Final HIPAA /HITECH Rule Released

Lockton Global Technology & Privacy Risks Practice
January 2013

On January 17, 2013 the U.S. Department of Health and Human Services ("HHS") released the long-awaited final rule modifying the HIPAA Privacy, Security, and Enforcement Rules, and the HITECH Act’s breach notification rule relating to protected health information ("PHI"). With limited exceptions the rule contains little that is new or unexpected.

The rule goes into effect on March 26, 2013. Covered entities and business associates must comply with applicable requirements of the rule by September 23, 2013.

Notwithstanding the September 23, 2013 compliance date, covered entities and business associates may continue to operate under existing HIPAA-compliant contracts for one year if the contracts are not renewed or modified between March 26, 2013 and September 23, 2013.

MAJOR PROVISIONS OF THE RULE

• Expand the definition of “Business Associate”

The final rule expands the HIPAA definition of "Business Associate" to include patient safety organizations, health information organizations, e-prescribing gateways and other persons or entities that transmit PHI to covered entities and that require access to PHI on a routine basis.

Subcontractors of business associates also will now be included in the definition.

• Make business associates directly liable for compliance with the requirements of the HIPAA Privacy and Security rules

The final rule adopts the HITECH Act’s requirement that business associates be directly liable for violations of the HIPAA rules. Further, the rule provides that business associates will be liable for the acts of their agents.
• **Strengthen limitations on the use and disclosure of PHI for marketing and fundraising purposes and prohibit the sale of PHI without the individual’s consent**

Under the final rule patient authorization will be needed for all treatment and health care operations communications where the covered entity or business associate receives financial remuneration for making the communications from a third party whose product or service is being marketed.

The rule eliminates the requirement that a covered entity’s Notice of Privacy Practices ("NPP") inform individuals that they may receive such subsidized communications and that they have the ability to opt out of them. While HHS does not discourage such notices, the expectation is that individuals will be informed of such communications during the authorization process.

The final rule expands the scope of personal information that may be disclosed without authorization to fundraisers using PHI and acting on behalf of the covered entity. It also strengthens provisions allowing individuals to opt out of fundraising communications.

• **Expand individuals’ rights to receive electronic copies of their health information**

Under the final rule if an individual requests an electronic copy of PHI that is maintained electronically by a covered entity the entity must provide it.

• **Limit disclosures to health plans of medical treatment for which the individual has paid out of pocket in full**

The final rule requires a covered entity to comply with an individual’s request not to disclose PHI related to services that the individual has fully paid for out of pocket.

• **Require modifications to, and redistribution of, a covered entity’s Notice of Privacy Practices**

The final rule requires a number of changes to a covered entity’s Notice of Privacy Practices. The NPP now must:

1. Describe uses and disclosures of PHI that require patient authorization
2. Include a statement regarding fundraising communications and an individual’s right to opt out must also be included
3. Inform individuals of their right to restrict disclosure of PHI related to services that the individual has paid for out of pocket
4. State that individuals have a right to be notified in the event there is a breach of their PHI.

HHS deems these changes to be material, and as a consequence the rule requires covered entities to redistribute their NPPs.

• **Modify various requirements to facilitate research and disclosure of child immunization records to schools**

Under the final rule covered entities may disclose child immunization records to schools without written authorization where applicable law requires the school to have the information before admitting the student. While no written authorization will be needed, covered entities will still need to obtain and document the agreement of the child’s parent or guardian to make the disclosure.

• **Increase access of family members and others to PHI of deceased individuals**

The final rule will allow a deceased person’s PHI to be disclosed to family members who were involved in his or her medical treatment unless the individual expressed a contrary preference.

The rule will also modify the definition of PHI exclude information pertaining to individuals who have been deceased for more than 50 years so that disclosure of such information will not violate HIPAA. The rule does not prevent states from enacting laws that would preclude disclosure for longer periods.
• **Adopt various HITECH Act enhancements to the HIPAA Enforcement Rule**

The final rule formally adopts the four categories of violations created in the HITECH Act, and requires investigation of complaints of possible violations resulting from willful neglect.

• **Change the HIPAA enforcement rule to include the civil money penalty structure provided by the HITECH Act**

The final rule adopts the penalty structure established in the HITECH Act. The penalties range from $100 to $50,000 per violation depending on the nature of the violation.

• **Modify the breach notification rule’s standard for when notification must be made**

Under the current interim final rule a “breach” is defined to mean “the acquisition, access, use, or disclosure of protected health information” which “poses a significant risk of financial, reputational, or other harm to the individual”. This definition requires an evaluation of the risk to be performed in assessing whether a breach has occurred.

In one of the most significant changes made in the final rule, the definition of “breach” is modified to state that “an impermissible use or disclosure of protected health information is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised.” This definition will require covered entities and business associates to treat an event as a breach (including providing notice to affected individuals) until they can demonstrate a low likelihood that the PHI has been compromised.

Demonstrating a low probability that PHI has been compromised may not be easy. The final rule states that, at a minimum, the following factors will have to be considered:

1. The nature and extent of the PHI involved
2. The person or persons who received the PHI
3. Whether the PHI was actually acquired or viewed
4. The extent to which the risk to the PHI has been mitigated.

In many situations it will be extremely difficult to assess all of these factors. That will likely force more events to be treated as breaches.

• **Change the HIPAA privacy rule to prohibit health plans from using or disclosing genetic information for underwriting purposes**

The final rule prevents the use of genetic information for underwriting purposes by all health plans with the exception of long term care plans.

**THE ROAD AHEAD**

Now that the final rule has been released, the uncertainty covered entities and business associates have faced concerning the regulatory treatment of PHI has at last come to an end. Because the final rule does not deviate significantly from the interim final rule that has been in effect for the past few years, most covered entities and business associates should not need to make large-scale changes to their current practices and procedures. There will be many smaller changes needed though.

While the provisions of the final rule were largely expected, the costs will nevertheless be significant. For example, HHS estimates that the cost to over 700,000 covered entities to amend their NPPs will be $55.9million in the first year. The cost to business associates to comply with the HIPAA Security Rule is estimated to be as high at $113million.

Data breach notification and privacy regulatory action frequency and costs are certain to increase as well. Fortunately both these costs can be covered by insurance. We see nothing in the final rule that would change that. As the final rule will require more events to be treated as breaches than are treated as such under the interim rule, covered entities and business associates that do not currently purchase data security and privacy policies should strongly consider doing so now.

---

1. The Health Insurance Portability and Accountability Act.
2. The Health Information Technology for Economic and Clinical Health Act.