Bloomberg BNA

Privacy and Security Law Report®

Health Data

The HIPAA Privacy Rule and Security Rule generally require that Covered Entities and Business Associates enter into written agreements to safeguard protected health information. Given the $5.8 million in settlement payments/fines from HHS enforcement actions over the last six months, individual companies that create, receive, maintain or transmit PHI, should have a written contract or arrangement that meets the applicable requirements of HIPAA, the author writes.

Recent OCR Enforcement Actions Emphasize the Importance of Executing HIPAA Business Associate Agreements

By Michael A. Dowell

Background Information

The Health Insurance Portability and Accountability Act (HIPAA) is the principal federal law regulating health information privacy. It applies to ''Covered Entities,'' which broadly consist of health care providers, health insurers and health care clearinghouses. 45 CFR § 160.103. The HIPAA Privacy Rule establishes the circumstances under which ''protected health information'' (PHI) (information that does or can identify an individual) can be accessed, used or disclosed, and grants individuals certain rights to their own health information. 45 CFR § 164.524. The HIPAA Security Rule mandates appropriate administrative, physical and technical safeguard to help ensure the confidentiality, integrity and security of PHI stored electronically. 45 CFR Part 164.

Michael A. Dowell is a partner and member of the Health Care Law Group at Hinshaw & Culbertson LLP in Los Angeles. Dowell counsels health-care companies and organizations on HIPAA privacy and security issues. He can be reached at 310-909-8000 or mdowell@hinshawlaw.com.

A ''Business Associate'' is a person or entity, other than a member of the workforce of a Covered Entity,'' who performs functions or activities on behalf of, or provides certain services to, a Covered Entity that involve access by the Business Associate to PHI. 45 C.F.R. 160.103. A ''Business Associate'' is also a subcontractor that creates, receives, maintains or transmits PHI on behalf of another Business Associate.

The HIPAA Privacy Rule and Security Rule generally require that Covered Entities and Business Associates enter into written agreements with their Business Associates to ensure that the Business Associates will appropriately safeguard PHI. *See* 45 C.F.R. 164.308(b). Business Associate status attaches upon creation or receipt of PHI for a function, activity or service being provided on behalf of the Covered Entity. Thus, individuals or companies that create, receive, maintain or transmit PHI—such as management services organizations, billing companies, hardware and software vendors—

 ISSN 1538-3423

should have a written contract or arrangement that meets the applicable requirements of HIPAA.

Failure to obtain a Business Associate agreement potentially leaves protected health information without administrative, physical or technical safeguards and makes the PHI vulnerable to misuse or improper disclosure.

Failure to obtain a Business Associate agreement potentially leaves PHI without administrative, physical or technical safeguards and makes the PHI vulnerable to misuse or improper disclosure. ''HIPAA's obligation on covered entities to obtain Business Associate agreements is more than a mere check-the-box paperwork exercise,'' Jocelyn Samuels, Director of the U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) said in a press release. ''It is critical for entities to know to whom they are handing PHI and to obtain assurances that the information will be protected,'' she said.

Three OCR enforcement actions over the past six months resulted in $5.8 million in settlement payments/fines that underscore the importance of executing Business Associate agreements.

Recent OCR Enforcement Actions

Triple S Management Corporation (Nov. 30, 2015). Triple-S Management Corporation (TRIPLE-S) (an insurance holding company based in San Juan, Puerto Rico, which offers a wide range of insurance products and services to residents of Puerto Rico through its subsidiaries), on behalf of its wholly owned subsidiaries, Triple-S Salud Inc., Triple-C Inc. and Triple-S Advantage Inc., agreed to pay $3.5 million and put in place a comprehensive HIPAA compliance program as a condition for settlement of potential violations of the HIPAA Privacy Rule and Security Rule . Press Release, U.S. Dept. of Health and Human Services, Triple-S Management Corporation Settles HHS Charges by Agreeing to $3.5 Million HIPAA Settlement, (Nov. 30, 2015) (14 PVLR 2202, 12/7/15).

Covered Entities and Business Associates should assess, update and revise, as necessary, the policies and procedures at least annually.

