

## Proposed Modifications to HIPAA Rules

On Wednesday, July 14, 2010, the Department of Health and Human Services (HHS) published its notice of proposed rulemaking entitled “Modifications to the HIPAA Privacy, Security, and Enforcement Rules under the Health Information Technology for Economic and Clinical Health Act” (HITECH). In addition to implementing many of the requirements set forth in HITECH, HHS proposed many changes to HIPAA beyond those expected under HITECH.<sup>1</sup> This alert does not provide a comprehensive list of all proposed changes. We encourage you to attend our webinar on July 29, 2010 for a more detailed overview and analysis of the proposed changes.

### Compliance Period:

- HHS proposes a 180 day general compliance period after the effective date of the final rule;
- Covered entities and business associates may also take advantage of an extended compliance period (discussed below) to bring business associate contracts into compliance.

### Select Changes for Business Associates:

- The proposed rule would clarify that the HIPAA Security Rule’s administrative, physical, and technical safeguards requirements and the Security Rule’s policies and procedures requirements now apply to business associates;
- Similarly, the proposed rule would clarify that many of the standards, requirements, and implementation specifications of the HIPAA Privacy Rule now apply to business associates;
- The definition of business associate would be expanded to include subcontractors of business associates, thereby making subcontractors subject to the HIPAA Privacy and Security rules in the same manner as business associates.

### Select Changes for Business Associate Agreements:

- The proposed rule would require business associate agreements to specify that business associates must comply, where applicable, with the Security Rule with regard to electronic PHI;
- Business associate agreements would have to require business associates to report breaches of unsecured PHI to the covered entity;

---

<sup>1</sup> HITECH introduced a number of important and new obligations for covered entities and their business associates under HIPAA. These new obligations include:

- Applicability of certain components of the HIPAA Privacy and Security rules to business associates;
- The requirement that covered entities and business associates provide notification to certain persons in the event of a breach of unsecured PHI;
- Establishment of new limitations on use and disclosure of PHI for marketing and/or fundraising purposes;
- Prohibition on the sale of PHI with limited exceptions;
- Establishing the use of a limited data set as meeting the minimum necessary standard for disclosure;
- Expansion of the rights of individuals to restrict disclosures of PHI and to obtain an accounting of disclosures of PHI from covered entities.

- All requirements for contracts between covered entities and business associates would apply in the same manner to contracts/arrangements between business associates and subcontractors.

#### **Extended Compliance Period for Amending Business Associate Agreements:**

- HHS proposes new transition provisions to allow covered entities and business associates (and business associates and business associate contractors) to continue operating under existing compliant contracts, under certain circumstances and if certain conditions are met, for up to one year after the compliance date of the final rules (the compliance date will be 180 days following the effective date of the final rule);
- HHS also proposes inclusion of evergreen contracts in the deemed compliance category even if such contracts automatically roll over after the effective date of the final rule.

#### **Changes to the HIPAA Marketing Rules:**

- Health care operations communications would not be considered marketing unless the communication is in writing and the covered entity receives financial remuneration in exchange for making the communication;
- Financial remuneration would become a newly defined term and would be defined as direct or indirect payment from or on behalf of a third party only when the third party's product or service is being described;<sup>2</sup>
- Marketing would not include communications by a provider for treatment purposes, including case management or care coordination, or to recommend alternative treatments;
  - If a provider receives financial remuneration in exchange for making such communications, the covered health care provider would have to notify patients in the notice of privacy practices (NPP) that such provider, having received remuneration from third parties, may send the individual communications concerning alternative treatments and/or health related products or services;
  - The NPP must also notify the individual of her right to opt out of receipt of such communications.

#### **Select Changes to the Research Authorization Process:**

- The proposed rule would allow combination of a research authorization that conditions research related treatment upon research participation (i.e., a conditioned authorization) with a research authorization that does not condition treatment upon research participation (i.e., an unconditioned authorization), provided that 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 (currently, HIPAA does not permit these so-called compound authorizations).

#### **Select Additional Changes for NPPs:**

- NPPs would have to (1) describe uses and disclosures of PHI requiring authorization by individuals and (2) provide that uses and disclosures not described will be made only with an individual's authorization;
- NPPs would also have to provide notice to individuals of any intention to contact individuals for fundraising purposes and notification of such individuals of their right to opt out of such communications.

<sup>2</sup> For example, while authorization would be required for a covered entity to communicate to patients regarding a new state of the art technology when paid to do so by the manufacturer of the new technology, authorization would not be required if a patient advocacy group were to pay the covered entity to notify patients about the same new technology.

**Other Proposed Changes:**

- Covered entities would be required to provide, with each fundraising communication, an easy opportunity for the individual to opt out of future fundraising communications, which the covered entity must respect (currently, the covered entity only has to make reasonable efforts in this regard);
- The proposed rule would establish that a covered entity is required to protect PHI of a deceased individual only for a period of 50 years following the date of death;
- The proposed rule would also make clear that not all participants in an Organized Health Care Arrangement need to be covered entities.

**Key Areas in which HHS Will Solicit Comments from the Public:**

- HHS encourages comments on whether to modify its past interpretation that authorizations for use/disclosure of PHI for research be study specific;
- HHS also encourages comments on aspects of the minimum necessary standard most in need of clarification (HHS proposes to leave the text of § 13405(b) of HITECH unchanged).

If you would like further information or assistance furnishing comments to HHS, please contact the Ropes & Gray attorney that usually advises you.