/BLOG/302109995

Keep a risk register, even if it is just a spreadsheet. Or try Simple Risk (https://www.simplerisk.it/), and work on just the top three. OCR also offers a free Security Risk Assessment tool for Windows® or iOS. You can find out more here: https://www.healthit.gov/providers-professionals/security-risk-assessment-tool

Understand when to say no to a vendor, program, or manager. Security is full of great new solutions, but you need to be assured that your organization can be effective with any given solution. You also need to make sure it can solve at least one of your top three challenges. (For example, see our take on threat intelligence at: http://resources.solarwinds.com/is-threat-intelligence-for-me/).

STEP 5: HAVE AN INCIDENT MANAGEMENT PLAN

Does everyone in your organization know who to call if they suspect a breach or identify a risk? Your plan doesn't have to be a sophisticated software platform that can discover, gather, identify, prepare, and disclose breaches or incidents, but everyone in the organization needs to know who to call first and second. And those first and second individuals need to be able to triage, notify appropriate management, and apply computer first aid.

Without a plan, you will spend precious time just trying to identify who needs to be involved with the incident. Then the email chains spin out of control, potentially leading to premature disclosure and unwanted media attention.

There are many other aspects to HIPAA that IT and security professionals will encounter, including records management, risk assessment, policy, breach notification, and training requirements. While these are outside the scope of this paper, you can find more information at www.healthit.gov.

SOLARWINDS LOG & EVENT MANAGER

SolarWinds® Log & Event Manager is an affordable, award-winning SIEM solution that produces out-of-the-box compliance reports for HIPAA. Log & Event Manager can be installed in minutes and easily generates compliance reports quickly using audit-proven templates.

NEXT STEPS

1. Watch these two HPAA compliance videos:

Improve Healthcare Security and HIPAA Compliance: Part 1
Improve Healthcare Security and HIPAA Compliance: Part 2

This two-part series covers the HIPAA/HITECH regulatory evolution, and goes through some practical tips that cost-sensitive healthcare organizations can take to move toward effective risk management.

2. Try SolarWinds Log & Event Manager for yourself. Download a free 30-day trial and have it up and running in about an hour.

Log & Event Manager is the fastest and easiest way to HIPAA compliance reporting.

ABOUT SOLARWINDS

SolarWinds provides powerful and affordable hybrid IT infrastructure management software to customers worldwide, including Fortune 500® enterprises, small businesses, government agencies, and educational institutions. We are committed to focusing exclusively on IT pros, and strive to eliminate the complexity that they have been forced to accept from traditional enterprise software vendors. Regardless of where the IT asset or end-user sits, SolarWinds delivers products that are easy to find, buy, use, maintain, and scale, while providing the power to address all key areas of the infrastructure from on-premises to the cloud. Our solutions are rooted in our deep connection to our user base, which interacts in our thwack® online community to solve problems, share technology and best practices, and directly participate in our product development process. Learn more today at http://www.SolarWinds.com/.