

# Highlights of the HIPAA Privacy and Security Rule Changes under the American Recovery and Reinvestment Act

By: **Mark C. Rogers, Esq.**

After seemingly endless debate, the federal economic stimulus package is now a reality. The American Recovery and Reinvestment Act of 2009 (the “Act”) was passed by Congress on February 13, 2009, and signed into law by President Obama on February 17<sup>th</sup>. Health care is a significant focus of the Act. In particular, Title XIII of the Act – Health Information Technology for Economic and Clinical Health Act – sets forth substantial changes to the HIPAA Privacy and Security Rules.<sup>1</sup> These changes mean that providers or “covered entities”<sup>2</sup> will need to amend their existing HIPAA Privacy and Security policies and procedures in order to be in compliance with the Act. This article provides an overview of the Act’s significant amendments to the HIPAA Privacy and Security Rules and how these amendments will affect Massachusetts providers.

## **Business Associates**

The Act requires business associates to comply with the administrative, physical, and technical safeguards of the HIPAA Security Rule. As a result, business associates will be required to develop written policies and procedures pertaining to the security of electronic protected health information (“PHI”). Furthermore, the Act prohibits business associates from using or disclosing PHI that is not in compliance with each of the required terms of a business associate

agreement. The Act provides that business associates who violate the HIPAA security standards or the terms of their business associate agreement will now be subject to the same civil and criminal penalties as the covered entities.

Covered entities will likely need to amend their business associate agreements to require their business associates to comply with the administrative, physical, and technical safeguards of the HIPAA Security Rule and to require that they adopt appropriate written policies and procedures. The U.S. Department of Health and Human Services (“HHS”) is expected to issue regulations specifically addressing what new provisions need to be incorporated into business associate agreements.

## **Accounting of Disclosures**

Covered entities that utilize or maintain electronic health records (“EHRs”) are required under the Act to provide individuals with an accounting of disclosures for disclosures of PHI through an electronic health record (EHR) that relate to treatment, payment, or health care operations. Previously, covered entities were exempt from providing individuals with an accounting of disclosures for such disclosures of PHI. In addition, the Act provides that for disclosures by business associates, the covered entity may provide the accounting or it may direct the individual to the business associate, who must comply

with the accounting of disclosure requirements.

A covered entity may impose reasonable fees on an individual for the production of an accounting of disclosures. However, the fees may not be greater than the covered entity’s labor costs in responding to the request.

The Secretary of HHS (the “Secretary”) is required to adopt standards that will detail what information must be included in accounting of disclosures for treatment, payment, and health care operations. The effective date of this provision of the Act depends upon when a covered entity acquires an EHR. If a covered entity acquired an EHR prior to January 1, 2009, it will not be required to begin making accountings until January 14, 2014. If a covered entity acquires an EHR after January 1, 2009, the effective date for these new accountings will be January 1, 2011. The Secretary may extend these effective dates until 2016 and 2013, respectively.

## **Privacy and Security Breach Notifications**

Prior to the Act, HIPAA did not require a covered entity or business associate to notify an individual about a privacy or security breach related to his/her PHI. The Act now requires a covered entity or business associate to notify individuals whose “unsecured protected health information” has been or is reasonably believed to have

been accessed, acquired, or disclosed as a result of a privacy or security breach. The Act defines “unsecured protected health information” to mean PHI that is not secured through the use of a technology or methodology specified by guidance issued by the Secretary.

On April 17, 2009, the HHS issued the aforementioned guidance specifying the technologies and methodologies that render PHI unusable, unreadable, or indecipherable to unauthorized individuals for purposes of the breach notification requirements under the Act.<sup>3</sup> According to the guidance, PHI is rendered unusable, unreadable, or indecipherable to unauthorized individuals only if it is (i) encrypted by “the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key”; or (ii) the media on which the PHI is stored or recorded has been destroyed.<sup>4</sup>

The Act requires notification to the affected individuals within sixty (60) calendar days of the discovery of the breach. Furthermore, if a breach involves more than 500 residents of a state, a covered entity must provide notice to prominent media outlets serving the state, as well as immediate notice to the Secretary. If a breach includes fewer than 500 individuals, the covered entity must notify the Secretary – but may do so as an annual submission. Pursuant to the Act, all breach notifications must contain the following: (i) a description of the incident, including the date of the breach and the date of the discovery of the breach (if known); (ii) a description of the type of PHI involved in the breach; (iii) guidance on what individuals should do to protect themselves from potential

harm resulting from the breach; (iv) a description of what the covered entity is doing in response to the breach, including how it is mitigating future harm and what it is doing to protect against further breaches; and (v) instructions for how individuals can contact the covered entity to obtain additional information (this should include a toll-free phone number, an email address, website or postal address).<sup>5</sup>

Massachusetts already has a “Security Breach Law” (G.L. c. 93H), which requires covered entities to provide notice to affected Massachusetts residents whose personal information has been subject to a security breach. The Massachusetts law provides that notice must be made “as soon as practicable and without unreasonable delay.”<sup>6</sup> Although the Massachusetts Security Breach Law states that a “person”<sup>7</sup> is not relieved from the duty to comply with the requirements of any applicable general or special federal law regarding the protection and privacy of personal information, it provides that a person who maintains procedures for responding to a breach of security pursuant to federal law is deemed to be in compliance with the Massachusetts Security Breach Law, if the person notifies: (1) Massachusetts residents of a security breach in accordance with the maintained or required procedures; and (2) the Massachusetts Attorney General’s Office and the Massachusetts Office of Consumer Affairs and Business Regulation.<sup>8</sup>

