Bloomberg Law Reports® Health Law

What Employers Need to Know about HIPAA Now – HIPAA revisions under the HITECH Act of 2009

By Shannon Hartsfield Salimone, Holland & Knight LLP

President Obama is bringing change to our nation. One of those changes involves the investment of "$10 billion a year over the next five years to move the U.S. health care system to broad adoption of standards-based electronic health information systems, including electronic health records."[1] This move toward electronic health records is accompanied by heightened concern for the privacy and security of those records. On February 17, 2009, new federal laws were passed relating to the promotion of health information technology that address some of those concerns. The Health Information Technology for Economic and Clinical Health Act, or the "HITECH Act,"[2] is part of the American Recovery and Reinvestment Act, commonly referred to as the "stimulus bill." The HITECH Act contains changes to the requirements imposed on health plans, health care clearinghouses, and most health care providers through the Health Insurance Portability and Accountability Act of 1996, or "HIPAA."[3]

Employers with self-insured employee health benefit plans need to be aware of this new law. It will require updating existing HIPAA compliance plans. The portions of the HITECH Act with the most significant immediate impact include the following:

- Employer-sponsored self-insured health plans will soon have an obligation to notify individual enrollees if their protected health information is compromised.
- If the information of more than 500 individuals is compromised, health plans must alert the media and the Department of Health and Human Services ("HHS"). Covered entities will have to annually send HHS a list of these breaches occurring during the year.
- The HITECH Act increases penalties for HIPAA violations, which now can reach as high as $1.5 million in fines for multiple violations of an identical provision during a calendar year.
- State attorneys general and even individuals will be able to bring actions for HIPAA violations.
- There are new restrictions on selling protected health information.
- Several of a health plan's HIPAA compliance documents, including the Notice of Privacy Practices and business associate agreements, will have to be updated to conform to the requirements of the HITECH Act.

The HITECH Act is designed to promote the development of health information technology. The Act establishes, within the Department of Health and Human Services, an "Office of the National Coordinator for Health Information Technology."[4] The Office will be headed by a National Coordinator, who will have numerous duties. These duties include, among other things, ensuring that health information is secure and protected. By February of 2010, the Office will also have a Chief Privacy Officer. This person will advise the National Coordinator on "privacy, security, and data stewardship of electronic health information."[5]

Breach Notification Requirements

Prior to the passage of the HITECH Act, there was no specific requirement in federal law that entities subject to HIPAA notify individuals if their medical information was compromised. The HIPAA Privacy Rule does contain a requirement that a covered entity mitigate potential harm if there is an unauthorized use or disclosure, but this regulation does not necessarily require notification to patients.[6] If an employer experienced a breach of its health plan data, it had to determine whether the plan's mitigation efforts required notice to individual enrollees. The HITECH Act will now require notification of individuals when there is a breach. A “breach” is defined 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.”[7]

A breach does not include unintentional access, acquisition or use by an employee or individual acting under the authority of a health plan, other covered entity, or business associate if the access, acquisition or use was made in good faith and within the scope of employment or the professional relationship. The information must not be further acquired, accessed, used or disclosed by any person. A breach also does not include inadvertent disclosures from individuals who are otherwise authorized to access protected health information at a facility operated by a covered entity or business associate to another similarly situated individual at that same facility. In other words, a stray e-mail accidentally sent from one employee to another would likely not be a breach, as long as the information is not further acquired, accessed, used or disclosed without the authorization of the person who is the subject of the information.[8] These new requirements must be incorporated into the business associate agreement between the health plan and its business associates.[9]

If a breach involving "unsecured protected health information" occurs, a health plan has 60 calendar days after discovery of a breach to notify the individuals involved.[10] A breach is considered to be discovered on the first day on which it becomes known to the covered entity or business associate by any person other than the individual committing the breach.[11] Protected health information is considered "unsecured" when it is not protected through the use of a technology or methodology specified by the Secretary of the Department of Health and Human Services in a guidance document. The Secretary has issued guidance specifying the technologies and methodologies that render protected health information unusable, unreadable, or indecipherable.[12]

The notice of a breach must contain, to the extent possible, the following:

1. A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known.
2. A description of the types of unsecured protected health information that were involved in the breach (such as full name, Social Security number, date of birth, home address, account number, or disability code).
3. The steps individuals should take to protect themselves from potential harm resulting from the breach.
4. A brief description of what the health plan or other covered entity involved is doing to investigate the breach, to mitigate losses, and to protect against any further breaches.
5. Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, Web site, or postal address.[13]

Notice must be provided by first class mail to the individual's last known address.[14] If the address is unavailable, and other contact information (such as a phone number or email address) is out of date, then a substitute form of notice must be provided, which may include a conspicuous posting on the covered entity's website home page or notice in major print or broadcast media. Such notice must include a toll-free phone number that individuals may call to learn whether their information was involved in a breach. If records of more than 500 residents of a state or jurisdiction were involved, notice must be provided to prominent media outlets in the area.[15] Notice must also be provided to the Secretary of the Department of Health and Human Services. If the information of less than 500 individuals was breached, the covered entity may maintain a log of such breach and report it annually to the Secretary.

