[buck research]

A Xerox Company

fyi© for your information©

Volume 33 | Issue 58 | October 1, 2010

HHS Proposes Changes to the HIPAA Privacy, Security and Enforcement Rules

The Health Information Technology for Economic and Clinical Health Act (HITECH), enacted as part of the American Reinvestment and Recovery Act (ARRA), significantly expanded the privacy, security and enforcement requirements imposed by the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Among other things, HITECH made business associates directly responsible for complying with HIPAA privacy and security rules, and provided for increased enforcement of those rules. The Department of Health and Human Services (HHS) recently issued proposed regulations to implement these provisions and to make other changes to existing HIPAA requirements.

Background

In addition to its portability provisions, HIPAA provides important privacy and security rights for individuals with respect to their protected health information. Prior to HITECH, HIPAA imposed privacy and security requirements only on covered entities (i.e., most health care providers, health plans and health care clearinghouses), and indirectly regulated business associates (e.g., third-party administrators, consultants, and other vendors) through their agreements with covered entities. As a result of HITECH, certain HIPAA provisions and penalties will now apply to business associates directly, just as they apply to covered entities. (See our April 27, 2009 *For Your Information*.) Other major changes to HIPAA made by HITECH include breach notification requirements, additional individual privacy rights, and strengthened enforcement with significantly increased penalties for HIPAA privacy and security violations.

HHS previously issued regulations implementing HITECH's breach notification requirements and its increased penalty provisions. (See our September 4, 2009 and November 18, 2009 *For Your Information* publications.) HHS has now proposed regulations implementing other HITECH provisions, most notably those relating to business associates.

HHS Guidance on Changes to HIPAA Rules

Expansion of Definition of Business Associate

The proposed regulations expand the definition of a business associate to include, among some additional entities, subcontractors or other agents of a business associate that handle PHI on behalf of the business

associate (however, the proposed regulations specify that covered entities do not have to enter into direct agreements with them). Like primary business associates, these subcontractors would be liable for penalties for noncompliance.

New Requirements for Business Associate Agreements

The standards for protecting information will now need to be reflected in business associate agreements and business associates will be subject to the HIPAA civil and criminal penalties for noncompliance. An "upstream" business associate must have a written agreement with its subcontractor containing satisfactory assurances that the subcontractor will comply with applicable provisions of the privacy and security rules. In addition, if a business associate knows of a pattern or practice of its subcontractor that constitutes a material breach or violation of the subcontractor's agreement, it would be required to take reasonable steps to cure the subcontractor's breach or terminate the contract, if feasible. Thus, a business associate that is aware of noncompliance by its subcontractor must respond in the same manner as a covered entity would respond to noncompliance by its business associate.

The proposed regulations would require business associate agreements to provide, among other things, that business associates will –

- establish administrative, technical, and physical safeguards and implement reasonable and appropriate security policies and procedures
- comply with the HIPAA privacy rule in carrying out a covered entity's obligation under the privacy rules
- ensure that subcontractors that create or receive PHI on behalf of a business associate agree to the same restrictions with respect to PHI applicable to the business associate, including reporting breaches of unsecured PHI to covered entities.

Transition Period for Business Associate Agreements

The proposed regulations provide a transition period for covered entities and business associates to revise existing business associate agreements to comply with the new requirements. Under the transition rule, a covered entity (or a business associate with respect to a subcontractor) will be deemed in compliance with the new documentation and contract requirements with respect to a particular business associate relationship for a period of time following the publication of the final regulations in the Federal Register if –

- the parties are operating pursuant to a written contract or arrangement that complied with the applicable privacy and security provisions in effect on the effective date of the contract, and
- the contract or other arrangement is not renewed or modified during the period beginning 60 days after the date the final regulations are published in the Federal Register and ending 240 days after the publication date.

An existing contract that meets these conditions will be deemed compliant until the date that is the earlier of (1) one year and 240 days after the date the final regulations are published in the Federal Register or (2) the date the contract is subsequently modified or renewed that is after 240 days after the date the final regulations are published. Evergreen contracts will be eligible for this relief provided they automatically renew without change.

Although covered entities and business associates can continue to operate under their existing agreements during this period, the business associate's obligation not to use or disclose PHI in a manner that is contrary to the privacy rule begins on the compliance date of the final regulations.

