



Smith Moore Leatherwood LLP's Monthly Newsletter For the Health Information Management and Technology Community

By: Barry Herrin and Trish Markus

March 2009

| Volume V, Number 3

THE ECONOMIC STIMULUS PACKAGE: CHANGES TO HIPAA

Title XIII of the American Recovery and Reinvestment Act of 2009, also known as the Health Information Technology for Economic and Clinical Health Act ("HITECH"), includes numerous provisions which significantly expand the scope, penalties, and compliance challenges of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). In brief, HITECH changes the application of the provisions of the HIPAA Privacy Rule and the HIPAA Security Rule, expands the definition of business associates to include health information exchanges and regional health information organizations, increases the penalties for violations of HIPAA, provides additional methods of enforcement, and requires proactive auditing of covered entities by the Secretary of the Department of Health and Human Services ("HHS").

One of the most troubling features of HITECH, however, is the definition of a "breach" for purposes of all of these expanded and new obligations. HITECH defines a breach as "the unauthorized acquisition, access, use, or disclosure of protected health information which **compromises** the security or privacy of such information, **except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information.**" A great deal of commentary during HITECH's short life has been devoted to teasing out these concepts of "compromise" and "retention," and we are hopeful that the regulations will explain more precisely what these terms mean. As drafted, it appears that no harm is necessary for a breach to occur. Further, the definition of "breach" does not include: (a) unintentional access by employees of covered entities or business associates if occurring within the scope of their duties and if the information is not the subject of a further breach; and (b) inadvertent disclosures within a covered entity by and to people otherwise authorized to access the information, which would cover a wide range of inadvertent disclosures in the treatment context.

Listed below are further highlights of HITECH and the effects of such provisions on covered entities and their business associates.

EXPANDED PENALTIES (Effective immediately)

Some provisions of HITECH take effect **immediately**; these relate to increased and expanded penalties for violations of the HIPAA Privacy Rule and the HIPAA Security Rule. First, if a violation occurs and the responsible entity did not know "and by exercising reasonable diligence would not have known" that a violation occurred, the minimum penalty for each such violation begins at \$100. Second, if there is a violation due to "reasonable cause and not to willful neglect," the minimum penalty for each such violation is \$1,000. Finally, if a violation is due to willful neglect, the minimum penalty for such a violation is \$10,000 (for violations that are corrected within 30 days) or \$50,000 (for violations that are not), not to exceed \$1,500,000 per calendar year for all similar violations. In addition to the civil monetary penalties which the federal government can impose, HITECH creates for the first



THE ECONOMIC STIMULUS PACKAGE: CHANGES TO HIPAA *(continued)*

time a private right of action for a violation of HIPAA that can be brought by state attorneys general on behalf of individual patients in the amount of \$100 per violation, with a maximum of \$25,000 per year. Courts are permitted to award damages, court costs, and attorneys' fees against persons found to have violated HIPAA. In light of these additions, expect to see more plaintiffs' lawyers taking an interest in HIPAA and alleged breaches of information.

In addition to these expanded penalties, on and after February 17, 2011, the Secretary of HHS will be required: (a) to investigate every complaint of a HIPAA violation to determine if a violation is due to willful neglect; and (b) to impose a civil monetary penalty for any violations of HIPAA determined to be due to willful neglect.

EXPANDED OBLIGATIONS – BUSINESS ASSOCIATES **(Effective 2/17/2010)**

Recall that previous guidance from HHS limited enforcement of HIPAA violations to covered entities, and not to business associates. HITECH amends several provisions of HIPAA so that business associates will be treated in the same fashion as covered entities. First, every requirement under the HIPAA Privacy Rule or the HIPAA Security Rule will apply to business associates, and not just to covered entities. This means, for example, that business associates will be required to adopt all of the technical (encryption, password protection, etc.), administrative (training, policy adoption, etc.), and physical (locks and other building security measures, for example) safeguards formerly applicable only to covered entities, and persons whose protected health information ("PHI") they store now may obtain an accounting of disclosures and may amend PHI stored by the business associate. Business associates also will be required to report a violation of their business associate agreements by a covered entity to HHS or, in the alternative, terminate the business associate agreement. Finally, the full range of civil and criminal penalties will apply to business associates.

This new series of provisions also requires all current business associate agreements to be amended to take two specific changes into account: first, business associate agreements must include all of HITECH's new security provisions; and second, because business associates now have an obligation to report a breach of a business associate agreement to HHS, business associate agreements should be amended to remove any obligations on the part of the covered entity or, in the alternative, require the business associate to notify the covered entity in the event that a breach is alleged. These changes may make it too expensive for some smaller business associates to remain able to provide services to covered entities. Small billing companies, small third party administrators of self-insured health plans, and similar businesses need to assess quickly the additional cost that this compliance burden will cause. Law firms will also have to adopt these protective measures for case files containing PHI that are received from covered entities.

