INFODOC

Legitimis

HIPAA 101

Legal Framework

In 1996, Congress enacted the Health Insurance Portability and Accountability Act ("HIPAA"),which seeks to provide insurance portability, fraud enforcement, and administrative simplification for the health care industry. Sections 261-264 of HIPAA direct the Department of Health and Human Services (HHS) to promulgate regulations and publicize standards for the electronic exchange, privacy, and security of health information.

Pursuant to this authority, HHS published four main "Rules," which are collectively referred to as the "Administrative Simplification" provisions: (1) the "Privacy Rule;" (2) the "Security Rule;" (3) the "Electronic Transactions and Code Sets Rules;" and (4) the "Unique Identifier Rules."

The Privacy Rule

The "Privacy Rule," which was originally published in 2000 and updated in 2002, can be found at CFR Parts 160 and 164, Subparts A and E. Under the Privacy Rule:

- "**Covered Entities**" (Health Plans, Health Providers, and Healthcare Clearinghouses) may not use or disclose "Protected Health Information (PHI)," which is defined as "all individually identifiable health information held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral."
- "**De-Identified Data**" (i.e., data that cannot be traced to a specific individual) is outside the scope of HIPAA and is therefore not subject to the Privacy Rule.
- There are two categories of **exceptions** (1) when HHS permits or requires use or disclosure of PHI and (2) when the person who is the subject of the PHI authorizes use or disclosure in writing.

The Security Rule

The "Security Rule," published in 2003 and available at CFR Parts 160 and 164, Subparts A and C, delineates a series of **administrative, technical, and physical security procedures** for Covered Entities to ensure the confidentiality, integrity, and availability of "Electronic Protected Health Information (e-PHI)."

There is significant overlap between the Security Rule and the Privacy Rule. Both rules govern the use and disclosure of health data by Covered Entities and exclude "De-Identified Data." The key difference is that, while the Privacy Rule applies to all PHI, the Security Rule only applies to PHI that a Covered Entity creates, receives, maintains, or transmits in **electronic** form ("e-PHI"). This does not include information that

is transmitted orally or in writing.

Under the Security Rule, Covered Entities must maintain **reasonable and appropriate administrative, technical, and physical safeguards** for protecting e-PHI. Specifically, they must:

- Ensure the confidentiality, integrity, and availability of all e-PHI they create, receive, maintain, or transmit;
- Identify and protect against **reasonably anticipated** threats to the security or integrity of the information;
- Protect against **reasonably anticipated**, impermissible uses or disclosures;
- Ensure compliance by their workforce.

Although the Privacy Rule and the Security Rule are, technically speaking, separate rules, organizations must not treat them as completely separate, independent rules with respect to compliance matters. Instead, there is significant overlap between the two, and compliance officers must take an **integrated, holistic approach** that ensures compliance with both rules. Conceptually, "privacy" is the goal and "security" is the means by which organizations can achieve that goal: organizations must implement security safeguards to mitigate risks to PHI in order to ensure privacy.

HITECH and Business Associates

In 2009, Congress passed the American Recovery and Reinvestment Act (the "ARRA," more commonly known as the "Stimulus"). The ARRA sought to improve health care delivery and patient care through significant investment in health information technology ("HIT").

To this end, the HITECH Act ("HITECH"), which is part of the ARRA, seeks to strengthen the Privacy Rule and the Security Rule by (1) **extending privacy and security obligations to "Business Associates" of Covered Entities** (previously, Business Associates were only indirectly covered by HIPAA, i.e., through a contract with a Covered Entity) and (2) adding privacy and security **breach notification requirements**.

In 2013, HHS announced the final version of the Omnibus Rule, which contains four "Final Rules":

- Final Rule One" makes final modifications to the HIPAA Privacy, Security, and Enforcement Rules mandated by HITECH.
- "Final Rule Two" adopts changes to the HIPAA Enforcement Rule.
- "Final Rule Three" replaces HITECH's breach notification "harm" threshold with a more objective standard.
- "Final Rule Four" modifies the Privacy Rule to prohibit most health plans from using or disclosing genetic information for underwriting purposes.