Stimulus Package Expands the Applicability and Penalties of the HIPAA Privacy and Security Regulations

Health care providers and businesses that play in the electronic medical/health record space should take heed: The Health Information Technology for Economic and Clinical Health Act ("HITECH Act"), which is part of the American Recovery and Reinvestment Act of 2009 (the "Stimulus Package"), was signed into law on February 17, 2009. HITECH will bring about major changes to the requirements, application and penalties associated with the Health Insurance Portability and Accountability Act of 1996 Privacy and Security Regulations (referred to jointly as "HIPAA" and singly as the "Privacy Regulations" and the "Security Regulations" for purposes of this Advisory). These changes will dramatically expand the application of HIPAA to covered entities, business associates, vendors of electronic health records and personal health records and, potentially, many other entities previously not directly covered by HIPAA.

Background

The purpose of the HIPAA Privacy Regulations and Security Regulations (effective for most "covered entities" in 2003 and 2005, respectively) is to protect the use and disclosure of individually identifiable "protected health information" ("PHI") and "electronic PHI" ("ePHI") by "covered entities" and their "business associates." The HIPAA obligations were expanded dramatically through the recent enactment of the HITECH Act.

With the anticipated increase in use of health information technology and the goal of use of electronic health records ("EHR") in the health care community by 2014, Congress thought it necessary to expand the reach of HIPAA through increased penalties and requirements. The most significant changes and potential action items for covered entities, business associates and non-HIPAA covered entities are noted in this advisory.

Major Changes

Mandatory Reporting of Breaches. HIPAA currently does not have a mandatory self-reporting or notification requirement for breaches of PHI by a covered entity. That has now changed: Similar to many states' security breach notification

Mandatory Reporting of Breaches – Action Items

- Submit comments during rulemaking process regarding the definition of "unsecure" PHI and seek clarification of the requirements.
- Review breach policies and procedures for potential issues. Update breach policies and procedures once interim final regulations have been issued.
- Audit privacy systems to ensure PHI is secure.
- Audit security systems once guidance on "unusable, unreadable, or indecipherable" is issued.
- Establish a breach action team.

Continued

laws, covered entities, business associates, vendors of personal health records, and certain other entities will be required in the near future to notify each individual whose unsecured PHI has been (or is reasonably believed to have been) accessed, acquired, or disclosed inappropriately. Moreover, business associates will be required to notify covered entities of these breaches. Notice also will have to be given to the Secretary of Health and Human Services ("HHS") and even the Federal Trade Commission ("FTC") in certain cases. Notice may also need to be posted via mass or local media or through the websites of the covered entities or HHS.

These new statutory requirements will be subject to rulemaking with interim final regulations to be issued not later than 180 days from February 17, 2009 (the date of enactment of the Stimulus Package). In addition, within 60 days of February 17, 2009, the Secretary of HHS will issue guidance specifying the technologies and methodologies to render PHI unusable, unreadable, or indecipherable to unauthorized individuals.

Business Associates – Action Items:

- Covered entities and business associates should comment on applicable proposed regulations.
- Covered entities and business associates should watch for regulations and technical safeguard guidance to be issued relating to these new requirements.
- Covered entities and business associates should review and/or revise their business associate agreements.
- Business associates should comply with new applicable HIPAA requirements.
- Business associates should revise policies and procedures to reflect changes.
- Business associates should establish breach reporting policies and procedures and should assess the requirements regarding reporting of "security incidents" versus reporting of "breaches of unsecured PHI."

Business Associates. Covered entities are required to enter into business associate agreements prior to disclosing PHI to businesses that perform billing, accounting, legal, or other services on behalf of covered entities. Currently, business associate agreements contractually bind partners to certain mandatory HIPAA requirements, but generally may not be enforced by HHS. Business associates will now be subject to direct statutory liability (including civil and criminal penalties) for certain breaches. This is a significant change for health care companies across the country which must come into HIPAA compliance themselves. Among other things, business associate agreements must be amended to add additional compliance requirements – a huge administrative burden to both covered entities and business associates.

When issued, regulations should shed light on the implications of these new requirements. For example, it remains to be seen whether business associate agreements that contain provisions to allow for automatic amendment to comply with the Privacy Regulations and/or Security Regulations changes will have to be amended. At a minimum, these agreements should be reviewed to determine whether or not an amendment is necessary.

