Locke Lord LLP

January 2013

New HIPAA Rule Tightens Obligations

Authors Tammy Ward Woffenden // 512-305-4776 // twoffenden@lockelord.com
Lane Wood // 214-740-8513 // lwood@lockelord.com
Jennifer Rangel // 512-305-4745 // jrangel@lockelord.com
Jan Reimann Newsom // 214-740-8639 // jnewsom@lockelord.com

The Department of Health and Human Services ("HHS") recently published its Final Rule implementing provisions of the Health Information Technology for Economic and Clinical Health ("HITECH") Act, which significantly modifies and expands requirements under HIPAA's Security and Privacy Rules. The Final Rule becomes effective on March 26, 2013. Covered entities and their business associates ("BAs") have until September 23, 2013, to comply with most new requirements and up until September 23, 2014, to renegotiate "grandfathered" BA agreements.

This article highlights some of the most notable provisions of the January 25, 2013, Final Rule.

BA Liability

The HITECH Act expands certain HIPAA liability to BAs. The Final Rule clarifies that BAs are directly liable for:

- failure to disclose protected health information ("PHI") when required by the Secretary;
- failure to diclose PHI to the covered entity, individual, or individual's designee, as necessary to satisfy a covered entity's obligations relatingto an individual's request for an electronic copy of PHI;
- failure to make reasonable efforts to limit PHI to the minimum necessary;
- failure to obtain BA agreements with subcontractors that create or receive PHI on their behalf;
- impermissible uses and disclosures;
- failure to provide covered entities with breach notification;
- failure to provide an accounting of disclosures; and
- failure to comply with the Security Rule.

Direct HIPAA liability is not contingent on whether a formal BA agreement is actually executed.

Expansion of "Business Associate"

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.

Marketing Communications

Prior authorization for all treatment and health care operations communications is required when a covered entity (or BA) receives "financial remuneration" for making the communication from a third party whose product or service is being marketed. "Financial remuneration" for this purpose means direct or indirect payment but does not include non financial benefits.

The authorization form must explain that PHI is being used for marketing purposes and disclose that the covered entity (or BA) is receiving financial remuneration from a third party for such communications. However, HHS clarifies that the authorization can broadly address marketing communications and is not required to list each third party or the specific items or services that are being marketed.

Sale of PHI

Sale of PHI without prior authorization is prohibited by the HITECH Act. 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.

Fundraising

Fundraising communications must include a clear and conspicuous opportunity to opt out of receiving any further fundraising communications. HHS gives covered entities discretion to decide what opt-out method to use, but the chosen methods cannot impose an undue burden or more than a nominal cost on individuals.

Notice of Privacy Practices

The Final Rule requires a covered entity to modify and redistribute its Notice of Privacy Practices ("NPP") to include the following:

- A description of uses and disclosures that require individual authorization, such as uses and disclosures of PHI for marketing purposes and sale;
- A statement that other uses and disclosures not described in the NPP will be made only with an individual's authorization, which may be revoked;
- A statement that covered entities will notify affected individuals following a breach of their unsecured PHI;
- A statement notifying an individual of the right to restrict disclosures of PHI to a health plan if the individual has paid out-of-pocket in full for the health care resulting in the PHI; and
- If fundraising is involved, a statement regarding an individual's right to opt out of receiving such communications.

Breach Assessment

The Final Rule eliminates the previous "risk of harm" standard used to determine whether an impermissible use or disclosure of unsecured PHI resulted in a "breach" and, alternatively, creates the presumption that such an incident is a breach unless the covered entity or BA demonstrates that there is a low probability that the PHI was compromised. Accordingly, the covered entity or BA must conduct a risk assessment that considers at least the following four factors:

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

Penalties

The Final Rule incorporates the following increased and tiered civil monetary penalty structure adopted by the HITECH Act:

- 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; and
- 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.

Next Steps

Covered entities and BAs should begin preparing for timely compliance with the Final Rule by September 23, 2013:

- Covered entities must revise and distribute new NPPs.
- Covered entities must comply with new breach notification requirements.
- BAs must achieve full compliance with the HIPAA Security Rule.
- Covered entities and BAs should review and revise HIPAA Privacy and Security policies and procedures.
- Individual authorizations must be modified, as applicable, to address marketing communications and sale of PHI.
- Unless "grandfathered", BA agreements must be executed, as necessary to comply with the Final Rule. This includes BAs bringing their subcontracts into compliance.

Covered entities and BAs with existing BA agreements that comply with the prior provisions of the HIPAA Rules have until either when the agreement is renewed or modified following September 23, 2013, or, at the latest, September 23, 2014, to come into full compliance with the Final Rule.

If you have any questions regarding these new requirements, please contact a member of the health care practice group of Locke Lord LLP. Our health care attorneys have the experience to assist you with HIPAA and HITECH compliance and audit preparedness.

About the Authors

Tammy Ward Woffenden
512-305-4776
twoffenden@lockelord.com

Lane Wood
214-740-8513
lwood@lockelord.com

Jennifer Rangel
512-305-4745
lwood@lockelord.com

Jan Reimann Newsom
214-740-8639
jnewsom@lockelord.com

Scan this code with your device's QR reader to learn more about Locke Lord's Healthcare practice.