Final Rule: Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules

Description: This final rule strengthens the privacy and security protections established under the Health Insurance Portability and Accountability of 1996 Act (HIPAA) for individual's health information maintained in electronic health records and other formats. This final rule also makes changes to the HIPAA rules that are designed to increase flexibility for and decrease burden on the regulated entities, as well as to harmonize certain requirements with those under the Department's Human Subjects Protections regulations. These changes are consistent with, and arise in part from, the Department's obligations under Executive Order 13563 to conduct a retrospective review of our existing regulations for the purpose of identifying ways to reduce costs and increase flexibilities under the HIPAA Rules.

Major Provisions

- Replaces the "harm" threshold from the interim rule on breach notification with a more objective standard;
    - Covered entities and business associates are required to assess the probability that PHI has been compromised instead of assessing the risk of harm to the individual.
    - The final rule clarifies that, unless covered entities or business associates specifically demonstrate that there is a "low probability that the PHI has been compromised" or that one of the exceptions to the definition of breach included in the rule applies, breach notification is required to be provided. The use of this presumption in the risk approach of the final rule is intended to ensure that the breach notification obligations are interpreted and applied in a uniform way by all covered entities and business associates.
- Requires business associates to comply with specific HIPAA privacy and security requirements and imposes direct liability for their noncompliance with these regulatory standards;
    - The Final Rule expands the definition of "business associate" to include a subcontractor that creates, receives, maintains, or transmits PHI on behalf of a BA. If PHI is involved, a subcontractor is considered a BA, despite how far "down the chain" the subcontractor provides services.
    - The Final Rule also modifies the definition of "business associate" to include an entity, such as a data storage company, that maintains PHI, even if the entity does not actually view the PHI. Health Information Organizations, E-Prescribing Gateways, and Vendors of Personal Health Records are also BAs under the Final Rule.
    - Direct HIPAA liability is not contingent on whether a formal BA agreement is actually executed.
- Incorporates the increased and tiered civil money penalty structure provided by HITECH;

    - There are four categories of HIPAA violations that reflect increasing levels of culpability, which range from not knowing of the violation to willful neglect and failure to correct the violation.
    - Four corresponding tiers of penalty amounts, which range from $100 per violation to $50,000 per violation
    - A maximum penalty of $1.5 million for all violations of an identical provision.
    - In accordance with the HITECH Act, the Final Rule also includes a prohibition on the imposition of penalties for any violation that is corrected within a 30-day time period, as long as the violation was not due to willful neglect.
- Prohibits most health plans from using or disclosing genetic information for underwriting purposes, as required by the Genetic Information Nondiscrimination Act.
    - To help clarify for health plans the types of uses and disclosures that are prohibited by this new provision, the Final Rule makes several definitional additions and changes, including the addition of definitions for the terms "genetic information," "genetic services," "genetic test," and "underwriting purposes."

Breach Assessment

The final rule requires a demonstration that there is a low probability that the PHI has been compromised through a risk assessment that, at a minimum, examines all of the following factors:

- The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
- The unauthorized person who used the PHI or to whom the disclosure was made;
- Whether the PHI was actually acquired or viewed; and
- The extent to which the risk to the PHI has been mitigated.

Individual Rights

The final rule also includes an expansion of individual rights by:

- Allowing patients to ask for a copy of their electronic medical record in an electronic form
    - Covered entities must provide an individual with a copy of their PHI that is maintained by the covered entity as electronic PHI in the electronic form and format requested by the individual if such format is readily producible. If the requested format is not readily producible, the covered entity must offer to produce the electronic PHI in at least one readable electronic format.
    - A hard copy may be provided if the requesting individual rejects any of the offered electronic formats.
    - The Final Rule decreases the total time covered entities have to respond to requests for access from 90 to 60 days by removing the provision allowing an additional 30 days if PHI is not maintained onsite. Covered entities now have 30 days to respond, unless they

provide the individual written notice of a one-time extension of up to 30 days, including the reason for the delay and the expected date of completion.

- Giving individuals who pay by cash authority to instruct their provider not to share information about their treatment with their health plan
- Setting new limits on how information is used and disclosed for marketing and fundraising purposes
    - HIPAA requires that covered entities permit individuals to request restrictions on the uses or disclosures of their PHI for treatment, payment, and health care operations purposes, as well as for disclosures to family members and certain other permitted purposes. While covered entities are not required to agree to such requests, if a covered entity does agree to the restriction, then the covered entity must abide by that restriction.
    - The Final Rule creates an exception to this general rule by providing that a covered entity must comply with an individual's request to restrict disclosure to a health plan if:
        1. the disclosure is for the purpose of carrying out payment or health care operations and is not otherwise required by law, and
        2. the PHI pertains solely to a health care item or service for which the individual, or person other than the health plan on behalf of the individual, has paid the covered entity in full.
- Prohibiting the sale of an individuals' health information without their permission
    - The Final Rule generally defines "sale of PHI" to mean disclosure of PHI by a covered entity or BA in exchange for direct or indirect remuneration. "Remuneration" can apply to the receipt of nonfinancial as well as financial benefits.
    - HHS clarifies that "sale of PHI" does not include 1) payments to a covered entity in the form of grants, contracts, or other arrangements to perform programs or activities, such as a research study or 2) payments received regarding exchange of PHI through a health information exchange. There are also limited exceptions to the prohibition, such as disclosures for public health or certain research activities.
    - Although the Final Rule explains that the sale of PHI includes disclosures for which the Covered Entity receives remuneration, it is important to note that, in many cases, disclosures of PHI to researchers will not be prohibited by the sale of PHI provision.

The Final Rule makes several changes to the Notice of Privacy Practices ("NPP") requirements of the Privacy Rule:

- The NPP must include a statement regarding the uses and disclosures of PHI that require an authorization, such as marketing, psychotherapy notes, and sale of PHI, and require that uses and disclosures not described in the NPP will be made only with the individual's authorization.
- The NPP must state that the Covered Entity may contact an individual to raise funds for the Covered Entity and that the individual has the right to opt out of receiving such fundraising communications.

- Health plans that underwrite are prohibited from using or disclosing PHI that is genetic information about an individual for underwriting purposes. Such health plans are required to include a statement in their NPP explaining this prohibition. The Final Rule notes that this requirement does not apply to issuers of long term care policies, which are not subject to the underwriting prohibition.
- The NPP must explain that the Covered Entity must agree to a request to restrict disclosure of PHI to a health plan if the individual has paid out of pocket in full for the health care item or service. The Final Rule notes that only covered health care providers (and not other Covered Entities) are required to include this explanation in the NPP.
- The NPP must notify individuals of their right to receive notification following a Breach of the individual's Unsecured PHI.

The final HIPAA rule will be published in the Jan. 25 Federal Register, and takes effect March 26. However, covered entities and their business associates generally will have until Sept. 23 to comply with most of the rule's provisions, including the changes to the breach notification requirements.