Increased Penalties

Before the HITECH Act, HIPAA applied only to covered entities, and not to business associates or to individual employees of covered entities. Under the HITECH Act, employees and other individuals can be found to have violated HIPAA and can be subject to criminal penalties.[16]

The HITECH Act increases civil monetary penalties for HIPAA violations. Depending on the facts and circumstances, penalties can now go as high as $50,000 per violation, not to exceed $1,500,000 for all such violations of an identical requirement or prohibition during a calendar year.[17] The increased penalties went into effect as of February 17, 2009, the date of enactment of the HITECH Act.[18]

Increased Enforcement

No later than three years from enactment of the HITECH Act, the Secretary of the Department of Health and Human Services is required to establish regulations setting forth a methodology to allow certain individuals to share in civil monetary penalties under HIPAA.[19] Specifically, an individual who is harmed by an act that constitutes a HIPAA violation may receive a percentage of any civil monetary penalty or settlement.

State attorneys general are now also given the power to enforce HIPAA. If the attorney general of a State has reason to believe that the interests of a citizen of the state have been threatened, the attorney general may bring a civil action on behalf of such state residents.[20] The attorneys general may recover statutory damages of up to $100 per violation, up to a maximum of $25,000 for all violations of an identical requirement or violation during a calendar year. A court also has the discretion to award costs of the action and reasonable attorney fees to the state.

This increased attention to enforcement makes it even more important for employers to make sure that their self-insured health plans comply with HIPAA's requirements.

Accounting for Disclosures

Under the original HIPAA Privacy Rule, an individual has a right to receive an accounting of disclosures of protected health information made by a covered entity in the six years prior to the date on which the accounting is requested, with certain exceptions.[21] For example, no accounting is required of disclosures to the individuals themselves, or disclosures pursuant to an authorization the individual has signed. Another exception provides that no accounting is required “[t]o carry out treatment, payment and health care operations . . .”.[22] The HITECH Act does away with this exception, to a certain extent. The exception for treatment, payment and health care operations does not apply to “disclosures through an electronic health record.”[23] Therefore, an individual has a right to an accounting of those disclosures made in the three years prior to the date on which the accounting is requested.[24] For entities using electronic health records as of January 1, 2009, the new requirement becomes effective on January 1, 2014. Entities not yet using electronic health records must comply with the new requirements as of

January 1, 2011 or the date that it acquires an electronic health record, whichever is later. Health plans, because they may handle only claims data instead of actual health records, may not necessarily be subject to the increased accounting requirements.

New Restrictions on Marketing and on the Sale of Protected Health Information

With limited exceptions, a health plan, other covered entity or business associate may not receive remuneration, directly or indirectly, in exchange for any protected health information, absent a signed authorization from that individual.[25] The prohibition on remuneration does not apply in the following cases:

A. The purpose of the exchange is for public health activities;

B. The purpose of the exchange is for research, and the price charged reflects the costs of preparation and transmittal of the data;

C. The purpose of the exchange is for the treatment of the individual;

D. The purpose of the exchange is for business management and general administrative activities of the entity;

E. The purpose of the exchange is for remuneration that is provided by a covered entity to a business associate for activities involving the exchange of protected health information that the business associate undertakes on behalf of and at the specific request of the covered entity pursuant to a business associate agreement;

F. The purpose of the exchange is to provide an individual with a copy of the individual's protected health information;

G. The purpose of the exchange is otherwise determined by the Secretary in regulations to be similarly necessary and appropriate as the above exceptions.[26]

The HITECH Act also contains new marketing restrictions. Specifically, a communication by a covered entity or business associate that is about a product or service and that encourages recipients of the communication to purchase or use the product or service shall not be considered a health care operation and will require the patient's authorization, with certain exceptions.[27] A communication will not be considered marketing, however, if it falls within certain portions of the definition of “marketing” in the HIPAA Privacy Rule.[28] Specifically, it is still OK to “market" if the communication is not made in exchange for remuneration and it describes a health-related product or service provided by the entity; it is for treatment of the individual; or if the communication is for case management or care coordination.[29]

If these types of communications are made in exchange for direct or indirect payment, then they may be prohibited.[30] These communications will be permissible if they describe “only a drug or biologic that is currently being prescribed for the recipient of the communication” and any payment is reasonable in amount. Also, the communication must be made by the covered entity and the covered entity must have obtained the patient's authorization. Alternatively, the communication may be made by a business associate of the covered entity and the communication must be consistent with the written contract between the business associate and the covered entity.

