Compliance Solutions

Staying on Top of Escalating HIPAA Challenges

WHITE PAPER

We protect what matters.

Stericycle®

Table of Contents

Introduction

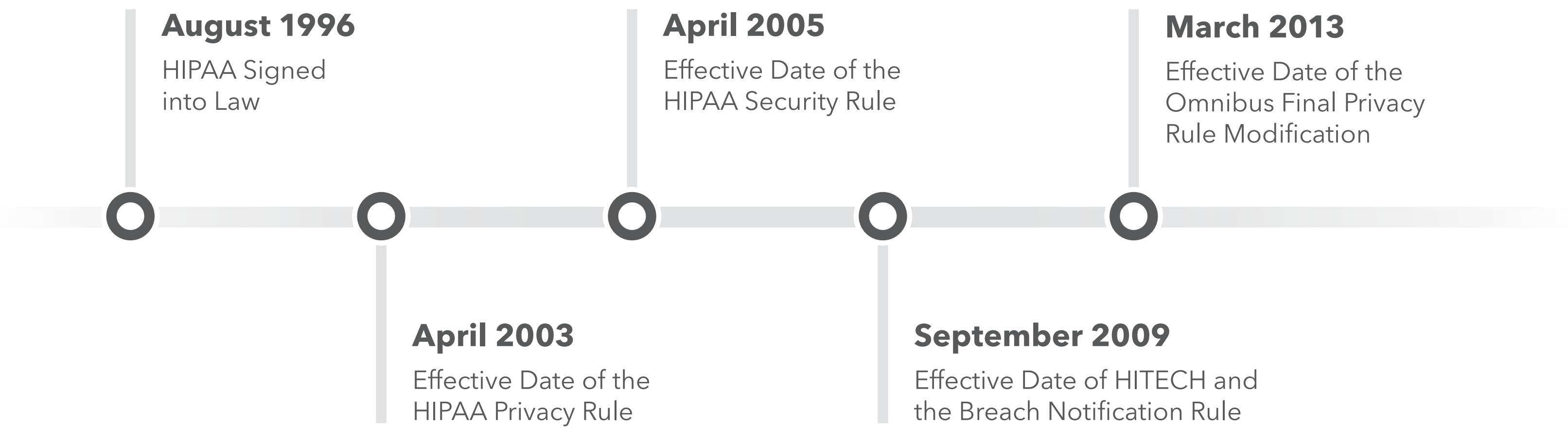
HIPAA Enforcement Adapts as Health IT Evolves

When the Health Insurance Portability and Accountability Act (HIPAA) was signed into law on August 21, 1996, computerized information technology had already been on a continual rise for over 20 years with the birth of the digital revolution, followed by the internet. HIPAA was as much a response to IT innovations as it was an encouragement of more ingenuity and expansion of health information technology (health IT). The U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) responded, "Widespread use of health IT within the health care industry will improve the quality of health care, prevent medical errors, reduce health care costs, increase administrative efficiencies, decrease paperwork, and expand access to affordable health care."

All true, but HIPAA has also unintentionally created regulatory and financial challenges for many health care organizations. 2018 had a significant amount of data threats and breaches signaling the continued importance of safeguarding electronic protected health information (ePHI) but more accurately and as we'll explore, all forms of protected health information (PHI).

- Anthem Blue Cross Blue Shield agreed to pay $16 million to the OCR for its 2015 breach—the largest health data breach and settlement in history. Cyberattacks gathered the PHI of over 79 million people.[1]
- Twelve states filed the first ever multistate data breach lawsuit against several health IT companies and their subsidiaries. The district attorneys of each state alleged that poor security practices led to PHI theft of 3.9 million patients.[2]
- Researchers found that PHI data breaches from 2009 through 2017 were more likely caused by internal error, not by external triggers like cyber-attacks.[3]
- Studies found that "paper and films were the most frequent location of breached data, occurring in 65 hospitals during the study period, whereas network servers were the least common location but their breaches affected the most patients overall."[4]
- The National Telecommunications and Information Administration (NTIA) issued a request for comment "on ways to advance consumer privacy while protecting prosperity and innovation." The request for comment garnered over 200 submissions, of which many expressed the challenges of fostering invaluable medical and IT advancements while also protecting PHI.

