Published on *The National Law Review* https://natlawreview.com

HIPAA Final Omnibus Rule Brings “Sweeping Change” to Health Care Industry

Article By:

Jennifer Orr Mitchell

Matthew S. Arend

On January 17, 2013, the **U.S. Department of Health and Human Services (HHS)** announced the release of the HIPAA final omnibus rule, which was years in the making. The final rule makes sweeping changes to the HIPAA compliance obligations of covered entities and business associates and comprises four final rules wrapped into one:

1. 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;
2. Changes to the HIPAA Enforcement Rule to incorporate the increased and tiered civil money penalty structure provided by the HITECH Act and to adopt the additional HITECH Act enhancements to the Enforcement Rule that were not previously adopted in the October 30, 2009 interim final rule, including provisions to address enforcement where there is HIPAA non-compliance due to willful neglect;
3. A final rule on Breach Notification for Unsecured Protected Health Information under the HITECH Act, which eliminates the breach notification rule's "harm" threshold and supplants an interim final rule published on Aug. 24, 2009; and
4. A 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 Oct. 7, 2009.

HHS estimates a total cost of compliance with the final omnibus rule’s provisions to be between $114 million and $225.4 million in the first year of implementation and approximately $14.5 million each year thereafter. Among the costs HHS associates with the final rule are: (i) costs to covered entities of revising and distributing new notices of privacy practices; (ii) costs to covered entities related to compliance with new breach notification requirements; (iii) costs to business associates to bring their subcontracts into compliance with business associate agreement requirements; and (iv)

costs to business associates to come into full compliance with the Security Rule. HHS attributes between $43.6 million and $155 million of its first year estimates to business associate compliance efforts. It is predicted that the true compliance costs for both covered entities and business associates will be far in excess of these HHS estimates.

Some of the key provisions of the final omnibus rule include:

- **Expanded definition of "business associate."** The definition of "business associate" has been expanded to include subcontractors of business associates, any person who "creates, receives, maintains, or transmits" protected health information on behalf of a covered entity, and certain identified categories of data transmission services that require routine access to protected health information, among others. A covered entity is not required to enter into a business associate agreement with a business associate that is a subcontractor; that obligation flows down to the business associate, who is required to obtain the proper written agreement from its subcontractors.
- **Direct compliance obligations and liability of business associates.** Business associates are now directly liable for compliance with many of the same standards and implementation specifications, and the same penalties now apply to business associates that apply to covered entities, under the Security Rule. Additionally, the rule requires business associates to comply with many of the same requirements, and applies the same penalties to business associates that apply to covered entities, under the Privacy Rule. Business associates must also obtain satisfactory assurances in the form of a business associate agreement from subcontractors that the subcontractors will safeguard any protected health information in their possession. Finally, business associates must furnish any information the Secretary requires to investigate whether the business associate is in compliance with the regulations.
- **Modified definition of "marketing."** The definition of "marketing" has been modified to encompass treatment and health care operations communications to individuals about health-related products or services if the covered entity receives financial remuneration in exchange for making the communication from or on behalf of the third party whose product or service is being described. A covered entity must obtain an individual's written authorization prior to sending marketing communications to the individual.
- **Prohibition on sale of PHI without authorization.** An individual's authorization is required before a covered entity may disclose protected health information in exchange for remuneration (i.e., "sell" protected health information), even if the disclosure is for an otherwise permitted disclosure under the Privacy Rule. The final rule includes several exceptions to this authorization requirement.
- **Clear and conspicuous fundraising opt-outs.** Covered entities are required to give individuals the opportunity to opt-out of receiving future fundraising communications. The final rule strengthens the opt-out by requiring that it be clear and conspicuous and that an individual's choice to opt-out should be treated as a revocation of authorization. However, the final rule leaves the scope of the opt-out to the discretion of covered entities. In addition to demographic information, health insurance status, and dates of health care provided to the individual, the final rule also allows covered entities to use and disclose: department of service information, treating physician information, and outcome information for fundraising purposes. Covered entities are prohibited from conditioning treatment or payment on an individual's choice with respect to the receipt of fundraising communications. In addition, the NPP must inform individuals that the covered entity may contact them to raise funds and that they have a right to opt-out of receiving such communications.
- **Right to electronic copy of PHI.** If an individual requests an electronic copy of protected health information that is maintained electronically in one or more designated record sets, the

covered entity must provide the individual with access to the electronic information in the electronic form and format requested by the individual, if it is readily producible, or, if not, in a readable electronic form and format as agreed to by the covered entity and the individual.

