The Health Insurance Portability and Accountability Act of 1996 (HIPAA)

By Hadar Kolberg, Adv. & Dan Or -Hof, Adv., Esq., CIPP/E; CIPP/US; CIPM

1. **What is HIPAA?**
2. **What are HIPAA's Main Rules?**
   - 2.1. **The Privacy Rule**
   - 2.2. **The Security Rule**
   - 2.3. **The Enforcement Rule**
   - 2.4. **The Breach Notification Rule**
   - 2.5. **The Omnibus Rule**
3. **Who Needs to Comply with HIPAA?**
   - 3.1. **What are Covered Entities?**
   - 3.2. **What are Business associates?**
4. **What is PHI and When Does HIPAA Protect PHI?**
5. **What are the Requirements for HIPAA Compliance?**
6. **Does ISO 27001, ISO 27002, or ISO 27799 Certification Suffice to Comply with HIPAA Requirements?**
7. **What are the Consequences of Non-Compliance?**
8. **What are the Main Considerations for HIPAA Compliance?**

1. What is HIPAA?

The Health Insurance Portability and Accountability Act of 1996, commonly known as HIPAA, is the primary U.S. federal law regulating the privacy and security of protected health information (PHI). In a nutshell, entities that store, collect, or process PHI of U.S. citizens and their service providers are obligated to implement appropriate safeguards to protect PHI by limiting the uses and disclosures of such information.

HIPAA compliance is regulated by the Department of Health and Human Services (HHS) and enforced by the Office for Civil Rights (OCR). A failure to meet HIPAA provisions can have serious financial, legal, and reputational consequences.

2. What Are HIPAA's Main Rules?

HIPAA's main rules are as follows:

2.1. The Privacy Rule.

The Privacy Rule covers the confidentiality of PHI, limiting the use and disclosure of such information and addresses the right of individuals to control the use of their PHI. Further information on the Privacy Rule is available at https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html.

2.2. The Security Rule.

The Security Rule sets the standards for administrative, technical, and physical safeguards to protect the confidentiality, integrity, and availability of electronic PHI. Further information on the Security Rule is available at https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html.

2.3. The Enforcement Rule.

The Enforcement Rule sets standards for the enforcement of HIPAA provisions (further information on the Enforcement Rule is available at

https://www.hhs.gov/hipaa/for-professionals/special-topics/enforcement-rule/index.html).

2.4. The Breach Notification Rule.

The Breach Notification Rule sets provisions regarding notices to individuals and the government when a breach of unsecured PHI occurs (further information on the Breach Notification Rule is available at https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html).

2.5. The Omnibus Rule.

The Omnibus Rule implements several provisions of the Health Information Technology for Economic and Clinical Health (HITECH) Act*****, to strengthen the privacy and security protections for PHI established under HIPAA (further information on the Omnibus Rule is available at https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/combined-regulation-text/omnibus-hipaa-rulemaking/index.html).

***The HITECH Act** is part of The American Recovery and Reinvestment Act of 2009 (ARRA). The HITECH Act encourages healthcare providers to adopt electronic health records (EHRs) and improve the privacy and security of PHI, by imposing financial

incentives for adopting EHRs and increased penalties for violations of the HIPAA provisions. The relevant requirements of HITECH were incorporated into HIPAA in the Omnibus Rule.

3. Who Needs to Comply with HIPAA?

HIPAA applies to individuals, organizations, and agencies that deal with PHI and meet the definition of either covered entities or business associates, as these terms are defined under HIPAA (see below).

Under HIPAA, covered entities are obligated to enter into agreements with their business associates to ensure the safeguarding of PHI. Thus, as part of an engagement between a covered entity and a business associate, some of HIPAA provisions are streamed down to business associates through the engagement contract, creating direct liability to business associates in the form of an agreement, in addition to their statutory liability.

3.1. What are Covered Entities?

HIPPA defines covered entities as one of the following:

3.1.1. **A Health Care Provider** that transmits PHI in an electronic form. This includes providers such as doctors, clinics, pharmacies, etc.;

3.1.2. **A Health Plan** such as health insurance companies; and

3.1.3. **A Health Care Clearinghouse** which are entities that process nonstandard format health information they receive from another entity into a standard health information format or vice versa, such as bulling services and repricing companies.

Further information on covered entities is available at https://www.hhs.gov/hipaa/for-professionals/covered-entities/index.html.

3.2. What are Business Associates?

A business associate is a person that performs activities involving the use or disclosure of PHI on behalf of or provides services to, a covered entity, but other than in the capacity of an employee of such covered entity.

Further information on business associates is available at https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/index.html

4. What is PHI and When does HIPAA protect PHI?

PHI is defined under HIPAA as individually identifiable health information, transmitted or maintained by electronic media or in any other form or medium.

HIPAA applies and protects PHI created, received, maintained or transmitted by a covered entity or a business associate.

5. What are the Requirements for HIPAA Compliance?

HIPAA addresses mainly covered entities. Thus, many of its requirements, such as the obligation to publish a privacy practices notice, apply only to covered entities and not to business associates. However, some of the HIPAA provisions also apply to business associates, which creates a direct liability of business associates (further information on business associates' direct liability is available at https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/factsheet/index.html).

