EPSTEIN BECKER GREEN | IMPLEMENTING HEALTH AND INSURANCE REFORM: *Opportunities & Challenges for Your Organization*

HEALTH CARE & LIFE SCIENCES | *Thought Leaders in Health Law®*

January 19, 2013

# Overview of Modifications to the HIPAA Privacy, Security, and Enforcement Rules

**RESOURCE LINKS**

**Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules: https://federalregister.gov/a/2013-01073**

**IMPORTANT DATES**

***March 26, 2013*: HIPAA rule becomes effective.**
***September 23, 2013:* Covered entities and their business associates have until this date to comply.**

On January 17, 2013, the Department of Health and Human Services released the highly anticipated, 563 page, Health Insurance Portability and Accountability Act ("HIPAA") regulations (the "Final Rule") that have been delayed for over 3 years. The Final Rule will be published in the Federal Register on January 25, 2013. The Final Rule addresses many of the compliance issues and unanswered questions facing covered entities and business associates. The effective date of the Final Rule is March 26, 2013--with a compliance date (for most provisions) by September 23, 2013 (there is an additional grace period for certain provisions). Epstein Becker Green is preparing an in-depth analysis of the Final Rule which will be forthcoming. In the meantime, below is a high level summary of the significant changes included in the Final Rule.

## *I. Changes to the Business Associate Relationship*

The Rule affects the business associate relationship by:

### 1. Expanding the Definition of Business Associates:

The Final Rule explicitly expands the definition of business associates to include: Health Information Organizations; E-prescribing Gateways; other entities that provide data transmission services for covered entities and that require access on a routine basis; entities that offer a personal health record to individuals on behalf of a covered entity; and subcontractors.

### 2. Clarifying Those Provisions that Apply to Business Associates and Clarifying the Direct Liability of Business Associates

As noted in the preamble to the Final Rule, the Final Rule clarifies the provisions in the Privacy and Security Rules that apply directly to business associates (for example complying with certain Security Rule requirements). In addition, the preamble notes that direct liability applies to business associates for failing to comply with those provisions. Additional provisions that create direct liability for business associates include a failure to:

- Comply with the terms of a business associate agreement related to the use and disclosure of Protected Health Information ("PHI");
- Provide of PHI to the Secretary upon demand;
- Provide of an electronic copy of PHI available to an individual (or covered entity) related to an individual's request for an electronic copy of PHI;
- Make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request; and
- Enter into business associate agreements with subcontractors that create or receive PHI on their behalf.

**3. Extending Business Associate Requirements to Subcontractors**

The Final Rule expressly states that subcontractors of business associates are also "business associates." Under the Final Rule, a subcontractor is any person or entity "delegated a function, activity, or service the business associate has agreed to perform for a covered entity or business associate." Business associates are obligated to enter into agreements with subcontractors in accordance with the requirements for business associate agreements.

**4. Providing an Agent/Principal Analysis for Business Associates**

The Final Rule and preamble make clear that, in certain circumstances, vicarious liability for a regulatory violation will attach to covered entities based on agency rules. The test for determining if a business associate constitutes an agent of the covered entity is whether the covered entity has the "right or authority to control the business associate's conduct in the course of performing a service on behalf of the covered entity," regardless of the terms of a business associate agreement. For liability to attach to a covered entity for the actions of its business associate, in addition to determining that the business associate is an agent of the covered entity, the business associate must have also been acting within the scope of the agency/principal relationship. This represents a change in the long standing position that covered entities are not "their brother's (business associate's) keepers."

**5. Requiring Changes to Business Associate Agreement Provisions**

Additionally, the Final Rule revises the business associate agreement provisions of the Privacy and Security Rules. In response to concerns about the administrative burden in implementing these provisions, the Final Rule provides for a one-year transition period, during which covered entities and business associates (and business associates and business associate subcontractors) may continue to operate under certain existing contracts.

## *II. Adopting Increased Civil Monetary Penalties*

The Final Rule also adopted the higher penalties for violations of HIPAA as proposed under the Health Information Technology for Economic and Clinical Health ("HITECH") Act. Under the Final Rule, monetary penalties for violations of HIPAA will be assessed based on the following table:

| Violation Category | Each Violation | Maximum for All Such Violations of an Identical Provision in a Calendar Year |
|---|---|---|
| (A) Did Not Know | $100 - $50,000 | $1,500,000 |
| (B) Reasonable Cause | $1,000 - $50,000 | $1,500,000 |
| (C)(i) Willful Neglect-Corrected | $10,000 - $50,000 | $1,500,000 |
| (C)(ii) Willful Neglect-Not Corrected | $50,000 | $1,500,000 |

The preamble notes that the manner in which the Office of Civil Rights ("OCR") counts violations could result in penalties higher than the $1.5 million limit that is reflected in the chart. For example, a security breach could constitute both an impermissible use/disclosure as well as a violation of the requirement to institute appropriate safeguards, resulting in possible penalties of up to $3 million.