Individual Rights. There are several changes to the rights an individual has under HIPAA, a few of which are highlighted here. Current law provides that individuals have the right to access their PHI and to receive copies of their medical records. Under the new law, individuals have the specific right to obtain copies of their ePHI.

Continued

Further, one of the most onerous provisions in the HITECH Act is a requirement that covered entities provide an accounting of disclosures of ePHI for treatment, payment and health care operations ("TPO") for the three years prior to the request. Without EHR software that automatically captures this type of information, this exception will be costly, if not impossible, to implement.

Individual Rights – Action Items:

- Comment on proposed regulations.
- Watch for regulations and compliance dates.
- Establish process for individuals to request and receive electronic copies of their medical records.
- Audit and amend accounting of disclosures policy and procedures.
- Ensure there is a process to capture required information in EHR software.
- Develop a methodology to track all disclosures for TPO and ensure business associates do the same.

Non-Covered HIPAA Entities. The HITECH Act also creates a new category of entities under HIPAA called "Non-Covered HIPAA Entities" which will be covered by HIPAA in some capacity in the future. Congress has directed the FTC and the Secretary of HHS to conduct a study on the privacy and security requirements for entities that are not covered entities and are not business associates of covered entities, including:

- vendors of personal health records;
- entities that offer products or services through the website of a vendor of personal health records;
- entities that are not covered entities and that offer products or services through the websites of covered entities that offer individuals' personal health records;
- entities that are not covered entities and that access information in a personal health record or send information to a personal health record; and
- third-party service providers used by a vendor or entity described above to assist in providing personal health record products or services.

This study, which must be completed by February 17, 2010, must include the requirements relating to security, privacy and notification in the event of a breach of PHI and the deadline by which regulations regarding these requirements must be issued.

Non-Covered HIPAA Entities – Action Item:

- Watch for study results.

New Penalties and Enforcement Provisions

HITECH also creates a new tiered-penalty structure and a new category of violation due to "willful neglect." Generally, this structure and accompanying penalties for violations are as follows:

- In a case in which a person neither knew nor had reason to know through the exercise of reasonable due diligence of a violation, a penalty for each such violation is at least $100 per violation, not to exceed $25,000 per calendar year for all such violations of an identical requirement or prohibition;
- In a case of a violation which is due to reasonable cause, and not willful neglect, a penalty for each such violation is at least $1,000 per violation, not to exceed $100,000 per calendar year for all such violations of

Continued

an identical requirement or prohibition;

- In a case of a violation due to willful neglect:
  - If it is cured within 30 days of when the entity knew or should have known of the violation, then the penalty is at least $10,000 for each such violation, not to exceed $250,000 per calendar year for all such violations of an identical requirement or prohibition;
  - If the violation is not so corrected, then the penalty is at least $50,000 for each such violation, not to exceed $1,500,000 per calendar year for all such violations of an identical requirement or prohibition.

In addition, HITECH permits state attorneys general to bring civil actions on behalf of affected residents to enjoin the defendant or obtain damages on behalf of residents in the amount of $100 for each such violation, not to exceed $25,000 per calendar year for all such violations of an identical requirement or prohibition. HHS is required to promulgate regulations regarding noncompliance due to willful neglect by August 17, 2010, with penalties to be imposed for such noncompliance by February 17, 2011. However, the effective date for the tiered increases in civil monetary penalties and the enforcement powers of state attorneys general is February 17, 2009.

For more information, contact any of the following Baker Donelson attorneys:

Atlanta, Georgia
Gina Ginn Greenwood 404.589.0009 ggreenwood@bakerdonelson.com
Thomas Baker 404.221.6510 tbaker@bakerdonelson.com

Nashville, Tennessee
Betty Steele 615.726.5603 bsteele@bakerdonelson.com
Thomas Bartrum 615.726.5641 tbartrum@bakerdonelson.com

Washington, DC
Alisa L. Chestler 202.508.3475 achestler@bakerdonelson.com
Donna Thiel 202.508.3414 dthiel@bakerdonelson.com

Baton Rouge
Donna Fraiche 504.566.5201 dfraiche@bakerdonelson.com

Birmingham
J. Andrew Lemons 205.250.8327 alemons@bakerdonelson.com

Jackson, Mississippi
Jonell Williamson 601.351.2427 jwilliamson@bakerdonelson.com

New Orleans, Louisiana
Danielle Trostorff 504.566.5224 dtrostorff@bakerdonelson.com