HIPAA Compliance Without The Headache

UpGuard

Table of Contents

Introduction

Ever since being signed into law by President Bill Clinton in 1996, the Health Insurance Portability and Accountability Act (HIPAA) has been a constant source of compliance confusion and difficulty for healthcare organizations and insurance providers. Primarily designed to help protect individuals and patients against loss, theft, or disclosure of sensitive medical information by healthcare providers and insurance providers, HIPAA has been widely criticized for stifling business agility and efficiency while not having a meaningful effect on patient data security and privacy. And now, a new slew of federal privacy and security audits are targeting not only healthcare providers, but also their business associates, insurers, and other entities. For those on the hook for satisfying HIPAA's expanding requirements, compliance will an ongoing hurdle for the foreseeable future.

It's not hard to understand why. Healthcare data is highly prized amongst cyber attackers, worth more than 10 times the value of credit card data on the black market. The reason for this is also easy to understand (and painfully evident to unfortunate victims): unlike a credit card number, healthcare and patient data like social security numbers and biometric patterns cannot be replaced. In these scenarios, individuals are effectively "hacked for life."

The high value of healthcare data combined with years of lackluster security controls has left the healthcare industry reeling from cyber attacks. At the end of 2015, the Office of Civil Rights (OCR) under the Health and Human Services department (HHS) published a list of data breaches as reported to them per HIPAA. 253 healthcare breaches occurred during the course of the year affecting 500 individuals or more with a total loss of over 112 million records.

Such data breaches are estimated to cost the healthcare industry around $5.6 billion every year. Unfortunately, this figure is expected to increase year after year as digitization accelerates and the healthcare industry continues to move towards connected care. This invariably means that more sensitive patient and healthcare data will be transmitted across the wire, over wifi networks, and between IoT and smart devices—not to mention stored and processed in the cloud.

Information technology is a crucial albeit costly endeavor for HIPAA-impacted organizations; in response, regulatory bodies have ramped up auditing and enforcement efforts in hopes of stifling the seemingly daily barrage of medical data breaches splashed across the headlines. For non-compliant organizations, the cost of non-compliance could include civil, criminal, and other penalties.

Data breaches are estimated to cost the healthcare industry around $5.6 billion every year

Top 10 Healthcare Data Breaches in 2015

Organization	Records Breached	Type of Breach
Anthem BlueCross	78,800,000	Hacking/IT Incident
Premera Blue Cross	11,000,000	Hacking/IT Incident
Excellus	10,000,000	Hacking/IT Incident
UCLA Health	4,500,000	Hacking/IT Incident
mie Medical Informatics Engineering	3,900,000	Hacking/IT Incident
CareFirst	1,100,000	Hacking/IT Incident
DMAS	697,586	Hacking/IT Incident
Georgia Department of Community Health	557,779	Hacking/IT Incident
Beacon Health System — Lighting the Way to Wellness	306,789	Hacking/IT Incident
DJO Global	160,000	Laptop Theft

Source: http://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

The Facts About HIPAA

HIPAA is the name of the statute, not the actual set of regulations that require adherence. Additionally, HIPAA does not solely deal with data privacy and security—the legislation consists of 5 titles that cover issues ranging from post-employment healthcare coverage to employers' deductions of company-owned life insurance premiums for income tax purposes:

- Title I - health care access, portability and renewability
- Title II - preventing health care fraud and abuse; administrative simplification; medical liability reform
- Title III - tax-related health provisions
- Title IV - application and enforcement of group health plan requirements
- Title V - revenue offsets

Subsequently, when professionals refer to HIPAA compliance—especially in the context of IT—they are usually referring to compliance with Title II.

ARRA and the HITECH Act

HIPAA was originally created to protect the health insurance rights of employees; the additional titles were introduced over time and address different concerns regarding patient privacy, security, healthcare tax implications, reporting requirements, and more. Though HIPAA's requirements have been mandated by law since its arrival over two decades ago, the recent enactments of The American Recovery and Reinvestment Act (ARRA) and the Health Information Technology for Economic and Clinical Health Act (HITECH) have eliminated any room for interpretation by providing more prescriptive compliance requirements.

The passing of ARRA and HITECH saw the increase of noncompliance fines/penalties to a maximum of $1.5 million per incident, as well as the creation of laws requiring the HHS to initiate audits for verifying compliance. Additionally, the new enactments expanded HIPAA's coverage scope to include all businesses and partners handling, processing, analyzing, and managing/storing healthcare or patient data—not just hospitals, physicians, and insurance companies.

