February 23, 2010

Practices & Industries

Education

The American Recovery and Reinvestment Act of 2009 (ARRA), signed into law by President Obama on February 17, 2009, included more than $20 billion to encourage the development of a nationwide health information technology (HIT) network. To address concerns over the privacy of protected health information (PHI) within this network, Title XIII of the ARRA, known as the Health Information Technology for Economic and Clinical Health Act (HITECH Act), included numerous provisions to strengthen the privacy and security rules under HIPAA.

Under current law, HIPAA and its accompanying regulations may be applied only to "covered entities" and not directly to business associates of covered entities (BAs). Rather, BAs are indirectly brought under HIPAA when they enter into HIPAA-compliant contractual agreements with covered entities. The HITECH Act amends HIPAA regulations and contains provisions that now directly apply HIPAA to BAs. Moreover, the additional security and privacy provisions of HITECH directly apply to business associates.

More specifically, HIPAA's definition of covered entities includes health plans and health care providers that transmit any health information in electronic form. "Health care providers" include entities that provide "care, services, or supplies related to the health of an individual." A business associate is an entity that, on behalf of a covered entity, performs "a function or activity involving the use or disclosure of individually identifiable health information…."

A school district could be considered a covered entity when it acts as a health care provider. A school district must also comply with the HIPAA privacy and security rules if it sponsors a self-insured medical plan (including HRAs and health FSAs), as those plans are considered "covered entities." Although application of HIPAA to covered entities is not new law, compliance has traditionally been poor, in part because there has been little or no federal enforcement. However, the Department of Health and Human Services has announced its intention to step up enforcement, making this a good time for school districts to determine if they are covered entities or maintain self-insured medical plans (including HRAs and FSAs) subject to HIPAA and to take the necessary steps to comply.

A school district might also be considered a business associate to the extent it performs functions on behalf of a covered entity whereby it encounters protected health information. Although not all aspects of the operation of a school district

may fall under the definitions of covered entity or business associate, an assessment should be undertaken to examine what functions would be covered by HIPAA, as covered entities and BAs alike are now directly liable for certain HIPAA violations.

Security and Privacy Provisions

Effective February 17, 2010, BAs must comply with the administrative, physical, and technical safeguard requirements of the HIPAA Security Rule. To achieve these objectives, BAs must designate a security official who will develop, implement, and evaluate the policies, procedures, and documentation standards intended to prevent violations of the Security Rule.

The HITECH Act also makes BAs directly liable for violation f the Privacy Rule. Under the new act, BAs will be statutorily obligated to comply with the privacy provisions in their usiness associate agreements related to protected health information. Therefore, a BA will now be liable to both the overed entity under the business associate agreement and liable to the Department of Health and Human Services (HHS) or state attorneys general directly under HITECH. here currently BAs are liable for violations of HIPAA security r privacy provisions by virtue of breach of contract with covered entities, under HITECH BAs would be directly liable to HHS and state attorneys general for violation of HIPAA. Thus, they would be directly civilly and criminally liable.

Under the HITECH Act, BAs will be required to take action if they become aware of "a pattern of activity or practice" by a covered entity that constitutes a breach of their business associate agreement. Specifically, BAs must cure the breach, terminate the business associate agreement, or report the breach to HHS. If the BA fails to take appropriate action, the BA will be in violation of HIPAA.

Additional provisions of the HITECH Act pertaining to marketing communications, disclosures to health plans, minimum necessary standards, fundraising restrictions, and prohibition on the sale of PHI also directly apply to BAs.

Breach Notification

In the past, covered entities were not required to notify affected parties in the event of a security breach involving unsecured PHI. Under HITECH, however, covered entities are obligated to notify individuals whose "unsecured" PHI "has been, or is reasonably believed by the covered entity to have been, accessed, acquired, or disclosed as a result of such breach." Similarly, BAs are now statutorily required to notify the covered entity of a breach of PHI. Covered entities must notify affected individuals within 60 days of discovery of the breach, so it is critical that BAs make a timely disclosure to the covered entity. These breach notification requirements became effective September 23, 2009.

Enforcement, Penalties, and Audits

The HITECH Act authorizes the attorney general of each state to enforce the security and privacy rules of HIPAA by filing a civil action in a U.S. district court to either enjoin the violator or to obtain monetary damages on behalf of the individual (s) affected. HHS is also obligated to investigate complaints of HIPAA violations due to "willful neglect." Effective when

the HITECH Act was enacted, the civil monetary penalties associated with HIPAA violations were increased. Criminal penalties will also be imposed on business associates to the same extent as on covered entities. Finally, HHS is required to conduct periodic audits of covered entities and BAs to ensure HIPAA compliance policies and procedures are in effect.

Amending Existing Business Associate Agreements

There is currently no consensus among health law practitioners regarding whether current business associate agreements must be amended to comply with the provisions of the HITECH Act. While the plain language of the statute states that the requirements of the HITECH Act "shall be incorporated into the business associate agreement between the business associate and the covered entity," there are no regulations or guidelines from HHS that covered entities and BAs could follow in drafting such new agreements.

Suggestions for Action

To ensure compliance when a school district is a covered entity (a health care provider) or sponsor of a covered entity (a self-insured medical plan):

- Enter into business associate agreements with entities that provide service in connection with a self-insured medical plan, such as third party claims administrators, lawyers, and accountants
- Enter into business associate agreements with entities that provide service in connection with the provision of health care or services
- Provide a privacy notice to all self-insured medical plan participants explaining their HIPAA rights
- Provide a privacy notice to all recipients of health care or services explaining their HIPAA rights
- Establish a privacy and security policy with regard to the self-insured medical plan and/or the provision of health care or services
- Appoint a privacy official to be the point person responsible for HIPAA compliance

To ensure compliance when a school district may be a BA:

- Given the liability now imposed directly on BAs, school districts should consider whether they are actually BAs. In the past, entities readily entered into business associate agree ments because the only liability was based on contract. Under the new law, however, with the imposition of direct HIPAA/HITECH liability, such school districts should enter these agreements only if they apply.
- BAs should begin to work on HIPAA compliance plans, creating policies and procedures so BAs are in compliance with HITECH (e.g. breach notification rules) and the security and privacy rules.
- BAs should begin to educate employees and staff regarding the new requirements imposed by the HITECH Act and HIPAA. For example, in the context of a breach of unsecured PHI, employees should be trained about what constitutes a breach and the time frame in which BAs must report a breach to the covered entity.

- School districts might consider amending existing business associate agreements.

For more information, please contact:

Michael J. Flanagan
716.848.1480
mflanagan@hodgsonruss.com

Bethany J. Hills
716.848.1554
bhills@hodgsonruss.com

Bonnie A. Redder
716.848.1239
bredder@hodgsonruss.com

Arthur A. Marrapese III
716.848.1751
Art_Marrapese@hodgsonruss.com

Amy L. Goerss, Law Clerk
716.848.1451
agoerss@hodgsonruss.com