Stimulus Package Expands HIPAA Privacy and Security and Adds Federal Data Breach Notification Law

MARCY WILDER, DONNA A. BOSWELL, AND BARBARA BENNETT

The authors discuss provisions of the Stimulus Package that affect covered entities already subject to the HIPAA Privacy and Security regulations and business associates.

Signed into law on February 17, 2009, the Stimulus Package known as the American Recovery and Reinvestment Act of 2009 ("ARRA") expands HIPAA to impose new privacy and security requirements on:

- Covered entities;
- Business associates; and
- Personal health record ("PHR") vendors and various other PHR-related entities.

The new law strengthens and expands the scope of the HIPAA privacy and security rules, enhances the HIPAA penalty provisions, provides for HIPAA enforcement by state attorneys general, regulates PHR vendors, and establishes a federal data breach notification law.

The privacy and security provisions will require substantial operational changes for HIPAA-covered entities and their business associates. This

---

Marcy Wilder, Donna A. Boswell, and Barbara Bennett, attorneys in the Washington, D.C., office of Hogan & Hartson LLP, can be reached at mwilder@hhlaw.com, daboswell@hhlaw.com, and bbennett@hhlaw.com, respectively.

Published in the April 2009 issue of Privacy & Data Security Law Journal.

article focuses on the provisions of the new law that affect covered entities already subject to the HIPAA Privacy and Security regulations ("HIPAA") and business associates.

ENFORCEMENT PROVISIONS ARE ENHANCED AND EXPANDED

Changes to the HIPAA enforcement provisions will require HHS to move away from the voluntary compliance framework currently in use and toward a penalty-based system. The new law requires the Secretary to investigate and impose penalties where violations are due to willful neglect. HHS may continue to use corrective action plans without penalties where there has been no willful neglect. HHS will be required to conduct periodic audits to ensure that covered entities and business associates comply with applicable rules. Funds collected under civil penalties and related settlements are to be provided to the HHS Office for Civil Rights for purposes of further HIPAA enforcement. The Secretary is instructed to establish a methodology by 2012 for distributing a percentage of the monetary penalties collected to individuals harmed by the violations.

The criminal penalties in the HIPAA statute will now apply to business associates as well as directly to employees "or other individuals" provided that the information that has been obtained or disclosed in violation of HIPAA is information maintained by a covered entity. This is widely understood as making clear that employees and recipients, as well as business associates, can be prosecuted for violations of HIPAA, and not just the covered entity.

The various "tiers" of penalties based on different levels of knowledge and/or willfulness have been modified and increased. In addition, state attorneys general ("AGs") have been provided with authority to bring an action parens patriae in federal district court in cases where the AG believes that residents are threatened or damaged by a person who violates the HIPAA Privacy or Security Rules. The AG may seek statutory damages, injunctive relief, and attorneys fees, but cannot institute an action if the Secretary has already done so. Prior to bringing a civil action, the AG must provide notice to the Secretary, who has the right to intervene, to be heard, and to file petitions for appeal.

BUSINESS ASSOCIATES HAVE INCREASED OBLIGATIONS AND ARE DIRECTLY SUBJECT TO CIVIL AND CRIMINAL PENALTIES

Under the new law, business associates will be required to comply with much of the HIPAA Security Rule, including the provisions related to physical, administrative, and technical safeguards and related documentation requirements. Business associates will be required to perform a HIPAA risk assessment and to put in place full-blown HIPAA Security policies; the more general security practices typically required through business associate contracts will no longer be sufficient.

The ARRA imposes new privacy requirements on covered entities (outlined below) and requires that these requirements be passed through to business associates. In addition, business associates will be directly subject to criminal and civil penalties for any use or disclosure of protected health information that is not in compliance with the provisions of the HIPAA Privacy Rule applicable to business associates and imposed through the business associate agreement.

The law also clarifies that Health Information Exchanges and Regional Health Information Organizations are required to enter into Business Associate Agreements with covered entities.

HIPAA PRIVACY AND SECURITY REGULATIONS PROVIDE MORE INDIVIDUAL PROTECTIONS AND IMPOSE ADDITIONAL BURDENS ON BUSINESS

The ARRA makes a number of changes to the HIPAA Privacy and Security Regulations. Highlights are listed below:

Accounting of Disclosures

Long considered among the most difficult provisions with which to comply, the accounting of disclosure provisions have been expanded. In the past, although individuals had a right to obtain an accounting of disclosures, covered entities were not required to account for treatment, payment, and health care operations disclosures — the most common and frequent types.

Published in the April 2009 issue of Privacy & Data Security Law Journal.

That exception has been rescinded for disclosures made through an "electronic health record," a term that is vaguely and broadly defined. For these disclosures, instead of providing an accounting of disclosures made by business associates, a covered entity may refer the requesting individual to its business associates, who would in turn be required to provide the accounting to the individual. HHS is directed to issue regulations on the new accounting for disclosure provisions and the regulatory approach will have a significant impact on just how burdensome these provisions will be to implement.

