

HEALTH CARE PRACTICE GROUP ADVISORY

Stimulus Package Means Changes to Providers' HIPAA Privacy and Security Policies

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 17th. Health care is a significant focus of the Act. In particular, Title XIII of the Act - Health Information Technology for Economic and Clinical Health, sets forth substantial changes to the HIPAA Privacy and Security Rules. These changes mean that providers or "covered entities" will need to amend their existing HIPAA Privacy and Security policies and procedures. This Advisory provides an overview of the Act's major changes to the HIPAA Privacy and Security Rules.

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. Furthermore, the Act prohibits Business Associates from using or disclosing protected health information ("PHI") that is not in compliance with each of the required terms of a Business Associate Agreement. The Act provides that Business Associates which 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 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.

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 that relate to treatment, payment or health care operations. Previously, covered entities were exempted from providing individuals with an accounting for disclosures of PHI related to treatment, payment and health care operations. 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 the United States Department of Health and Human Services (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.

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 their 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 directs the Secretary to issue guidance within sixty (60) days of the Act’s passing on what constitutes “unsecured protected health information”.

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 less than 500 individuals, the covered entity must notify the Secretary – but may do so as an annual submission.

Massachusetts law already requires covered entities to provide notice to affected Massachusetts residents whose personal information has been subject to a security breach. The Massachusetts law (G.L. c. 93H, § 3) provides that notice must be made “as soon as practicable and without unreasonable delay.” The Act does not preempt the Massachusetts law, and therefore, providers in Massachusetts will need to comply with both laws.

Requests for Privacy Restrictions

HIPAA currently provides that a covered entity has the discretion to not comply with an individual’s request to restrict the disclosure of their PHI that relates to treatment, payment and health care operations. The Act amends the HIPAA provision to require covered entities to comply with requests from individuals to restrict the disclosure of their 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.

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 their PHI in electronic format. This provision of the Act may require covered entities to review their EHR system for necessary technical upgrades.

Increased HIPAA Enforcement

Pursuant to the Act, the Secretary will 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 will 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.

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. 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. 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.

Conclusion

The Act represents significant changes to the HIPAA Privacy and Security Rules. Providers need to review and revise their current privacy and security policies/procedures to ensure compliance with the Act. The Rogers Law firm is available to provide these services on a fixed-fee basis. If you have any questions or concerns, please do not hesitate to contact any of the attorneys at The Rogers Law Firm.

This Advisory is published by The Rogers Law Firm to keep you informed of developments in health law. The Advisory should not be construed or relied upon as legal advice or legal opinion on any specific facts or circumstances. If you have any questions or concerns regarding the Advisory or would like legal advice or legal opinion concerning a specific matter, please do not hesitate to contact any of the attorneys at The Rogers Law Firm at 617-723-1100.