BUCK COMMENT. *It is not known when HHS will release final regulations. Plan sponsors will need to be ready to implement contract changes once the regulations are finalized. Importantly, the transition period does not extend to other compliance obligations.*

Other Changes of Significance to Employers

Notice of Privacy Practices

The proposed regulations would require modifications to a plan's notice of privacy practices with the addition of a description of the uses and disclosures of PHI that require an authorization, including most uses and disclosures of psychotherapy notes or for marketing purposes.

Because HHS considers these changes to be material, under existing rules covered entities would have to revise and redistribute their notice within 60 days of the effective date of the change. However, in recognition of the potential cost of these changes, HHS is considering several alternative options for the timing of new notices, including a requirement that new notices be provided at the next annual distribution to plan members.

Minimum Necessary PHI

A key provision of the HIPAA privacy rules generally requires, with limited exception, that covered entities limit the use or disclosure of, and requests for, PHI to the "minimum necessary" information needed to accomplish the intended purpose. HITECH provides that a covered entity will be in compliance with the minimum necessary requirement only if it limits PHI, to the extent practicable, to the limited data set. A limited data set excludes identifiers such as names, street addresses, social security numbers, and telephone numbers. A covered entity may use, disclose or request additional information only when such information is needed; such information is subject to the "minimum necessary" standard.

BUCK COMMENT. *ARRA required HHS to issue guidance on what constitutes "minimum necessary," and the proposed regulations are soliciting comments on particular issues the guidance should address. In the meantime, the current privacy rule remains in effect and covered entities and business associates should reexamine their procedures for use and disclosure of PHI as part of their periodic risk assessment.*

Expanded Enforcement and Penalties

Business associates and covered entities that violate HITECH and certain privacy and security provisions are subject to the same civil and criminal penalties. Under the proposed regulations, a business associate would also be civilly liable under agency principles for violations by its workforce members and its subcontractors in certain circumstances. By eliminating an existing exception, the regulations also expand the liability of a covered entity for violations by its business associates. Significantly, the covered entity would remain liable for the acts of its business associate who act as plan agents, regardless of whether it has a compliant business associate agreement in place.

HITECH's new tiered penalty structure recognizes the following degrees of violation –

- violations which the person did not know of and with reasonable diligence would not have known of
- violations due to reasonable cause and not to willful neglect
- violations due to willful neglect.

The proposed regulations clarify what constitutes "reasonable cause" for penalty purposes. Under the revised definition, reasonable cause is "an act or omission in which a covered entity or business associate knew, or by exercising reasonable diligence would have known, that the act or omission violated an administrative simplification provision of HIPAA, but in which the covered entity or business associate did not act with willful neglect." Violations involving reasonable cause will be subject to a minimum penalty of $1,000 per violation, while those involving willful neglect will be subject to a minimum penalty of $10,000 per violation. Maximum penalties can go as high as $1.5 million for willful neglect involving multiple individuals' PHI. In determining a penalty amount, the proposed regulations require HHS to consider the nature and extent of the violation and the resulting harm. The regulations would permit HHS to take into account, among other things, the number of individuals affected, the duration of the violation, and whether the violation interfered with an individual's ability to secure health care.

> ***BUCK COMMENT.*** *Based on the limited number of examples given in the proposed regulations, it appears that plan sponsors will be able to avoid the most serious HIPAA penalties if they can demonstrate that their plans had appropriate, up-to-date privacy and security policies and procedures in place, and made some attempt to follow such policies. Plan sponsors are well advised to take care in selecting vendors who handle PHI, and to regularly review the compliance of those vendors.*

Effective Dates

Although many of the HITECH changes were effective on February 18, 2010, HHS recognizes that compliance by covered entities and business associates will be difficult until the changes to the HIPAA rules are finalized. HHS has indicated that covered entities and business associates will have 180 days after the effective date of the final

regulations to come into compliance with most of the regulations' provisions. The 180-day period would not apply where a different compliance date is provided. As described above, HHS has also provided an additional transition period following the compliance deadline for covered entities and business associates to make the required changes to their existing business associate agreements or arrangements.

Conclusion

Although certain provisions will not take effect until HHS has issued final guidance, plan sponsors should begin to map out their game plans for compliance. Plan sponsors should reexamine their administrative, physical, and technical safeguards to protect PHI and ensure that all staff who come into contact with PHI have had adequate HIPAA training.

In the coming months, plan sponsors and business associates should review existing contracts and modify them when and as appropriate, taking into account the availability of the transition period. In view of the new liability risks, plan sponsors may also want to consider monitoring their current or prospective business associates to determine the adequacy of their privacy and security practices.

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