[buck research]

fyi® for your information®

Volume 32, Issue 24, April 27, 2009

New HIPAA Privacy and Security Requirements in Stimulus Bill

The recently enacted American Reinvestment and Recovery Act (ARRA) includes a significant expansion of the privacy and security requirements of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) that affects both covered health plans and business associates. In particular, ARRA imposes breach notification requirements, makes business associates directly responsible for complying with HIPAA privacy and security rules, and provides for increased enforcement activity and penalties for noncompliance. Many of the changes will not take effect until next year, but some are effective now.

Background

Along with its portability provisions, HIPAA provides important privacy and security rights for individuals with respect to their protected health information. Prior to ARRA, HIPAA imposed privacy and security requirements only on covered entities, i.e., health care providers, health plans and health care clearinghouses. Business associates (e.g., third-party administrators, consultants, and other vendors) were not directly covered by the HIPAA rules, but they were indirectly regulated through business associate agreements with covered entities. Now, certain HIPAA provisions and penalties will apply to business associates directly, just as they apply to covered entities.

HIPAA Changes in ARRA

The major changes to HIPAA were included in one title of ARRA, the Health Information Technology for Economic and Clinical Health Act (HITECH). The HITECH provisions include the direct regulation of business associates, breach notification requirements, additional individual privacy rights, and strengthened enforcement with significantly increased penalties.

Application of Security Standards and Privacy Provisions to Business Associates

Security Standards. Under HITECH, certain HIPAA security standards, such as establishing administrative and physical safeguards and implementing reasonable and appropriate policies and procedures, now apply directly to business associates (i.e., persons or entities that perform a function or activity involving the use or disclosure of protected health information (PHI) for a HIPAA covered entity). Business associates will now be required to conduct a formal risk assessment, appoint a security officer, develop written security policies and procedures, and train their employees on HIPAA and how to protect PHI. Further, business associates will be required to implement safeguards to protect electronic PHI, such as encrypting emails and computer files and limiting access

to PHI. As required under the law, HHS has just issued initial guidance on technologies and methods for the protection of PHI.

These new requirements will need to be reflected in business associate agreements. Business associates will now be subject to the same civil and criminal penalties for noncompliance as covered entities.

Privacy Provisions. Prior to HITECH, business associates were indirectly required to meet privacy requirements through the business associate agreement. The new law requires them to comply with each applicable requirement of the HIPAA privacy provisions. As with the new security requirements, the additional privacy requirements must be incorporated into business associate agreements and business associates will be subject to the same civil and criminal penalties for noncompliance as covered entities.

> ***BUCK COMMENT.*** *Group health plan sponsors will have to amend their business associate agreements and may want to take steps to assure that their business associates are in compliance.*

Modifications of Certain Definitions

The new law provides definitions of terms that for the most part reference definitions under the HIPAA administrative simplification standards. However, certain terms are newly defined. For example, breach is generally defined as an unauthorized acquisition, access, use, or disclosure of unsecured protected health information which compromises the security or privacy of the information, excluding certain inadvertent or unintentional disclosures. An electronic health record (EHR) is generally described as a patient health record that can assist the patient and clinicians in decision making.

> ***BUCK COMMENT.*** *A small but growing number of employer-sponsored plans offer members access to their EHRs. It should be noted that not all electronic PHI is considered an EHR.*

Breach Notification Requirements

Prior to HITECH, HIPAA generally did not require health plans and other covered entities to notify individuals or the Secretary of Health and Human Services (HHS) of a PHI privacy or security breach, and business associate agreements only required business associates to report such breaches to the covered entity.

Under the new law, HIPAA covered entities that have a breach with respect to unsecured PHI – or reasonably believe a breach has occurred – must notify each affected individual without reasonable delay and no later than 60 days after the discovery of the breach. Similarly, business associates that have a breach must notify the covered entity within 60 days, identifying each individual whose unsecured PHI was, or is reasonably believed to have been, accessed or disclosed during the breach. In addition, if 500 or more individuals are impacted, covered entities must also notify HHS. If the breach involves more than 500 residents of a state or geographic area, notice is to be provided to "prominent media outlets" serving the state or area. The burden of proving compliance with the notice requirements is on the covered entity or business associate.

