HIPAA Privacy & Security Rules

The HIPAA Privacy Rule provides federal protections for individually identifiable health information held by covered entities and their business associates and gives patients an array of rights with respect to that information. At the same time, the Privacy Rule is balanced so that it permits the disclosure of health information needed for patient care and other important purposes. To read the full text of the HIPAA Privacy Rule, go to Modifications to the HIPAA Privacy Rule – Final Rule.

The Security Rule specifies a series of administrative, physical, and technical safeguards for covered entities and their business associates to use to assure the confidentiality, integrity, and availability of electronic protected health information. To read the full text of the HIPAA Security Rule, go to Security Standards – Final Rule (PDF).

The HIPAA Privacy and Security Rule requirements are explained in detail under My Assessments.

HIPAA Privacy & Security Rule Updates

The U.S. Department of Health and Human Services released final regulations in 2013 that address the recent legislative changes made to the Health Insurance Portability and Accountability Act's privacy and data security rules.

Also known as HIPAA, the changes incorporate privacy and data security rules from the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act, according to an HHS release.

The majority of the new regulations prohibit the sale of protected health information and the use of it for marketing and fund-raising purposes, the release states.

A new standard will also be applied to how to determine what qualifies as a breach of unsecured PHI by a health plan or a business associate. Under the new rules a breach will be presumed to have occurred unless the health plan or business associate demonstrates that there is a low probability that the PHI has been compromised, according to the statement.

Health plans no longer need to place business associates under contract to maintain the confidentiality of the plan's PHI. HIPAA's privacy and data security rules now directly apply to business associates, as do the law's civil and criminal penalties, the release explains.

According to the release, for each potential breach, a new rule requires a formal risk assessment. If a breach is found to have occurred, the offending health plan is required to notify each affected individual within 60 days of the discovery of the breach, according to the statement.

Summary of the HIPAA Omnibus Rule

HHS summarized the over 500 pages of the Omnibus Rule as follows:

"This omnibus final rule is comprised of the following four final rules:

1. Final modifications to the HIPAA Privacy, Security, and Enforcement Rules mandated by the Health Information Technology for Economic and Clinical Health (HITECH) Act, and certain other modifications to improve the Rules, which were issued as a proposed rule on July 14, 2010. These modifications:
    a. Make Business Associates of Covered Entities directly liable for compliance with certain of the HIPAA Privacy and Security Rules' requirements.
    b. Strengthen the limitations on the use and disclosure of protected health information for marketing and fundraising purposes, and prohibit the sale of protected health information without individual authorization.
    c. Expand individuals' rights to receive electronic copies of their health information and to restrict disclosures to a health plan concerning treatment for which the individual has paid out of pocket in full.
    d. Require modifications to, and redistribution of, a Covered Entity's notice of privacy practices.
    e. Modify the individual authorization and other requirements to facilitate research and disclosure of child immunization proof to schools, and to enable access to decedent information by family members or others.
    f. Adopt the additional HITECH Act enhancements to the Enforcement Rule not previously adopted in the October 30, 2009, interim final rule, such as the provisions addressing enforcement of noncompliance with the HIPAA Rules due to willful neglect.
2. Final rule adopting changes to the HIPAA Enforcement Rule to incorporate the increased and tiered civil money penalty structure provided by the HITECH Act, originally published as an interim final rule on October 30, 2009.
3. Final rule on Breach Notification for Unsecured Protected Health Information under the HITECH Act, which replaces the breach notification rule's "harm" threshold with

a more objective standard and supplants an interim final rule published on August 24, 2009.

4. Final rule modifying the HIPAA Privacy Rule as required by the Genetic Information Nondiscrimination Act (GINA) to prohibit most health plans from using or disclosing genetic information for underwriting purposes, which was published as a proposed rule on October 7, 2009."