EXPANDED OBLIGATIONS – UNSECURED INFORMATION **(Effective no later than 9/16/2009)**

HITECH defines "unsecured PHI" as PHI that is "not secured by a technology standard that renders [PHI] unusable, unreadable, or indecipherable to unauthorized individuals" and is "developed or accredited" by a standards organization accredited by ANSI. This definition will apply only if the Secretary of HHS does not develop and promulgate his or her own definition in a regulation before April 17, 2009. Assuming that the statutory definition will apply, covered entities and business associates will have to notify patients of any unauthorized disclosure of, access to, or acquisition of their unsecured PHI **or of any reasonable belief that such has occurred**. This notice must be provided within 60 days of the date the unauthorized disclosure, access, or acquisition of unsecured PHI is discovered (or reasonably should have been discovered), and must be given to each individual whose unsecured PHI is affected. If the number of affected individuals exceeds 500 residents of a single state, a notice

THE ECONOMIC STIMULUS PACKAGE: CHANGES TO HIPAA *(continued)*

must be published in the media (and given to the Secretary of HHS). For disclosures affecting fewer than 500 persons in a single state, a log of such disclosures must be maintained and forwarded to the Secretary of HHS each year. The Secretary, in turn, will post on an HHS website the names of each covered entity involved in a breach affecting at least 500 residents.

The notice must contain at least the following information: (1) a brief description of what happened; (2) a description of the types of unsecured PHI that were involved in the breach (name, Social Security Number, etc.); (3) the steps individuals should take to protect themselves from potential harm; (4) a brief description of what the covered entity is doing to investigate the breach, mitigate damage, and protect against further breaches; and (5) contact information at the covered entity for questions by patients.

Unlike the definition of a “security incident” under the HIPAA Security Rule, which would apply only to electronic PHI, these notice requirements apply to **all** PHI. These notice requirements will take effect for breaches occurring 30 days after the promulgation of regulations by the Secretary of HHS, which must occur on or before August 17, 2009.

EXPANDED OBLIGATIONS – RHIOs, HIEs, AND PHR VENDORS **(Effective 2/17/2010)**

Under HIPAA, one of the perceived threats to maintaining the privacy of PHI in extended network environments was that regional health information organizations (RHIOs) and health information exchanges (HIEs) were not considered business associates of covered entities and, accordingly, were thought not to have any privacy obligations to the persons whose records were stored on their networks. Nor were private companies that helped either covered entities or individual patients collect and manage personal health records (PHRs) considered business associates of covered entities. Beginning on February 17, 2010, every RHIO, every HIE, and each vendor who contracts with covered entities to help the covered entities provide a PHR to their patients must enter into a business associate agreement (or, if applicable, a data use agreement) and “shall be treated as a business associate.”

EXPANDED OBLIGATIONS – ACCOUNTING FOR DISCLOSURES **(Effective no earlier than 1/11/2011)**

Covered entities have certain obligations to account for disclosures of PHI. HITECH adds a new burden of accounting for those entities that maintain PHI in electronic health records. Whereas, under the HIPAA Privacy Rule, covered entities were not required to account for disclosures of PHI made for purposes of treatment, payment, and health care operations, HITECH now requires covered entities and business associates to account for all electronic disclosures of PHI even for such purposes. The accounting must produce disclosures made for 3 years prior to the date of the request for accounting. In complying with the accounting obligation, a covered entity may choose either: (a) to produce an accounting of all disclosures made by itself and all of its business associates; or (b) to produce an accounting of all disclosures made by itself and a list of all business associates receiving electronic PHI (who then will have to provide the accounting to patients). The Secretary of HHS is required to promulgate regulations describing what information needs to be made available through this new accounting of disclosures requirement.

There are two separate effective dates for this expanded accounting obligation. For covered entities and business associates currently using an electronic health record system, the effective date is January 1, 2014. For covered entities and business associates who acquire an electronic health record system after January 1, 2009, the effective date is the later of January 1, 2011 or the date that the electronic health record system is acquired.

THE ECONOMIC STIMULUS PACKAGE: CHANGES TO HIPAA *(continued)*

The reason that late adopters have less time to comply is presumably because the systems that are being adopted from now on can be engineered from the start to comply with this requirement, whereas existing systems will likely need to be re-engineered to comply. The Secretary of HHS can extend both of these deadlines for up to a maximum of two years by regulation.

Keep in mind that the accounting requirement only applies to disclosures (that is, releases of PHI outside the covered entity) and not to uses (which are understood to be within the covered entity). Even so, absent some significant limiting provisions in the Secretary's forthcoming regulations, the costs to covered entities (and, to a lesser extent, business associates) to comply with this requirement will be truly extraordinary. Such entities should consider submitting comments, either individually or through state professional organizations, to the proposed regulations noting the nature and extent of the burden that these accounting requirements will impose.