HIPAA Regulatory Timeline



August 1996
HIPAA Signed into Law

April 2003
Effective Date of the HIPAA Privacy Rule

April 2005
Effective Date of the HIPAA Security Rule

September 2009
Effective Date of HITECH and the Breach Notification Rule

March 2013
Effective Date of the Omnibus Final Privacy Rule Modification

Risks and Compliance Challenges

For health care organizations, a PHI breach can result in a multiplex financial and public relations catastrophe. Whether by internal negligence or external nefarious means, impermissible use or disclosure of PHI that is not properly secured and managed with an eye towards privacy could result in adversely impacting patients, civil suits and regulatory penalties ranging from 100 to 1.5 million dollars per violation category for every year the violation was allowed to persist.[5] All this, of course, creates a loss of trust from the provider's community and various stakeholders.

The threat and challenge of risk assessment is compounded by a level of ambiguity in HIPAA's design: "Given that the health care marketplace is diverse, the Security Rule is designed to be flexible and scalable so a covered entity can implement policies, procedures, and technologies that are appropriate for the entity's size, organizational structure, and risks to consumers' ePHI."[6] In response to the above-mentioned request for comment from the NTIA, the American Medical Informatics Association pointed out even more challenges in navigating HIPAA regulations. They wrote, "We note that the feared 'patchwork' of different state policies, is the reality for health care data. This issue has become more pronounced in the era of digital health records, creating challenges to information exchange, complicating compliance, and generating perverse outcomes based on variable interpretation."[7]

Health care workers will often find themselves moving from one patient to the next, using numerous computer stations and other electronic devices along the way, and throughout this route, incorporating various cloud-based devices in patient care. Hackers are finding ways to begin cyber-attacks on hospital networks by entering through error messages in medical devices including X-ray and other imaging systems.[8]

A recent survey shows that cyber and PHI related threats are among health care leaders' top 5 concerns in 2019.[9]

The Potential for Security Breaches Expands

Cyber threats and the difficulties of protecting ePHI is substantial. On top of that, a study in the American Journal of Managed Care found that electronic locations, such as servers and email breaches, usually expose the largest number of patients' ePHI, however hard copy paper and films were the most frequent location of breached PHI. Additional studies released in 2018 found that most PHI breaches are committed by insiders.[10]

Under HIPAA & HITECH regulations, all breaches affecting more than 500 individuals require the health care provider and/or covered entities (provider's business associates, vendors, etc.) to give notice to the affected individuals and the HHS. In addition, if the breach affects more than 500 residents of a single state or smaller jurisdiction, then media must also be informed.

In 2018, over 400 cases were under investigation by the OCR due to breaches of unsecured PHI affecting more than 500 people. The health care providers under investigation ranged from numerous small-town single-physician practices and other small medical businesses to the largest of health care conglomerates. In cases of email phishing of company accounts or the theft of employee devices, patients are not the only victims. Health care leaders/owners also bear the burden of having their businesses compromised. In other cases, it may have been blatant criminal activity of employees or business associates of the providers under investigation. In all cases, safeguards should have been in place to prevent PHI breaches.

Regardless, if you are a health care leader of a nationwide hospital or a private owner of a small local clinic, the thought of a security breach might be alarming. The potential data-breach locations widen as we consider how hardcopy PHI has proven to remain vulnerable, combined with an ever-increasing speed of innovation and aptly named, disruptive technologies that enhance patient care but often bring additional vulnerabilities to PHI. Health care organizations of all sizes are at risk of not staying compliant with HIPAA regulations, as well as being subject to overwhelming financial restitution and damage to their reputation.

Strategies for Improving Compliance

Creating a comprehensive HIPAA compliance program for your facility means developing a compliance strategy that includes a solid and broad-reaching security and privacy-compliant framework, with the flexibility to accommodate your business's growth, embrace expansion of new technology and, as much as possible, support your employee's patient care.

Wrap Your Head Around the Problem

First, you need to closely examine and document the multiple ways your organization's PHI is currently and may potentially be shared internally and externally. Become aware of how these exchanges happen through inbound and outbound routes, and how secure they may be. How and for what purposes is the information shared? Best practice is to develop a table or chart to organize and manage your findings for analysis and to prepare for training your organization, a HIPAA requirement. Your risk management practices should include reviewing all points of contact, types of data sharing and purpose of the relationships. The more detailed the assessment the more likely you are to uncover all the gaps within your ePHI and overall PHI security and privacy.

The various entities connected to your operations, who may have even the most limited accessibility to PHI, need to be accounted for and bound by Business Associate Agreements (BAA). All Business Associates commit in the BAA to have their staff that accesses or can be exposed to PHI to be fully trained and have their own fully developed privacy and security compliance programs. Business associates may include consultants, accountants, data analysts, external coders, etc.