Penalties are also assessed based on consideration of certain factors such as:

- The nature and extent of the violation, including consideration of:
  - the number of individuals affected; and
  - the time period during which the violation occurred.
- The nature and extent of the harm resulting from the violation, including consideration of:
  - whether the violation caused physical harm;
  - whether the violation resulted in financial harm;
  - whether the violation resulted in harm to an individual's reputation; and
  - whether the violation hindered an individual's ability to obtain health care.
- The history of prior compliance with the administrative simplification provisions, including violations, including consideration of:
  - whether the current violation is the same or similar to previous indications of noncompliance;
  - whether and to what extent there have been attempts to correct previous indications of noncompliance;
  - responses to technical assistance from the Secretary provided in the context of a compliance effort; and
  - response to prior complaints.
- The financial condition of the covered entity or business associate, including consideration of:
  - financial difficulties that affected the ability to comply;
  - whether the imposition of a civil money penalty would jeopardize the ability to continue to provide, or to pay for, health care; and
  - the size of the covered entity or business associate.
- Such other matters as justice may require.

## *III. Definitional Changes*

### 1. Definition of Electronic Media – Covered Transmissions

The Final Rule provides a new definition of the phrase "electronic media" with the new definition excluding the transmission of PHI via paper, facsimile, voice, or telephone "if the information being exchanged did not exist in electronic form immediately before the transmission." The Final Rule makes clear, however, that PHI stored on photocopiers or facsimile machines is covered by HIPAA and covered entities and business associates must ensure that the PHI stored on these devices is protected from unauthorized access.

**2. Definition of Marketing**

The Final Rule expands upon the requirement of the HITECH Act and removes certain communications from a long-standing exception to marketing under the Privacy Rule. As a result, the Final Rule now requires an individual authorization prior to making any treatment and health care operations communications, if those communications involve financial remuneration for making the communications from a third party whose product or service is being marketed. However, the exceptions for face-to-face communications and promotional gifts of a nominal value are maintained. The Final Rule also incorporates (from the HITECH Act) the exceptions for refill reminders, and maintains the exceptions for communications promoting health in general that do not promote a product or service from a particular provider, and communications about government and government-sponsored programs.

## *IV. Research Authorization Changes*

The Final Rule amends requirements for authorizations related to research. Specifically, the Final Rule allows a covered entity to combine conditioned and unconditioned authorizations for research as long as the authorization clearly differentiates between the conditioned and unconditioned research components and clearly allows the individual the option to opt in to the unconditioned research activities. The Final Rule also modifies a prior interpretation that research authorizations must be study-specific.

## *V. Prohibition on Receiving Remuneration for the Disclosure of PHI*

The Final Rule prohibits a covered entity or business associate from receiving direct or indirect remuneration in exchange for the disclosure of PHI unless the covered entity has obtained an individual's valid authorization. The Final Rule clarifies that "remuneration" includes both nonfinancial and financial benefits. Nevertheless, the Final Rule includes several exceptions to the prohibition including those disclosures made:

- for public health purposes;
- for certain research purposes;
- for treatment and payment purposes;
- that are related for sale, transfer and merger activity;
- for business associate activities (that are otherwise in compliance with the Privacy Rule);
- to individuals when requested;
- as required by law; and
- that otherwise fit into the requirements of the Privacy Rule.

## *VI. Requirements for Notices of Privacy Practices*

The Final Rule makes significant changes to requirements regarding covered entities' Notice of Privacy Practices. In particular, the Final Rule now requires a covered entity to include in its Notice of Privacy Practices:

- Certain statements in the notice regarding uses and disclosures that require authorization;
- A statement about fundraising communications and an individual's right to opt out of receiving such communications;
- Information about an individual's right to restrict certain disclosures of PHI to a health plan where the individual pays out of pocket in full for the health care item or service (only health care providers are subject to this requirement); and
- A statement of an affected individual's right to be notified following a breach of unsecured PHI.