Notice is generally to be provided in writing by first class mail to the affected individual's last known address, but electronic notification is allowed in limited circumstances, and certain postings may be required where contact information is lacking. Telephone contact or other means may be appropriate in situations requiring urgency due to imminent misuse. HHS is required to issue regulations on these notification requirements by August 16, 2009, and the duty to notify individuals of security breaches is effective 30 days after their issuance.

HITECH also extends the breach notification requirements to vendors of personal health records (PHRs) and other non-HIPAA covered entities (e.g., entities offering products and services through a PHR vendor's website). These entities must notify both the affected individual and the Federal Trade Commission (FTC) upon discovering a security breach of "unsecured PHR identifiable health information." The FTC, which will have enforcement authority over these breaches, has just issued a proposed breach notification rule for comment and is required to issue interim final regulations by August 16, 2009.

Access to Electronic Health Records and Disclosures

When PHI is maintained by a covered entity as an EHR, the new law gives individuals the right to request and receive their information in electronic format from that entity at a reasonable cost. Covered entities may not charge a fee that exceeds the labor costs of responding to an individual request (as opposed to copying, labor and postage costs currently). Importantly, an individual who has fully paid for a health care item or service out-of-pocket may now prohibit disclosure of PHI to his or her health plan for payment or healthcare operation purposes (but not for treatment purposes).

Existing law gives individuals the right to an accounting of certain PHI disclosures for up to 6 years, but not to otherwise permissible disclosures for treatment, payment or health care operations. Under HITECH, individuals will also have the right to receive an accounting of all EHR disclosures made by covered entities or their business associates during the three years preceding the request for an accounting – even those for treatment, payment, or healthcare operation purposes. This requirement will apply to disclosures for current users of EHRs beginning in 2014. For non-users of EHRs, it will apply when the covered entity acquires EHRs or January 1, 2011, whichever date is later.

> ***BUCK COMMENT.*** *This requirement will be particularly burdensome as it dramatically increases the records that will need to be kept and monitored by covered entities.*

The sale of EHRs or PHI obtained from EHRs is prohibited absent a valid authorization unless the sale is for certain public health and other limited reasons. HHS is required to issue regulations by August 17, 2010, to take effect six months after issuance.

Minimum Necessary Information

HIPAA generally requires that covered entities limit PHI to the "minimum necessary" when using or disclosing PHI for purposes other than treatment. ARRA mandates that HHS issue guidance on what constitutes "minimum necessary" by August 17, 2010. In the meantime, covered entities and business associates should reexamine

their procedures for use and disclosure of PHI and limit disclosures to the limited data set (i.e., excluding identifiers such as names, street addresses, social security numbers, telephone numbers) to the extent practicable. Certain activities, such as claims audits, will require additional information, but parties should ensure that the disclosed data set is limited to accomplish the intended purpose.

Expanded Enforcement and Penalties

Since the HIPAA privacy regulations took effect in 2003, enforcement has been limited to HHS and few penalties have been assessed against covered entities. HITECH seeks to change this pattern by substantially increasing the penalties for noncompliance and mandating penalties in certain circumstances. Further, the new law allows state attorneys general to bring enforcement actions to secure money damages on behalf of state residents.

The new law increases civil penalties, which vary based on the type of violation (i.e., no knowledge, reasonable cause and willful neglect), and allows a portion of the penalty to be distributed to affected individuals. It also requires HHS to periodically audit covered entities. When HIPAA was first enacted, penalties for violations were set at $100 each to a maximum of $25,000 per year for similar violations. This level of penalties will now only apply when the violations could not reasonably have been known. Violations involving "reasonable cause" will be subject to a minimum penalty of $1,000 per violation and those involving willful neglect will be subject to a minimum penalty of $10,000 per violation. The overall maximum for all violations of the same requirement is now $1.5 million per calendar year.

Effective Dates

Generally, the HITECH changes (including those to the business associate rules) will take effect on February 17, 2010. However, the increase in penalties is effective immediately.

Conclusion

Although most of the HITECH provisions are not yet effective, and certain provisions will not take effect until HHS has issued guidance, plan sponsors should begin to map out their game plans for compliance. Plan sponsors should now confirm that their up-to-date physical, technical and administrative safeguards are in place to protect PHI and all staff who come into contact with PHI have had adequate HIPAA training. In coming months, plan sponsors should update business associate agreements and HIPAA privacy and security policies and procedures.

Buck's consultants are available to review the new HIPAA requirements with you and to assist in your compliance efforts.