



HIPAA ORIENTATION AND CERTIFICATION

THE EVOLUTION OF HIPAA

- The Health Insurance Accountability and Affordability Act was passed in 1996.
- HIPAA- the gigantic statute itself- addressed several significant and varying issues for the healthcare industry, including insurance portability, fraud, and abuse issues, and significantly, privacy and security of health information. HIPAA also included provisions related to transactions and code sets meant to modernize and standardize the flow of health information electronically. And it was this push to transition health care to the digital age that prompted calls for more defined privacy and security rules.
- It was not until December 2000 that **HHS** published the first final Privacy Rule, and later modified it in another final rule making in 2002, that the privacy provisions of HIPAA were implemented. Significantly, the Privacy Rule set forth limitations on the way covered entities could use and disclose protected health information (PHI), provided individuals with rights to their PHI, and mandated that most covered entities create HIPAA privacy compliance programs by 2003.
- Separately, HHS issues the final HIPAA Security Rule in 2003 that set forth the administrative, physical, and technical safeguards that covered entities must have in place to protect electronic PHI. Covered entities must have in place to protect electronic PHI. Covered entities were required to comply with the Security Rule by 2005.

THE EVOLUTION OF HIPAA

- In February 2009, the Stimulus Bill- and with it, the HITECH Act- changed the game for privacy and security of PHI. The HITECH Act increased privacy and security obligations – both in terms of what must be done and who must comply, increased penalties for noncompliance, increased oversight and enforcement, and included the first federal breach notification obligation. In a nutshell, the HITECH Act added real teeth to HIPAA making it far less likely that covered entities and their business associates would ignore privacy and security compliance or even make it anything less than high priority.
- Finally, in January 2013, HHS issued the final HIPAA Omnibus Rule that implements the HITECH Act' privacy and security provisions, thereby modifying the HIPAA Privacy and Security Rules.

WHAT DOES THIS ALL MEAN?

We must continue to identify and address new risks, account for new technologies (e.g., no one was worrying about iPhones, iPads, or the cloud back in 1996, were they?), and continue to be vigilant in implementing policies and procedures to address these new issues and train those who have access to PHI.

(Rebecca Fayed, "Happy Birthday, HIPAA: How the Law Evolved, and What's in Store," The Advisory Board Company, August 23, 2013)

WHAT IS PHI?

According to the US Department of Health and Human Services, **protected health information (PHI)** is individually identifiable information that is:

- Transmitted by electronic media;
- Maintained in electronic media; or
- Transmitted or maintained in any other form or medium (includes paper and oral communication).

18 PHI IDENTIFIERS

1. Name
2. Address (all geographic subdivisions smaller than state, including street address, city, county, or ZIP code)
3. All elements (except years) of dates related to an individual (including birth date, admission date, discharge date, date of death, and exact age if over 89)
4. Telephone numbers
5. FAX number
6. Email Address
7. Social Security Number
8. Medical Record Number
9. Health Plan Beneficiary Number
10. Account Number
11. Certificate/License Number
12. Vehicle Identifiers and Serial Numbers (including license plate numbers)
13. Device Identifiers or Serial Numbers
14. Web URLs
15. IP Address
16. Biometric Identifiers (including finger or voice prints)
17. Full-face Photographic Images and Any Comparable Images
18. Any Other Unique Identifying Number, Characteristic, or Code

HOW DOES EHI PROTECT PHI?

Our Complete Compliance Plan

- Privacy Statement
- Business Associate Agreements
- Employee Handbook
- Employee Confidentiality Agreement and Non Sanction Certification
- Incident Response Plan
- Disaster Preparation and Recovery
- Risk Assessment Plan
- Quarterly HIPAA Awareness Training
- Visitor Orientation and Acknowledgement

WHY DO WE DO THIS?

1. Covered entity or individual did not know (and by exercising reasonable diligence would not have known) the act was a HIPAA Violation.
2. The HIPAA violation had a reasonable cause and was not due to willful neglect.
3. The HIPAA violation was due to willful neglect but the violation was corrected within the required time period.
4. The HIPAA violation was due to willful neglect and was not corrected.

- \$100-50,000 for each violation up to a maximum of \$1.5 million for identical provisions during a calendar year
- \$1,000-\$50,000 for each violation, up to a maximum of \$1.5 million for identical provisions during a calendar year
- \$1,000-\$50,000 for each violation, up to a maximum of \$1.5 million for identical provisions during a calendar year
- \$50,000, or more for each violation, up to a maximum of \$1.5 million for identical provisions during a calendar year

Criminal Penalties

Tier	Potential Jail Sentence
Unknowingly or with reasonable cause	Up to one year
Under false pretenses	Up to five years
For personal gain or malicious reasons	Up to ten years

SECURITY AND PRIVACY TRAINING ACKNOWLEDGEMENT FORM

I _____ acknowledge and agree that I fully understand the HIPAA Privacy and Security rules and the definition of Protected Health Information (PHI) that have been explained to me. I have had the opportunity to ask questions regarding those rules, and I am fully aware of my responsibility regarding the opportunity safeguarding of any PHI of which I may become aware during the course of my visit with Enable Healthcare Inc.

I further agree, that as a condition of being allowed to visit within EHI's facility, that I should become aware of any PHI, I will not disclose to anyone the information contained in or related to such PHI, including the existence of such PHI, nor will I use such PHI for my own direct or indirect benefit or sell any data contained in the PHI.

Signature

Date

Enable Healthcare Inc. Witness