For instance, HIPAA requires covered entities to enter into agreements with their business associates to ensure the safeguarding of PHI (Business Associate Agreement – BAA). Business associates are under the same obligation to enter into agreements with their business associates (subcontractor business associate).

To meet HIPAA requirements, covered entities and business associates must implement policies and procedures designed to protect the privacy, security, and integrity of PHI. Examples for such policies and procedures are Breach Notification Procedure, Data Retention and Destruction Policy, Audit and Investigation Response Procedure, etc.

Further requirements that apply both to covered entities and business associates are appointment of personnel and documentation obligations.

6. Are ISO 27001, ISO 27002, or ISO 27799 Certifications Sufficient to Comply with HIPAA Requirements?

The ISO/IEC 27000 is a series of sets of Information Security Management Systems (ISMS) standards, published by the International Organization for Standardization (ISO). These constitute an information security framework that provides general information security best practices. Most of HIPAA Security Rule concepts can be found under the ISMS certifications, yet the ISMS certifications do not address all of HIPAA requirements.

For example, while ISMS certifications require segregation of network, HIPAA Security Rule includes a specific requirement regarding the isolation of health care clearinghouse functions, where such health care clearinghouse is a part of a larger organization.

Another example pertains to documentation retention time. While ISMS certifications include general provisions such as: "Some records may need to be securely retained to meet statutory, regulatory or contractual requirements, as well as to support essential business activities"; and "The time period and data content for information retention may be set by national law or regulation", HIPAA requires retaining documentation for 6 years from the date of its creation or the date when it was last in effect, whichever is later.

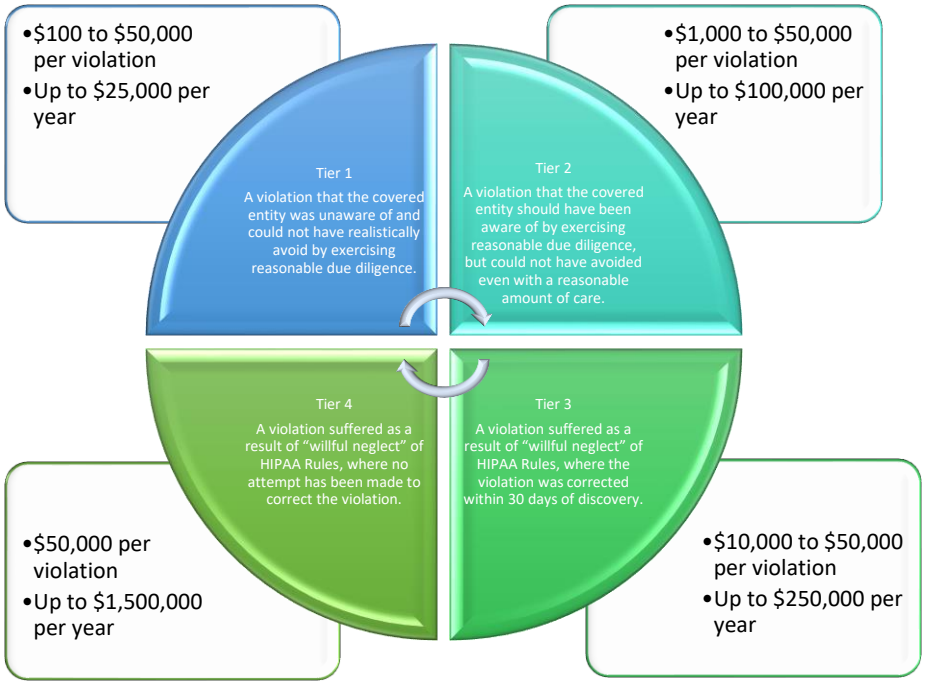
7. What are the Consequences of Non-Compliance?

In addition to severe potential reputational damages, covered entities and business associates risk both contract and federal or state government sanctions for failures to protect the privacy and security of PHI as required by HIPAA.

A covered entity might hold a business associate liable for violating one or more of the BAA provisions. Likewise, a business associate can hold its business associates contractually liable.

Furthermore, an impermissible use or disclosure that compromises the security or privacy of the PHI is generally deemed to be a breach that might trigger a civil monetary or criminal penalty.

Civil monetary penalties are imposed by the Office for Civil Rights (OCR), based on the severity of the violation. The four categories used for the OCR to determine the amount of the fines are as follows:



In 2018 alone, the OCR settled ten enforcement cases, in a total amount of $28.7 million. The single largest individual HIPAA settlement in history until now was with Anthem, Inc. for the amount of $16 million.

Further information on 2018 OCR HIPAA settlements is available at https://www.hhs.gov/sites/default/files/2018-ocr-hipaa-summary.pdf.

Additionally, on January 16, 2018, in *Byrne v. Avery*, the Connecticut Supreme Court ruled that a HIPPA breach can give rise to a tort cause of action for violation of a patient's health care privacy (Byrne v. Avery Center for Obstetrics & Gynecology, P.C., 327 Conn. 540, __ A.3d(January 16, 2018)).

8. What Are the Main Considerations for HIPAA Compliance?

- Risk Assessment
- Breach Notification

- Necessary agreements
- Privacy Practices Notice
- HIPAA Compliance Policies and Procedures
- Personnel Designations

This is **not** an exhaustive list of HIPAA requirements.

Please note: This article does not constitute legal advice.