NEW OBLIGATIONS – RESTRICTIONS ON DISCLOSURE OF PHI (Effective 2/17/2010)

Under the original HIPAA Privacy Rule (45 CFR § 164.522), covered entities were not required to agree to a patient's request to restrict the disclosure of that patient's PHI. HITECH now requires covered entities and business associates to agree to requested restrictions if: (1) the disclosure is to be made to a health plan for purposes other than treatment; and (2) if the patient or someone else pays in full for the care that is the subject of the PHI. This means that patients can prevent third-party payors from having access to records of care for which the payor is not financially responsible. This restriction would not apply if the payor is also a provider of health care treatment (such as HMOs, for example). Covered entities should consider whether their current technology will enable them to keep track of such requests and ensure that such information is not disclosed in violation of a patient's request. Where a provider participates in a RHIO, such tracking may be particularly difficult to accomplish absent sophisticated technology and training.

In addition, HITECH makes it very clear that the sale of PHI by covered entities or business associates is not permitted, except in very limited circumstances, without a specific advance patient authorization. This authorization must include a "specification of whether the [PHI] can be further exchanged for remuneration by the entity receiving [PHI]." This certainly will have the effect of limiting the sale of data by data clearinghouses and RHIOs as a source of revenue, unless that data is de-identified. This new restriction will apply 6 months after the Secretary of HHS promulgates regulations, which must occur on or before August 17, 2009. As under HIPAA, HITECH does not prohibit the sale of properly de-identified information.

NEW OBLIGATIONS – PHR VENDORS AND BREACHES OF SECURITY (Effective no earlier than 8/17/2009)

Vendors of PHRs have notice obligations similar to those of covered entities and business associates with respect to "breaches of security" of "unsecured PHR identifiable health information," which is individually identifiable health information (as defined under the original HIPAA Privacy Rule) that is held by a PHR vendor and that is "unsecured." HITECH defines "unsecured" as "not secured by a technology standard that renders [PHI] unusable, unreadable, or indecipherable to unauthorized individuals" and is "developed or accredited" by a standards organization accredited by ANSI. Arguably, there will be few PHRs that will contain paper records, so the primary focus of this portion of HITECH naturally will gravitate towards electronic solutions; however, any paper PHR still would be covered by this provision.

THE ECONOMIC STIMULUS PACKAGE: CHANGES TO HIPAA *(continued)*

Vendors of PHR solutions are not the only ones affected by this new requirement. Persons or entities that provide services to PHR vendors and that “access, maintain, retain, modify, record, store, destroy, or otherwise hold, use or disclose” unsecured PHR identifiable health information must notify the vendor to whom they provide services of any “breach of security.”

In addition to the notice required to be provided to each patient (which is the same as the notice required of covered entities and business associates), notice also must be given to the Federal Trade Commission, which has jurisdiction to enforce this portion of HITECH and which must promulgate regulations implementing this requirement on or before August, 17, 2009.

The troubling part of this new provision is the definition of “breach of security,” which means the acquisition without authorization of any unsecured PHR identifiable health information. This extremely broad definition—broader than most states security breach notification laws—will require PHR vendors and their service providers to develop a robust list of anticipated and permissible uses and disclosures of PHR information in an attempt to limit liability.

NEW OBLIGATIONS – MARKETING AND FUNDRAISING ACTIVITIES **(Effective 2/17/2010)**

HITECH clearly states that all patients must have the opportunity to opt out of communications regarding fundraising, and that fundraising communications may no longer be considered “health care operations.” HITECH also severely limits marketing communications, providing that any communication designed to encourage the purchase of a product or service must be considered marketing instead of “health care operations.” Covered entities also are severely limited in their ability to receive payment from a third party in exchange for communicating with their patients in a way that would have been considered marketing under the HIPAA Privacy Rule. These restrictions apply on and after February 17, 2010.

NEW OBLIGATIONS – GOVERNMENT OVERSIGHT **(Effective no earlier than 2/17/2010)**

The Secretary of HHS is required to conduct “periodic audits to ensure” that covered entities and business associates are in compliance with the HIPAA Privacy Rule and the HIPAA Security Rule. If there is no requirement for the promulgation of regulations to implement this requirement, then the Secretary of HHS could begin conducting such audits as soon as February 17, 2010. If the audits are dependent on the enactment of implementing regulations, then the audits of those obligations could begin no sooner than February 17, 2011. However, this is yet another area of the statute that is less than clear. We recommend that covered entities and business associates prepare for audits to begin no later than February 17, 2010 for all HIPAA requirements in effect as of the date of HITECH’s adoption and for all provisions of HITECH that are implemented by that date.

CONCLUSION

Covered entities and business associates (old and new) should familiarize themselves with the compliance deadlines of the various HITECH provisions and institute a strategy for achieving compliance with each requirement. Even for those requirements that may be altered by subsequent regulations, the practical technological and operational effects of each obligation are sufficiently complex that a head start on thinking about how to approach each issue most likely will pay dividends in the end.

THE ECONOMIC STIMULUS PACKAGE: CHANGES TO HIPAA (continued)

For more information on HITECH and its effects on covered entities and business associates, contact:

Barry Herrin

404-962-1027

barry.herrin@smithmoorelaw.com

Trish Markus

919-755-8850

trish.markus@smithmoorelaw.com