- **Right to restrict disclosures to health plans.** When an individual requests a restriction on disclosure of his or her protected health information, the covered entity must agree to the requested restriction (unless the disclosure is otherwise required by law), if the request for restriction is on disclosures to a health plan for the purpose of carrying out payment or health care operations and if the restriction applies to protected health information for which the health care provider has been paid out of pocket in full. Covered health care providers will need to employ some method to flag or make a notation in the record with respect to the protected health information that has been restricted to ensure that such information is not inadvertently sent to or made accessible to the health plan for payment or health care operations purposes, such as audits by the health plan.
- **GINA changes for some health plans.** Health plans that are HIPAA covered entities, except issuers of long term care policies, are prohibited from using or disclosing an individual's protected health information that is genetic information for underwriting purposes. The rule does not affect health plans that do not currently use or disclose protected health information for underwriting purposes.
- **Provision for compound authorizations for research.** A covered entity may combine conditioned and unconditioned authorizations for research, provided that the authorization clearly differentiates between the conditioned and unconditioned research components, clearly allows the individual the option to opt in to the unconditioned research activities, and the research does not involve the use or disclosure of psychotherapy notes. For research that involves the use or disclosure of psychotherapy notes, an authorization for a use or disclosure of psychotherapy notes may only be combined with another authorization for a use or disclosure of psychotherapy notes.
- **Required changes to Notice of Privacy Practices (NPP).** NPPs must be modified and distributed to individuals to advise them of the following: (1) for health plans that underwrite, the prohibition against health plans using or disclosing PHI that is genetic information about an individual for underwriting purposes; (2) the prohibition on the sale of protected health information without the express written authorization of the individual, as well as the other uses and disclosures for which the rule expressly requires the individual's authorization (i.e., marketing and disclosure of psychotherapy notes, as appropriate); (3) the duty of a covered entity to notify affected individuals of a breach of unsecured protected health information; (4) for entities that have stated their intent to fundraise in their notice of privacy practices, the individual's right to opt out of receiving fundraising communications from the covered entity; and (5) the right of the individual to restrict disclosures of protected health information to a health plan with respect to health care for which the individual has paid out of pocket in full.
- **Broader disclosure of decedents' PHI.** Covered entities are permitted to disclose a decedent's protected health information to family members and others who were involved in the care or payment for care of the decedent prior to death, unless doing so is inconsistent with any prior expressed preference of the individual that is known to the covered entity.
- **Disclosure of proof of immunizations to schools.** A covered entity is permitted to disclose proof of immunization to a school where State or other law requires the school to have such information prior to admitting the student. While written authorization will no longer be required to permit this disclosure, covered entities will still be required to obtain agreement, which may be oral, from a parent, guardian or other person acting in loco parentis for the individual, or from the individual himself or herself, if the individual is an adult or emancipated minor.
- **Tiered and enhanced enforcement provisions.** The final rule conforms the regulatory

language of the rule to the enhanced enforcement provisions of the HITECH Act. Penalties for non-compliance are based on the level of culpability with a maximum penalty of $1.5 million for uncorrected willful neglect.

As detailed above, the changes announced by HHS expand many of the requirements to business associates and subcontractors. Fortunately, the final rule provides a slight reprieve in one respect. It allows covered entities and business associates up to one year after the 180-day compliance date to modify business associate agreements and contracts to come into compliance with the rule.

Perhaps the most highly anticipated change found in the final omnibus rule relates to what constitutes a “breach” under the Breach Notification Rule. The final rule added language to the definition of breach to clarify that an impermissible use or disclosure of PHI is presumed to be a breach unless the covered entity (or business associate) demonstrates that there is a low probability that the PHI has been compromised. Stated differently, the rule removes the subjective harm standard and modifies the risk assessment to focus instead on the risk that the PHI has been compromised. The final rule also identifies four objective factors covered entities and business associates are to consider when performing a risk assessment to determine if the protected health information has been compromised and breach notification is necessary: (1) the nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification; (2) the unauthorized person who used the protected health information or to whom the disclosure was made; (3) whether the protected health information was actually acquired or viewed; and (4) the extent to which the risk to the protected health information has been mitigated.

The final omnibus rule does not address the accounting for disclosures requirements, which is the subject of a separate proposed rule published on May 31, 2011, or the penalty distribution methodology requirement, which HHS has stated will both be the subject of future rulemaking.

The Office of Civil Rights has characterized the new rules as “the most sweeping changes to the HIPAA Privacy and Security Rules since they were first implemented.” Leon Rodriguez, the Director of the Office of Civil Rights, stated, “These changes not only greatly enhance a patient’s privacy rights and protections, but also strengthen the ability of my office to vigorously enforce the HIPAA privacy and security protections, regardless of whether the information is being held by a health plan, a health care provider, or one of their business associates.”

The HIPAA final omnibus rule is scheduled to be published in the Federal Register on January 25, 2013 and will go into effect on March 26, 2013. Covered entities and business associates must comply with the applicable requirements of the final rule by September 23, 2013. Entities affected by this final rule are strongly urged to begin an analysis of their existing HIPAA compliance policies and procedures and take steps to comply with the final rule.

The HHS Press Release announcing the final rule is available at:
http://www.hhs.gov/news/press/2013pres/01/20130117b.html

The full text of the rule is currently available at:
https://www.federalregister.gov/articles/2013/01/25/2013-01073/modifications-to-the-hipaa-privacy-security-enforcement-and-breach-notification-rules

National Law Review, Volume III, Number 19