## *VII. Changes to Individual Rights*

### 1. Specific Disclosures Allowed

The Final Rule makes several amendments to the Privacy Rule to allow specific disclosures. For example, the Final Rule adopts the proposal to permit covered entities to disclose a decedent's PHI to family members and others who were involved in the care or payment for care of the decedent prior to death, unless doing so would be inconsistent with any known preference of the individual. The Final Rule also permits a covered entity to disclose proof of immunization to a school where law requires the school to have such information prior to admitting the student. Covered entities need to first obtain agreement, which may be oral, before disclosing such information. Moreover, the Final Rule generally adopts proposals to allow a covered entity to use or disclose to a business associate or institutionally related foundation certain PHI from an individual for the covered entity's fundraising, without his or her authorization.

### 2. Individuals' Requests to Restrict Disclosure of PHI

The HITECH Act requires covered entities to comply, in certain situations, with an individual's request to restrict disclosure of his or her PHI. The Final Rule implements this provision of the HITECH Act. Specifically, a covered entity must comply with such a request when (1) it involves disclosure to a health plan or its business associate, (2) the purpose of the disclosure is to carry out payment or health care operations and is not otherwise required by law, and (3) the PHI pertains only to a health care item or service for which the individual (or person on behalf of the individual) has paid the covered entity in full.

### 3. Strengthening Individuals' Access to PHI

The Final Rule strengthens a provision in the Privacy Rule regarding an individual's right to access his or her PHI. Specifically, the Final Rule amends the previous rules to require that, if an individual requests an electronic copy of PHI that is maintained electronically in one or more

designated record sets, the covered entity must provide him or her with access to the information in the electronic form and format requested by the individual. Moreover, if requested by an individual, a covered entity must transmit the copy of PHI directly to another person designated by the individual.

### *VIII. Modifications to the Breach Notification Rule Under the HITECH Act*

The Final Rule has expanded the definition of "breach." Under the Final Rule, any impermissible use or disclosure of PHI is presumed to be a "breach." Accordingly, breach notification is required in all situations except when the covered entity or business associate can demonstrate that there is a low probability that the information has been compromised.

Significantly, the Final Rule eliminates the harm standard which allowed entities to avoid notification if they could demonstrate that the breach posed no significant risk of harm to the individual. Instead, under the Final Rule, breach notification may be avoided if the entity can demonstrate through a risk assessment that there is a low probability that the PHI has been compromised. The Final Rule further provides the factors that must be used in the risk assessment. These include:

- 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.

### *IX Modifications to the HIPAA Privacy Rule under GINA*

The Final Rule expressly incorporates "genetic information" into the definition of PHI and prohibits the use or disclosure of genetic information for underwriting purposes to all health plans that are covered entities (with the exception of issuers of long term care policies). With respect to group health plans, health insurance coverage, or Medicare supplemental policies, "underwriting purposes" means:

- Rules for, or determination of, eligibility (including enrollment and continued eligibility) for, or determination of, benefits under the plan, coverage, or policy;
- The computation of premium or contribution amounts under the plan, coverage, or policy;
- The application of any pre-existing condition exclusion under the plan, coverage, or policy; and
- Other activities related to the creation, renewal, or replacement of a contract of health insurance or health benefits.

## Conclusion

The Final Rule significantly changes the requirements for compliance among both covered entities and business associates. The effective date of the Final Rule is March 26, 2013 – with a compliance date (for most provisions) by September 23, 2013 (there is an additional grace period for certain provisions). EBG attorneys will continue to monitor and review the Final Rule to assist organizations

in determining how to make the requisite changes to their policies, procedures, and practices in order to come into compliance with the Final Rule.

*****

*This summary was prepared by Brandon Ge and Ophir Stemmer.*

For assistance with your Privacy and Security compliance needs, please contact one of the attorneys below or the member of the firm who normally handles your legal matters.

**Mark E. Lutes**
Member of the Firm
Epstein Becker Green
Washington, D.C.
(202) 861-1824
MLutes@ebgaw.com

**Robert J. Hudock**
Member of the Firm
Epstein Becker Green
Washington, D.C.
(202) 861-1893
RHudock@ebglaw.com

**Patricia M. Wagner**
Member of the Firm
Epstein Becker Green
Washington, D.C.
(202) 861-4182
PWagner@ebglaw.com

If you would like to be added to our mailing list, please click here, complete the form below or contact:

Lisa C. Blackburn
Business Development Manager
National Health Care and Life Sciences Practice
Epstein Becker & Green, P.C.
1227 25th St., NW, Suite 700
Washington, D.C. 20037
phone 202/861-1887 – fax 202/296-2882
lblackburn@ebglaw.com

Name:_____ Title:_____

Company/Firm/Organization:_____

Street Address:_____

City:_____ State:_____ Zip Code:_____

Phone No.:_____ Fax No.:_____

E-mail Address:_____