Outline of Key Changes to the HIPAA Privacy, Security, Enforcement and Breach Notification Rules

By Boris Segalis, CIPP/US

Editor’s Note: This content comes from the InfoLawGroup post New HIPAA/HITECH Rules Implementation Roadmap: Countdown Begins to September 23, 2013 Compliance Deadline with the author’s permission.

Overview of the New Rules

The changes that the Rules bring for most organizations include:

- The expansion of the definition of Business Associates to include subcontractors that access PHI;

- The imposition of direct liability under the Rules on Business Associates for compliance with certain HIPAA Privacy and Security Rule requirements;

- Additional and revised provisions that covered entities and Business Associates must include in their BAAs, and a requirement for all existing BAAs to comply with the new Rules by September 22, 2014;

- Additional disclosures in covered entities’ HIPAA Privacy Notices, including informing individuals of their right to be notified of breaches of their PHI;

- Substantial lowering of the threshold for notification of affected individuals in the event of a breach of PHI, and a requirement to conduct a documented risk assessment in the event notification is not provided in reliance on the harm threshold; and

- An expansion of individuals’ rights to access their PHI.

Several other significant changes are primarily relevant to covered health care providers and certain non-covered third parties. These changes include:

- Individuals’ enhanced ability to restrict disclosures of certain PHI; this revision affects mostly covered health care providers;
• Restrictions on the circumstances in which adherence programs can be conducted without individuals’ authorization; these changes are most relevant to pharmacies and adherence communications providers and their service providers, and non-covered organizations that sponsor adherence communications; and

• Clarification of the circumstances in which providers of patient health record portals are subject to HIPAA; these requirements primarily concern covered and non-covered portal owners, sponsors and operators.

We address these requirements in detail below:

**Business Associate Definition Scope Expansion**

The Rules clarify the circumstances in which vendors are deemed to be Business Associates, and expand the definition of “Business Associate” to include most subcontractors that access PHI.

**Vendors**

The Rules clarify that vendors that require “routine” or “more than random” access to PHI are Business Associates, while those that act as “mere conduits” for or have “random access” to PHI continue to be outside the scope of the definition. This distinction is not based on whether a vendor or a subcontractor has an “opportunity” to access the data, but rather on whether that opportunity is “transient” or “persistent,” with persistent opportunity more likely to deem a vendor a Business Associate. While entities that are “mere conduits” for PHI are not Business Associates, the Rules emphasize that this exception is narrow. It is limited to entities providing data transmission services, including services that involve temporary storage of PHI that is incident to the transmission, i.e., courier services and their electronic equivalents, such as ISPs or telecoms.

For those looking for clarity, the HHS notes that the determination of whether access to PHI is “routine” or “more than random” is fact-specific, based on (1) the nature of the services and (2) the extent to which the vendor needs access to the PHI to perform the services. The HHS expects to issue additional guidance on the types of entities that are and are not Business Associates under the Rules.

Examples of vendors that are likely to be deemed Business Associates include:

• Providers of data transmission services, to the extent they require “routine access” to the PHI;

• Data storage or document storage vendors – whether or not they view the PHI they maintain;

• Operators of portals or other interfaces created on behalf of covered entities that allow patients to share their data with the covered entity; and

• Entities that provide oversight and governance for electronic health information exchanges.

**Subcontractors**

The Rules also deem a Business Associate any subcontractor to the extent the subcontractor requires access to PHI (a “subcontractor” is an agent or other person other than a member of the workforce to whom a Business Associate delegates a covered function or activity). The “access” analysis applicable to first tier vendors applies equally to subcontractors. Importantly, a subcontractor that accesses PHI for the purposes of the Business Associate’s own management or administration or legal compliance does not itself become a Business Associate by virtue of such access. While subcontractors whom the Rules deem Business Associates have direct obligations to
comply with the Security Rule and certain provisions of the Privacy Rule, the new Rules continue to require Business Associates to obtain assurances of confidentiality of the PHI from non-Business Associate subcontractors.