ARRA and HITECH place special emphasis on Title II, which addresses how firms should protect electronically stored patient and medical health data. Specifically, the HIPAA Privacy Rule and the HIPAA Security Rule under Title II dictate how HIPAA-covered firms should secure patient data, as well as provide standards for maintaining patient data security on an ongoing basis.

HIPAA Title II

HIPAA Title II is the main focus of compliance efforts for IT. This section deals with security and privacy controls and includes the following requirements, categorized under Administrative Simplification provisions:

- Unique Identifiers Rule (National Provider Identifier) – mandates that all healthcare entities have a unique 10-digit national provider identifier number (NPI).
- HIPAA Privacy Rule – puts forth national standards for protecting patient data and individual's healthcare information.
- Transactions and Code Sets Rule - mandates that covered organizations standardize their electronic data interchange (EDI) processes for submitting and processing insurance claims.
- HIPAA Security Rule - sets standards for maintaining optimal patient data security.
- Enforcement Rule - establishes guidelines for investigating HIPAA non-compliance violations.

PHI and EPHI

Entities that handle medical records and other patient health information are required by law to comply with HIPAA regulations. This type of data is referred to as protected health information (PHI) and can range from information about an individual's physical condition and psychological state to their emotional health and financial status. This includes patient and healthcare data in any form—not just electronic—that is individually identifiable.

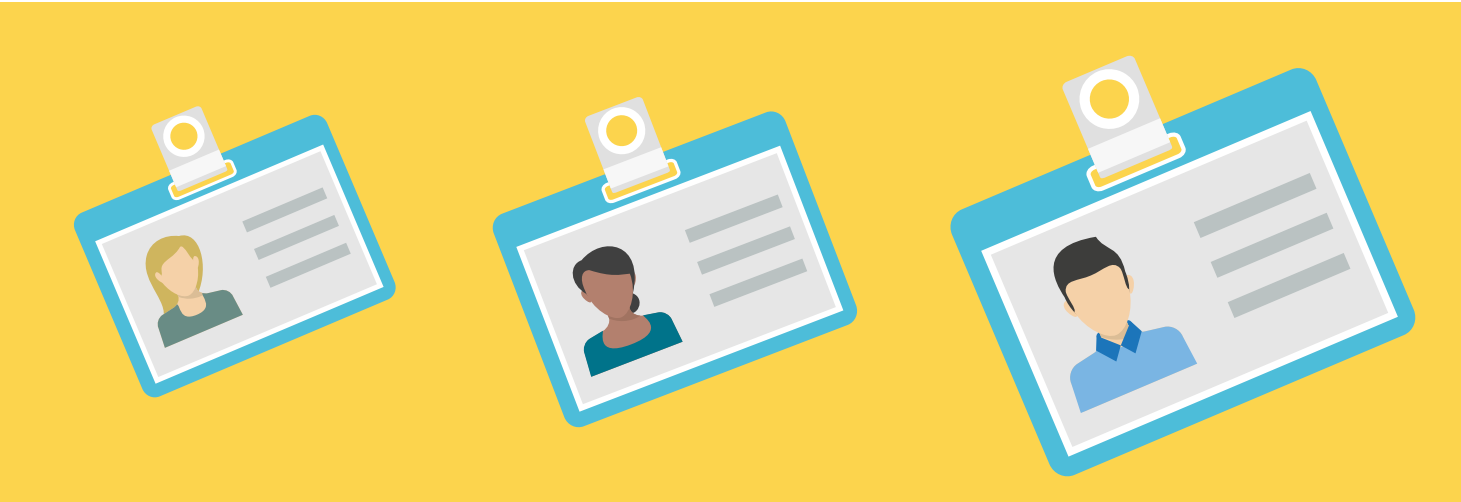
The HSS defines PHI as individually identifiable information that is:

1. Except as provided in item 2 of this definition,
    - transmitted by electronic media;
    - maintained in electronic media; or
    - transmitted or maintained in any other form or medium (includes paper and oral communication).
2. Protected health information excludes individually identifiable health information:
    - in education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g;
    - in records described at 20 U.S.C. 1232g(a)(4)(B)(iv);
    - in employment records held by a covered entity (see below for definition) in its role as employer; and
    - regarding a person who has been deceased for more than 50 years.