The HITECH Act also restricts fundraising activities. Any written fundraising communications must, in a clear and conspicuous manner, allow the recipient to opt out of receiving future communications.[31]

New Requirements for Business Associates

Until the passage of the HITECH Act, only covered entities, including health plans, health care clearinghouses, and most health care providers, were subject to HIPAA's requirements. Under HITECH, third parties who require protected health information to perform services for covered entities, known as “business associates,” will become legally obligated to comply with certain HIPAA requirements. Prior to the passage of the HITECH Act, business associates had to comply with privacy and security requirements found in contracts with covered entities, but did not have any direct legal requirements under HIPAA. Specifically, sections of the HIPAA Security Rule dealing with administrative safeguards,[32] physical safeguards,[33] technical safeguards,[34] and policies and procedures[35] will apply to business associates directly, as if they were covered entities themselves.[36]

Business associates are now required by law to comply with the privacy provisions of their business associate agreements.[37] The additional requirements of the HITECH Act related to privacy are applicable to business associates and must be incorporated into the agreement between the business associate and the covered entity. If a business associate violates the HITECH Act's privacy requirements, penalties shall apply in the same manner that they would apply to a covered entity.

A More Detailed "Minimum Necessary" Rule

The HITECH Act expands on HIPAA's "minimum necessary" rule[38] by requiring the entity to limit the protected health information used, disclosed, or requested to the "limited data set" whenever possible.[39] The "limited data set" is defined as protected health information that excludes the following direct identifiers of the individual or of relatives, employers, or household members of the individual:

1. Names;
2. Postal address information, other than town or city, State, and zip code;
3. Telephone numbers;
4. Fax numbers;
5. Electronic mail addresses;
6. Social security numbers;
7. Medical record numbers;
8. Health plan beneficiary numbers;
9. Account numbers;
10. Certificate/license numbers;
11. Vehicle identifiers and serial numbers, including license plate numbers;
12. Device identifiers and serial numbers;
13. Web Universal Resource Locators (URLs);
14. Internet Protocol (IP) address numbers;
15. Biometric identifiers, including finger and voice prints; and
16. Full face photographic images and any comparable images.[40]

An entity can use more than the limited data set, but only if necessary to accomplish the intended purpose of such use, disclosure, or request.[41] No later than 18 months after enactment of the

HITECH Act, the Secretary of the Department of Health and Human Services must issue guidance on what constitutes the "minimum necessary."[42]

Restrictions on Certain Routine Disclosures

Under the HIPAA Privacy Rule, an individual could request that a covered entity restrict how protected health information was used or disclosed for treatment, payment, or health care operations purposes, but the covered entity did not have to agree to such request.[43] Under the HITECH Act, the covered entity must comply with an individual's requested restriction if the disclosure is to a health plan for purposes of carrying out payment or health care operations (and is not for treatment purposes), and the information pertains solely to a health care item or service for which the health care provider involved has been paid out of pocket in full.[44]

Conclusion

In light of the above, employers will have a lot to accomplish to implement the new provisions of the HITECH Act for their self-insured health plans. Although the increased penalties apply immediately, and the increased breach notification requirements apply after publication of regulations, most of the provisions of the Act take effect on February 17, 2010. Employers should get started now to ensure compliance.

Shannon Hartsfield Salimone is a partner in the Tallahassee office of Holland & Knight. She advises clients on state and federal health care regulatory matters including corporate and regulatory compliance, data privacy, licensure, prescription drug distribution and pedigree requirements and telemedicine.

---

[1] *See* http://www.whitehouse.gov/agenda/technology/ (visited April 27, 2009).
[2] Pub. L. 111-5 (Feb. 17, 2009).
[3] Pub. L. 104-91 (Jan. 6, 1996).
[4] Pub. L. 111-5, § 3001.
[5] *Id*.
[6] *See* 45 CFR §164.530.
[7] Pub. L. 111-5, §13400.
[8] *Id*.
[9] *Id*.
[10] *Id*. at § 13402.
[11] *Id*.
[12] 74 Fed. Reg. 19006 (April 27, 2009).
[13] Pub. L. 111-5, §13402.
[14] *Id*.
[15] *Id*.
[16] Pub. L. 111-5, §13409.
[17] Pub. L. 111-5, §13410.
[18] *Id*.
[19] *Id*.
[20] *Id*.
[21] 45 C.F.R. §164.528.
[22] *Id*. at (a)(1)(i).
[23] Pub. L. 111-5, §13405.
[24] *Id*.
[25] *Id*. at §13405(d).
[26] *Id*.

[27] Pub. L. 111-5, §13406.
[28] *Id*.
[29] *See* 45 C.F.R. §164.501.
[30] Pub. L. 111-5, §13406.
[31] Pub. L. 111-5, §13406.
[32] 45 C.F.R. §164.308.
[33] 45 C.F.R. §164.310.
[34] 45 C.F.R. §164.312.
[35] 45 C.F.R. §164.316.
[36] Pub.. L. 111-5, §13401.
[37] *Id*. at §13404.
[38] 45 C.F.R. §164.514(d)(4).
[39] Pub. L. 111-5, §13405.
[40] 45 C.F.R. §164.514(e)(2).
[41] Pub. L. 111-5, §13405.
[42] *Id*.
[43] 45 C.F.R. §164.522(a)(1)(ii).
[44] Pub. L. 111-5, §13405.