Minimum Necessary

The Secretary is required to issue guidance on what is the "minimum necessary" information for a permitted disclosure, and until such time as the guidance is issued, there is a safe harbor for disclosures limited to a "limited data set" as defined in existing regulations, plus whatever additional information the covered entity or business associate determines to be the minimum necessary required for the purpose.

Right to Request Restrictions

Covered entities are required to agree to a request to restrict the disclosure to a health plan of information relating to a treatment episode where the individual has paid for that episode of treatment out-of-pocket.

Right to Request Electronic Copies of Records

Individuals currently have a right to request a copy of their records. The ARRA provides a new right to consumers to obtain their records in electronic form when such information is maintained by the covered entity in an EHR. In addition, the individual has a right to direct the covered entity to transmit an electronic copy of the record directly to a person or entity designated by the individual.

Prohibition on Remuneration

Using health care fraud and abuse terminology, the ARRA states that a covered entity is prohibited from directly or indirectly receiving remu-

neration in exchange for protected health information without an authorization of the individual that specifically addresses further exchanges for remuneration. There are limited exceptions that include treatment, limited health care operations, public health activities, and research where the payment reflects the cost of preparation and transmission of data. The Secretary is directed to issue further regulations addressing these issues.

Marketing

The provisions of the HIPAA privacy regulation governing use or disclosure of information for marketing are modified by prohibiting certain communications for which direct or indirect payment is received, that otherwise could be permissible as "health care operations." The statute specifies that payment that is "reasonable in amount" as defined by the Secretary in a new regulation is not covered by this new provision where the communication pertains to a drug or biologic that is currently prescribed for the recipient of the communication. This provision targets communications that are made by covered entities such as pharmacies, health care providers, and health plans, when the communications are paid for by third parties.

Fundraising

A covered entity that uses protected health information as permitted by the existing regulations is required to provide a conspicuous opportunity to opt out of future fundraising communications. This is already a requirement under the Privacy Rule and the effect of this change is not readily apparent.

De-identification

HHS is directed to issue guidance within 12 months on best practices for implementing HIPAA requirements for de-identifying protected health information.

Published in the April 2009 issue of Privacy & Data Security Law Journal.

NEW FEDERAL SECURITY BREACH NOTIFICATION REQUIREMENTS

The ARRA establishes a federal security breach notification law that will require HIPAA-covered entities to notify each individual whose "unsecured protected health information" is reasonably believed to have been accessed, acquired, or disclosed by a "breach." Business associates will be required to notify the covered entities on whose behalf they are maintaining the PHI. The definition of a "breach" is complex and will require careful analysis with respect to a given incident.

"Unsecured protected health information" means that the information is not secured through a technology specified by the Secretary. The statute requires that the HHS Secretary issue guidance on the definition of "unsecured" protected health information.

The new federal statute includes detailed requirements regarding the content, timeliness, and methods of providing notice to individuals, as well as notice to the Secretary and the media in the event that 500 or more individuals are reasonably believed to be affected. The Secretary will post the list of covered entities that have experienced breaches on its web site. In addition, almost every state has enacted its own data breach notification law, and many of these have specific timelines, content requirements, and state agency notification requirements. Unlike most of the state notice laws, the federal notice requirement includes breaches of health information and is not limited to electronic information. Covered entities will need to comply with both federal and state requirements.

The new federal law also includes breach notification requirements for non-HIPAA covered PHR vendors and other health care stakeholders that are not covered by HIPAA. Such entities are required to notify affected individuals as well as the Federal Trade Commission ("FTC"), which is charged with enforcing consumer protection laws. The FTC is obligated to notify the HHS Secretary of health care data breach reports it receives. In these cases, the FTC may take enforcement action under Section 5 of the FTC Act, which governs unfair and deceptive practices.

Published in the April 2009 issue of Privacy & Data Security Law Journal.

PRIVACY EDUCATION

The Secretary is required to designate an employee in each HHS regional office (not later than six months after the date of enactment) to provide guidance to covered entities, business associates, and individuals on their rights and responsibilities relating to privacy and security.

The Office for Civil Rights within HHS is required to develop and maintain a multifaceted national education initiative to enhance public transparency regarding the uses of protected health information.

REPORTS AND POSSIBLE FURTHER RULEMAKING

The law includes numerous requirements for reports and analyses by the Comptroller General and others with respect to key issues relating to uses and disclosures of protected health information currently permitted by the HIPAA Privacy regulations. There is likely to be extensive HHS rule-making activity to implement the changes required by the federal stimulus package. Please note that the provisions summarized here are only a portion of the many significant provisions set forth in the health care privacy sections of the ARRA.

Published in the April 2009 issue of Privacy & Data Security Law Journal.