Hybrid Entities

The Rules now require hybrid entities to include within the covered component of the entity Business Associate-like functions that were previously outside the covered component. An example of a hybrid entity includes an organization that is not generally in the business of providing health care, but, for example, operates on-site health clinics.

Suggested Action Items

- Inventory vendors that provide services to the cover entity; Business Associates should in turn inventory their subcontractors;
- Determine whether the vendors are Business Associates under the revised Rules;
- Review whether each vendor or subcontractor requires access to PHI to perform services for the covered entity or first tier vendor, or whether the access should be curtailed or data de-identified;
- Enter into Business Associate agreements with vendors and subcontractors that have become Business Associates under the Rules;
- Consider reminding vendors/subcontractors about their obligation to review the Rules and ensure compliance with the relevant Privacy and Security requirements; and
- Examine internal health-care related operations, such as on-site clinics and health care plans, to ensure that Business Associate-like functions are brought within the covered components of those organizations.

Direct Applicability of Certain Privacy and Security Requirements to Business Associates

Direct Applicability of Security Rule Requirements

The new Rules make Business Associates directly responsible to regulators for complying with the Security Rule. The HHS does not view this direct extension of liability as burdensome to Business Associates because, previously, covered entities were required to flow the requirements of the Security Rule to Business Associate via a contract.

Direct Applicability of Certain Privacy Rule Requirements

The Rules require Business Associates to:

- Use or disclose PHI only as permitted or required by the BAA or required by law; any other use or disclosure of PHI would be a violation of the HIPAA Privacy Rule for which the Business Associate would be directly liable (such a violation would likely be deemed a breach subject to the requirement to notify affected individuals);
- Not use or disclose PHI in a manner that would violate the Privacy Rule if done by the covered entity;
- Disclose PHI when required by the HHS to investigate or determine the Business Associate’s compliance with HIPAA/HITECH;
• Disclose PHI to the covered entity, or to the individual or individual’s designee to facilitate compliance with the individual’s request for his or her electronic PHI;

• Provide an individual or the individual’s designee with a copy of their PHI in an electronic format, if the individual so chooses, to the extent the entity maintains PHI in an electronic health record;

• Limit the PHI that Business Associates use, disclose or request to the minimum necessary to accomplish the intended purposes of the use, disclosure or request; and

• Respond to known noncompliance with the Rules or BAA restrictions by their Business Associate subcontractors.

As a result, Business Associates are directly liable under the Rules for failures to fulfill these responsibilities, including:

• Uses and disclosures of PHI that are inconsistent with the relevant BAA or with the Privacy Rule;

• Uses and disclosures of PHI that would violate the Privacy Rule if done by the covered entity;

• Failure to disclose PHI when required by the Secretary of the HHS to investigate and determine the Business Associate’s compliance with the Rules;

• Failure to disclose PHI to the covered entity, or to the individual to whom the information pertains, or the individual’s designee, as necessary to fulfill covered entity’s obligations to provide the information to the individual;

• Failure to make reasonable effort to limit PHI to the minimum necessary to accomplish the intended purposes of use or disclosure of, or request for, the PHI;

• Failure to enter into a BAA with subcontractors that access PHI on their behalf; and

• Failure to take reasonable action in response to a covered subcontractor’s noncompliance with the Rules or the requirements of the BAA.

Business Associates’ direct liability for violations of the Privacy Rule continues to be limited, and, except as articulated above, liability for Privacy Rule obligations that a covered entity may delegate to a Business Associate remains contractual to the covered entity.

Suggested Action Items

• Business Associates should review the Rules’ relevant provisions and ensure that they have the policies, procedures and processes in place to comply with the privacy and security requirements for which they are directly liable under the Rules;

• Business Associates should ensure that they have processes in place to monitor their covered subcontractors’ compliance with the Rules’ and the limitations of the BAAs, and mechanisms in place to take measures to address noncompliance;

BAA Updates
**Key Date**

While the Rules make significant changes to BAA requirements, covered entities and Business Associates (and Business Associates and their subcontractors) may continue to operate under existing agreements until *September 22, 2014*.