Individually identifiable health information is a subset of health information and includes demographic information collected from an individual. Additionally, it is:

1. created, or received by a health care provider, health plan, or health care clearing house; and
2. relates to past, present, or future physical or mental health conditions of an individual; the provision of health care to the individual; or past, present, or future payment for health care to an individual, and
    - that identifies the individual; or
    - with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Individually Identifiable Information



Data classified as individually identifiable information can describe an individual, their employer, or family member. HIPAA classifies individually identifiable information types into the following 18 categories:

- Name
- Address
- All dates (and date elements) related to an individual
- Telephone numbers
- Fax number
- Email address
- Social Security number
- Medical record number
- Health plan beneficiary number
- Account number
- Certificate/license number
- Vehicle identifiers and serial numbers, including license plate numbers
- Device identifiers or serial numbers
- Website URLs
- IP addresses
- Biometric identifiers (e.g., finger or voice prints)
- Full-face photographic images and any comparable images
- Any other unique identifying number, characteristic, or code

Electronic protected health information (ePHI) includes any PHI that is created, stored, transmitted, or received electronically. This includes current and future technologies for accessing, transmitting, and/or receiving ePHI:

1. Media containing data at-rest (e.g., storage)
    - PCs with internal hard drives used at work, home, or traveling
    - External portable hard drives, including iPods and similar devices
    - Magnetic tape
    - Removable storage devices (e.g., USB memory sticks, CDs, DVDs, and floppy disks)
    - PDAs and smartphones
1. Data in transit, via wireless, Ethernet, modem, DSL, or cable network connections
    Email
    File transfer

Covered Entities

HIPAA's privacy and security rules legally apply to all covered entities. A covered entity is any party who transmits any health or patient information in electronic form. This usually includes the following:

- Health Plans
- Healthcare Clearing Houses
- Healthcare Providers (e.g., doctors, hospitals, clinics)
- Insurance Providers
- Self-Insured Businesses
- Businesses sponsoring a group health plan for employees (e.g., flexible spending accounts)

Conclusion

As mentioned previously, most IT professionals are concerned with HIPAA Title II, which deals with proper handling of ePHI in healthcare transactions. These measures are a constant challenge for administrators and operators responsible for maintaining and securing a covered entity's infrastructure. IT environments and systems are subject to a myriad of conditions on a daily basis that threaten the consistency and integrity required for HIPAA Title II compliance.

For example, the natural tendency of IT asset configurations to move towards entropy—also known as drift—is a common condition that could lead to non-compliant systems and processes. Additionally, misconfigurations due to application and system spot fixes can also cause environments to fall out of compliance. These scenarios often result in data breaches caused by negligence—an offense punishable under HIPAA.

As of late, many forward-thinking firms operating in highly-regulated industries have embraced a model for compliance that is easier to validate, sustain, and adapt for future changes. Known as compliance-as-code, this methodology involves wrapping regulatory constraints and requirements such as those outlined in HIPAA Title 2 into automated workflows and testing/validations pipelines. Tools like UpGuard's platform for digital resilience make policy-driven HIPAA compliance an efficient, testable, repeatable, and of course—auditable.

Critics have argued that HIPAA has ruined healthcare economics; that is, the stringent requirements for compliance have made it harder and increasingly unfeasible for those in health/medical industries to provide their services. The unfortunate reality is that—like cybercrime and data breaches—HIPAA is here to stay. Covered entities should instead position themselves for continuous compliance, as a function of the organization's overall digital resilience strategy. For more about digital resilience, please check out UpGuard's ebooks on the matter—as well as other ebooks on compliance, security, and more.

Sources

http://searchdatamanagement.techtarget.com/definition/HIPAA

http://www.forbes.com/sites/danmunro/2015/12/31/data-breaches-in-healthcare-total-over-112-million-records-in-2015/

http://www.modernhealthcare.com/article/20160321/NEWS/160329977

http://www.washingtontimes.com/news/2015/dec/10/hackers-likely-to-breach-1-in-3-health-care-custom/
http://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

http://www.welivesecurity.com/2014/09/25/healthcare-security/

http://www.beckershospitalreview.com/healthcare-information-technology/10-ways-patient-data-is-shared-with-hackers.html

http://www.lexology.com/library/detail.aspx?g=8b66e71d-f892-4227-91f7-0eb63a28f40b

http://osp.od.nih.gov/office-clinical-research-and-bioethics-policy/clinical-research-policy/hipaa-administrative-simplification-statute-and-rules

http://diginomica.com/2015/04/30/compliance-as-code-brings-high-velocity-to-enterprise-it/

http://swreflections.blogspot.com/2015/04/towards-compliance-as-code.html