### **Requests for Privacy Restrictions**

HIPAA currently provides that a covered entity has the discretion to not agree to comply with an individual’s request to restrict the disclosure of his/her PHI that re-

lates to treatment, payment and health care operations. The Act amends the HIPAA provision to require covered entities to comply with requests from an individual to restrict the disclosure of his/her PHI that relates to treatment, payment and health care operations if: (i) the restriction relates to disclosure to a health plan for purposes of carrying out payment or health care operations; (ii) the restriction does not relate to disclosure to a health plan for the purpose of carrying out treatment; and (iii) the PHI pertains solely to a health care item or service for which the health care provider involved has already been paid out-of-pocket in full.<sup>9</sup>

### **Marketing and Fundraising Communications**

Currently, a covered entity can only issue a marketing communication to an individual with that individual’s prior written authorization, unless such communication meets one of the following exceptions to the definition of marketing under the HIPAA Privacy Rule: (i) a communication made by a covered entity about the entity’s own health related products or services; (ii) a communication for treatment purposes; or (iii) communications for case management or care coordination of the individual or to recommend alternative treatments, therapies, health care providers, or settings of care. A communication that meets one of the above exceptions does not require an authorization from the individual, as the authorization is most likely considered to be for treatment or healthcare operations purposes under the HIPAA Privacy Rule.

The Act provides that a marketing communication is not considered

a healthcare operation unless it meets one of the exceptions to the definition of marketing **and** the covered entity does not receive direct or indirect remuneration for making the communication. If a covered entity does receive direct or indirect remuneration, the communication will not be considered marketing if the communication is for treatment purposes or if: (i) the communication is about a current drug or biologic the recipient is taking and any payment is reasonable as defined by the Secretary; (ii) the communication is made by a covered entity based on a valid HIPAA authorization from the individual; or (iii) the communication is made by a business associate of a covered entity in accordance with a business associate agreement.

The Act requires that any fundraising communications from a covered entity shall state in a “clear and conspicuous manner” that the recipient has the right to opt-out of receiving further fundraising communications.<sup>10</sup> An opt-out by an individual shall be treated as a revocation of authorization under the HIPAA Privacy Rule.

The Act’s restrictions on marketing and fundraising communications pertain to such communications made after February 17, 2010.

### **Electronic Health Record Access**

The Act provides that if a covered entity uses or maintains an EHR with respect to PHI, an individual shall have the right to obtain a copy of his/her PHI in electronic format. This provision of the Act may require covered entities to review their EHR system for necessary technical upgrades.

### **Minimum Necessary**

The Secretary is required to issue guidance within 18 months of the passage of the Act on what the term “minimum necessary” encompasses in terms of the disclosure, use and request of PHI under the HIPAA Privacy Rule.

### **Sale of PHI**

The Act prohibits a covered entity or business associate from directly or indirectly receiving remuneration in exchange for PHI without a valid authorization from the individual that includes a specific authorization as to what PHI may be sold. The prohibition does not apply to the sale of PHI related to:

- Public health activities;
- Research, and the price charged reflects the costs of preparation and transmittal of the data;
- Treatment of the individual;
- Sale, transfer, merger or consolidation of all or part of the covered entity;
- Business associate functions pursuant to a business associate agreement; and
- Providing an individual with a copy of his/her PHI.

The prohibition also does not apply to any activity deemed necessary and appropriate by the Secretary. In accordance with the Act, the Secretary must promulgate regulations pertaining to the prohibition on the sale of PHI.

### **Increased HIPAA Enforcement**

Pursuant to the Act, the Secretary is required to impose a civil penalty for a violation due to willful neglect

and to conduct a formal investigation of any complaint if a preliminary investigation indicates willful neglect. Furthermore, within three (3) years of the enactment of the Act, the Secretary must issue regulations providing a methodology for sharing civil monetary penalties or monetary settlements with individuals harmed by violations. Obviously there is great concern about this provision from the provider perspective as this sharing of monetary settlements and penalties could incentivize individuals to file HIPAA complaints.

### **New Penalties**

The Act significantly increases the civil monetary penalties for violations of both HIPAA and the Act. Currently, HIPAA provides for a \$100 penalty for each violation with a cap of \$25,000 for multiple violations in a given calendar year. The Act amends this to increase the penalty to \$1,000 for each violation “due to reasonable cause and not willful neglect.” with a cap of \$100,000 each calendar year.<sup>11</sup> The Act also provides that if a violation was due to willful neglect, but was corrected, the penalty shall be \$10,000 for each violation with a \$250,000 annual cap.<sup>12</sup> Finally, the Act states that if a violation was due to willful neglect and was not corrected, the penalty shall be \$50,000 for each violation with a \$1,500,000 annual cap.<sup>13</sup>

### **Conclusion**

The Act represents significant changes to the HIPAA Privacy and Security Rules. Massachusetts providers need to review and revise their current privacy and security policies/procedures to ensure compliance with the Act.