**Requirements**

The Rules now require Business Associates to enter into BAAs with their subcontractors pursuant to the same requirements that apply to covered entities with respect to their first tier vendors. The Rules do not require covered entities to enter into BAAs with their covered subcontractors.

Further, the Rules modify the provisions that govern the content of BAAs, mandating that BAAs:

- Require Business Associates that carry out covered entity’s obligations under the Privacy Rule to comply with the requirements of the Privacy Rule that are applicable to that obligation;
- Require Business Associates to comply, where applicable, with the Security Rule in handling PHI;
- Require Business Associates to ensure that any subcontractors enter into a contract or other arrangements to protect the security of PHI; and
- Require Business Associates to report security incidents to covered entity “as required by Section 164.410 of the breach notification rules.”

**Suggested Action Items**

- Covered entities and Business Associates should prepare and update BAA form agreements to fit their requirements and comply with the new Rules;
- Identify Business Associates and, for Business Associates, subcontractors that will be required to sign a new or updated BAA;
- Ensure that, going forward, new Business Associate engagements use the updated BAA; and
- Initiate update cycle for BAAs with existing Business Associates to ensure that all BAAs are up to date by September 22, 2014.

**HIPAA Privacy Notice Updates**

The Rules introduce several new requirements for content of HIPAA Privacy Notices and mandate the redistribution of the updated notices.

**Additional Requirements for HIPAA Privacy Notices**

In addition to the existing HIPAA Privacy Rule requirements, the new Rules require the HIPAA Privacy Notice to inform individuals that:

- They have a right to be notified following a breach of their unsecured PHI;
- They may be contacted to raise funds and have the right to opt out of receiving such communications;
• Most uses of and disclosures of PHI for marketing purposes and sales of PHI require the individual’s authorization (entities that record or maintain psychotherapy notes also must state specifically that most uses or disclosures of such notes require the individual’s authorization);

• Uses and disclosures not described in the Privacy Notice will be made only with the authorization from the individual; and

• Covered health care providers must state in their Privacy Notices that individuals have the right to restrict certain disclosures of PHI to a health plan when the individual (or any person other than the health plan) pays for treatment at issue out of pocket in full.

Redistribution of HIPAA Privacy Notices

The Rules deem the revisions to HIPAA Privacy Notices “material,” and therefore, require redistribution of the updated HIPAA Privacy Notices. Accordingly, pursuant to the existing HIPAA Privacy Rule, covered entities must (1) prominently post the revised Privacy Notice (or a summary linked to the notice) on their site by the effective date of the changes (i.e., September 23, 2013 at the latest), and (2) provide the revised Privacy Notice in the covered entity’s next annual mailing to affected individuals. If the notice is not provided via a website, the covered entity must provide it to affected individuals within 60 days of the effective date of the updated notice.

Suggested Action Items

• Update HIPAA Privacy Notice to comply with the new Rules;

• Verify that the notice accurately reflects the covered entity’s actual practices;

• Determine the appropriate mechanism for redistributing the Privacy Notice; and

• Redistribute the Privacy Notice within the appropriate timeframe.

Breach Notification Requirement Update

The Rules introduce comprehensive updates to the requirements governing the investigation and response to potential breaches of electronic PHI. Specifically, the Rules lower the threshold for notification of affected individuals in the event of unauthorized access to PHI by:

• Abandoning the current harm threshold that required notification only if the individuals affected by a breach were exposed to a “significant risk of financial, reputation or other harm;” and instead

• Presuming that notification is required in all circumstances, except when:

- The covered entity conducts a risk assessment that establishes that there is a “low probability” of compromise of the PHI; or
- One of the existing exceptions to the definition of the breach applies (i.e., unintentional good faith acquisition, access, or use of PHI by a workforce member; inadvertent disclosure between two individuals who are otherwise authorized to access the PHI; or disclosure to an unauthorized person who would not reasonably have been able to retain such information).
The required risk assessment to determine the probability of PHI compromise must be thorough, completed in good faith, and reach conclusions that are reasonable. To meet these requirements, the risk assessment must consider at least:

- The nature and extent of the PHI involved (i.e., types of identifiers, likelihood of re-identification, and the amount of data and its sensitivity);
- The type of unauthorized person who used the PHI or to whom the data was disclosed;
- Whether the PHI was actually acquired or viewed; and
- The extent to which risk to the PHI has been mitigated.