Consider what the Centers for Medicare & Medicaid Services (CMS) indicate as common elements of violations:[11]

- Impermissible PHI use and disclosure
- Use or disclosure of more than the minimum necessary PHI
- Lack of PHI safeguards
- Lack of administrative, technical, or physical ePHI safeguards
- Lack of individuals' access to their PHI

Once you acknowledge where your security and privacy needs improvement, you'll need to create a system that is not just HIPAA compliant but, with all due respect to your personnel, it needs to be as foolproof as possible. Organizations of all sizes should have administrative, physical and technical controls in place. In addition to making sure employees are properly trained, administrators should be sure that:

- All patients receive Notice of Privacy Practices
- Investigation processes, resulting action plans and breach risk assessments are in place in case a potential breach must be analyzed for breach determination
- All business associate agreements are HIPAA compliant
- Periodic assessments of your HIPAA compliance, both privacy and security are scheduled and conducted

Have a Plan for Breach Notification

Despite the best controls, organizations may experience a breach and they should have robust policies in place that address how they will notify affected parties. The action plans should also address the roles of what business associates need to do in the event of a breach, which also is delineated in the BAA, including the required timeframe to notify the covered entities.[12]

Incorporate HIPAA Compliance into an Overarching Strategy

HIPAA compliance should be a part of a larger effort to improve organization-wide compliance. While there are many similarities between the requirements of different regulatory bodies—such as the HHS, Occupational Safety and Health Administration (OSHA) and the Environmental Protection Agency (EPA)—there are areas that are unique to each set of standards. For example, each regulatory body may require policies and procedures, performance audits and staff education and training, but the nuances within those requirements may differ. To see where HIPAA compliance fits, and how it diverges, organizations may want to develop a chart that can highlight the commonalities and variations. You can use this chart to help with planning and resource allocation, as well as when selecting outside compliance vendors.

Stay Prepared

Even though HIPAA legislation is not new, organizations should be revisiting their compliance programs to make sure they are up to date. By examining current communications, assessing risk, and incorporating HIPAA compliance into a global strategy, organizations can proceed along the path to comprehensive compliance, as well as be ready as possible to accommodate new technologies, regulatory updates and your business's growth.

Visit **stericycle.com/hipaa** to learn how Stericycle can help your organization develop a comprehensive HIPAA compliance program.

Sources

1. U.S. Department of Health and Human Services, News, https://www.hhs.gov/about/news/2018/10/15/anthem-pays-ocr-16-million-record-hipaa-settlement-following-largest-health-data-breach-history.html, accessed 1/28/19.

2. Health IT Security, HIPAA and Compliance News, https://healthitsecurity.com/news/12-states-sue-business-associate-for-2015-health-data-breach, accessed 1/28/19.

3. Becker's Healthcare, Hospital Review, https://www.beckershospitalreview.com/cybersecurity/internal-errors-more-likely-to-cause-healthcare-breaches-than-outside-threats.html, accessed 1/28/19.

4. The American Journal of Managed Care, Journals, https://www.ajmc.com/journals/issue/2018/2018-vol24-n2/data-breach-locations-types-and-associated-characteristics-among-us-hospitals, accessed 2/28/19.

5. U.S. Department of Health and Human Services, HIPAA for Professionals, https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html, accessed 1/28/19.

6. U.S. Department of Health and Human Services, HIPAA for Professionals, https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html, accessed 1/28/19.

7. National Telecommunications and Information Administration, Publications 2018, https://www.ntia.doc.gov/files/ntia/publications/amia_response_to_ntia_rfi_on_data_privacy_outcomes_and_goals_vfinal.pdf, accessed 1/28/19.

8. Zingbox, Press Releases, https://www.zingbox.com/press-releases/zingbox-identifies-cyber-attack-trend-press-release/, accessed 1/28/29.

9. Proviti, Insights, https://www.protiviti.com/US-en/insights/top-risks-2019-healthcare, accessed 1/28/19.

10. JAMA Network, Journals, https://jamanetwork.com/journals/jamainternalmedicine/article-abstract/2715158, accessed 1/28/19.

11. Centers for Medicare & Medicaid Services, Outreach & Education, https://www.cms.gov/Outreach-and-Education/Medicare-Learning-Network-MLN/MLNProducts/Downloads/HIPAAPrivacyandSecurityTextOnly.pdf, accessed 1/28/19.

12. U.S. Department of Health and Human Services, HIPAA for Professionals, https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html, accessed 1/28/19.

stericycle.com

♻ Printed on post-consumer recycled paper.

Stericycle®