The Rules provide detailed guidance on considering and weighing these factors. The HHS indicated that it will issue further guidance on conducting risk assessments of frequently-occurring scenarios.

**Suggested Action Items**

- Revise PHI breach investigation and notification policies, procedures and processes to ensure compliance with the new, lower notification threshold; and
- Implement a process to conduct and document risk assessments for determining the probability of PHI compromise in the event of a breach.

**Revised Restriction on Sale of PHI**

The Rules define the sale of PHI as any disclosure of the information for which the covered entity or Business Associate receives remuneration from or on behalf of the recipient. Such remuneration may be direct or indirect, and financial or non-financial. The Rules prohibit such sales, except with a written authorization of the individual to whom the PHI pertains. The authorization must explain (in terms left to the disclosing entity’s discretion) that the disclosure will result in the covered entity or Business Associate receiving remuneration for the PHI.

The Rules permit disclosures of PHI without the individual’s authorization pursuant to several exceptions, such as:

- Disclosures by a Business Associate in connection with performance of services for a covered entity (or by a subcontractor for a first tier Business Associate vendor);
- Disclosures to individuals to whom the PHI pertains to comply with the individual’s request for access to the PHI or accounting for the disclosure of the information;
- Disclosures of PHI required by law;
- Disclosures associated with grants or other arrangements to perform studies; and
- Certain disclosures for public health purposes and for research purposes (if the remuneration reflects a reasonable fee to cover the cost of data preparation and disclosures).

Entities that disclose PHI, should verify that the disclosures do not constitute a “sale” under the new Rules. The revised requirements will apply to any disclosures after September 25, 2013.
Fundraising Restrictions

The Rules require fundraising communication to include a method for the recipient to opt out from receiving such communications. The opt-out methods may not burden recipients with more than nominal cost, and may include a toll-free number or an email address, but not a requirement to write and send a letter, for example, which would be considered too burdensome.

The Rules also clarify that the PHI that may be used for fundraising purposes is limited to individuals’ names, addresses, other contact information, age, gender, date of birth, dates during which the individual received the relevant health care, general department of treatment, and treatment outcome information.

The Rules prohibit conditioning of treatment or payment on the individual’s choice with respect to receiving fundraising communications.

Marketing – Changes in Adherence Communications Requirements

The new Rules require authorization for all treatment and health care operations communications where the covered entity or the covered entity’s Business Associate receives financial remuneration specifically for making the communication from a third party whose product or service is being marketed. The Rules, however, exempt from this authorization requirement refill reminders or communications about a drug or biologic agent currently being prescribed to the individual. The HHS clarified that “adherence communications encouraging individuals to take their prescribed medications as directed fall within the scope of the exception.” However, for this exception to apply, the financial remuneration for sending the communication must be “reasonably related” to the cost of making the communication, i.e., limited to the costs of drafting, printing and mailing the communications, and associated costs. If, however, the remuneration includes an additional payment (e.g., to encourage covered entity’s or its Business Associate’s continued willingness to send the communications), the exception likely will not apply, and the patient’s authorization will be required to send the communications.

Notably, the new Rules represent a departure from the HHS’s previous characterization of adherence communications in 2002, when the agency did not agree that “the simple receipt of remuneration should transform a treatment communication into a commercial promotion of a product or service.... For example, health care providers should be able to, and can, send patients prescription refill reminders regardless of whether a third party pays or subsidizes the communication. The covered entity also is able to engage a legitimate business associate to assist it in making these permissible communications.”

In addition to the HIPAA/HITECH Rules, adherence communications may also be subject to state laws, such as the California Confidentiality of Medical Information Act (CMIA), which is more restrictive than HIPAA/HITECH and is not preempted by the federal rules. The practice is also subject to self-regulatory requirements of the National Consumer League’s (NCL’s) Best Practices for Pharmacy Direct to Patient Communications.

Suggested Action Items

- Covered entities and Business Associates that provide adherence communications should examine their programs to ensure continued compliance with the new Rules, as well as with existing requirements under state laws and self-regulatory requirements.
Organizations that subsidize or provide adherence communications will need to examine the financial aspects of their relationships to ensure that the programs do not require individuals’ authorization under the new Rules.

**Expansion of Individuals’ Rights**

The Rules expand individuals’ rights to restrict certain disclosures of their PHI and enhance individuals’ access to their PHI.

*PHI Disclosure Restrictions – Applicable Primarily to Covered Health Care Providers*

The Rules specifically require covered entities to comply with individuals’ requests to restrict the disclosure of their information; to the extent the disclosure satisfies three conditions:

- The disclosure is for purposes of carrying out payment or healthcare operations;
- The disclosure is not otherwise required by law or regulations (including Medicare, Medicaid, and other requirements); and
- The PHI subject to the request pertains solely to a health care item or service for which the individual (or family member, or anyone other than the health plan) paid in full.

The requirement to restrict disclosure would also bar disclosures to Business Associates. Under the Rule, the individual retains the discretion to determine for which services he or she wants to pay out of pocket.

A disclosure of PHI in violation of this requirement would violate the Privacy Rule and, therefore, potentially trigger breach response and notice obligations.

*Enhanced PHI Access Rights*

The Rules require covered entities to provide an individual or the individual’s designee with access to the individual’s PHI, if an individual requests an electronic copy of his or her PHI that a covered entity maintains in the ordinary course of business.

Covered entities must produce the information in the form and format requested by the individual to the extent it is readily producible in such form and format. Otherwise the PHI must be provided to the individual in another agreed-upon computerized format, such as MS Word or Excel, text, HTML or PDF. A covered entity that uses or maintains electronic health records with respect to the requested information must provide a copy of the information in an electronic format.

The rule establishes a 30-day period (with an extension available under certain circumstance) for covered entities to comply with an access request, and allows covered entities to charge certain reasonable fees to produce the information.

One of the key goals of the enhanced access rights is to allow individuals better access to electronic health records and to facilitate individuals’ ability to direct the transmission of their records to, for example, an online portal on which the individual maintains her personal health records.

*Suggested Action Items*
• With respect to individuals’ right to restrict the disclosure of their information, covered entities (particularly, health care providers) should ensure that their policies are consistent with the new Rules and that they have implemented the technical means to comply with individuals’ preferences.

• The enhanced access requirements should prompt covered entities to ensure that they have the technical means to provide copies of individuals’ electronic PHI in an appropriate electronic format consistent with the Rules’ requirements.

PHR Portals

The Rule clarifies that companies that offer personal health record services (e.g., personal health information storage portals) directly to individuals are not subject to HIPAA, while those that offer such services on behalf of covered entities are Business Associates. The HHS notes that companies that offer services directly to individuals will not become Business Associates by virtue of entering into interoperability relationships with covered entities to enable consumers to share their information with covered entities, or for covered entities to provide data to a portal, for example, pursuant to the individual’s written authorization.

The HHS observed that health information portals represent a new opportunity that will likely call for additional guidance in the future.

Final Thoughts

The new Rules represent an evolution in enhancing the protection of and access to PHI. While this is a comprehensive update that will require a significant implementation effort, the HHS has made it clear that it intends to issue further guidance on many aspects of the new Rules. Thus covered entities, Business Associates and other organizations that come in contact with health information should continue to monitor this space closely. The OCR listserve is a good resource for staying current.

Boris Segalis is a partner at InfoLawGroup LLP. He counsels clients on data confidentiality, privacy, security and management issues.