After receiving multiple breach notifications from TRIPLE-S involving unsecured PHI, OCR initiated investigations to ascertain the entities' compliance with HIPAA Rules. OCR's investigations indicated widespread non-compliance throughout Triple-S, including: (1) failure to implement appropriate administrative, physical and technical safeguards to protect the privacy of its beneficiaries' PHI; (2) impermissible disclosure of its beneficiaries' PHI to an outside vendor with which it *did not have an appropriate Business Associate agreement;* (Specifically, OCR found that there was ''impermissible disclosure of its beneficiaries' PHI to an outside vendor with which it did not have an appropriate Business Associate agreement.); (3) use or Disclosure of more PHI than was necessary to carry out mailings; (4) failure to conduct an accurate and thorough risk analysis that incorporates all information technology (IT) equipment, applications and data systems utilizing ePHI; and (6) failure to implement security measures sufficient to reduce the risks and vulnerabilities to its ePHI to a reasonable and appropriate level. Triple-S Management Corporation Resolution Agreement and Settlement Agreement, (Nov. 30, 2015).

The settlement agreement requires TRIPLE-S to establish a comprehensive compliance program designed to protect the security, confidentiality and integrity of the personal information it collects from its beneficiaries, that includes: (1) a risk analysis and a risk management plan; (2) a process to evaluate and address any environmental or operational changes that affect the security of the ePHI it holds; (3) policies and procedures to facilitate compliance with requirements of the HIPAA Rules; and (4) a training program covering the requirements of the Privacy, Security and Breach Notification Rules, intended to be used for all members of the workforce and Business Associates providing services on TRIPLE-S premises.

North Memorial Health Care (March 16, 2016). North Memorial Health Care of Minnesota (a comprehensive, not-for-profit health care system in Minnesota that serves the Twin Cities and surrounding communities) agreed to pay $1,550,000 to settle charges that it potentially violated the HIPAA Privacy Rule and Security Rule by failing to enter into a Business Associate agreement with a major contractor and failing to institute an organization-wide risk analysis to address the risks and vulnerabilities to its patient information (15 PVLR 623, 3/21/16). OCR initiated its investigation of North Memorial following receipt of a breach report on Sept. 27, 2011, which indicated that an unencrypted, password-protected laptop was stolen from a Business Associate's workforce member's locked vehicle, impacting the electronic protected health information (ePHI) of nearly 10,000 individuals. Press Release, U.S. Dept. of Health and Human Services, $1.55 million settlement underscores the importance of executing HIPAA business associate agreements, (March 30, 2016).

OCR's investigation indicated that North Memorial *failed to identify Accretive Health, Inc. (which performed billing activities on behalf of the hospital) as a Business Associate, and failed to have in place with Accretive a Business Associate Agreement, as required under the HIPAA Privacy Rule and Security Rule*. North Memorial Health Care Resolution Agreement and Settlement Agreement, (March 30, 2016). North Memorial gave its Business Associate, Accretive Health, Inc., access to North Memorial's hospital database, which stored the ePHI of 289,904 patients. Accretive also received access to non-electronic protected health information as it performed services on-site at North Memorial.

The investigation further determined that North Memorial failed to complete a risk analysis to address all of the potential risks and vulnerabilities to the ePHI that

  PVLR ISSN 1538-3423

it maintained, accessed, or transmitted across its entire IT infrastructure—including but not limited to all applications, software, databases, servers, workstations, mobile devices and electronic media, network administration and security devices, and associated business processes.

In addition to the $1,550,000 payment, North Memorial is required to develop an organization-wide risk analysis and risk management plan, and adhere to a corrective action plan that includes training appropriate workforce members on all policies and procedures newly developed or revised pursuant to this corrective action plan.

Raleigh Orthopaedic Clinic (April 19, 2016). Raleigh Orthopaedic Clinic, P.A. of North Carolina (Raleigh Orthopaedic) (a provider group practice that operates clinics and an orthopaedic surgery center in the Raleigh, North Carolina area) agreed to pay $750,000 to settle charges that it potentially violated the HIPAA Privacy Rule by providing protected health information (PHI) for approximately 17,300 patients to a business partner without first executing a Business Associate agreement (15 PVLR 869, 4/25/16).

OCR initiated its investigation of Raleigh Orthopaedic following receipt of a breach report on April 30, 2013. OCR's investigation indicated that Raleigh Orthopaedic released the x-ray films and related protected health information of 17,300 patients to an entity that promised to transfer the images to electronic media in exchange for harvesting the silver from the x-ray films. Raleigh Orthopedic *failed to execute a Business Associate agreement with this entity* prior to turning over the x-rays and PHI. Press Release, U.S. Dept. of Health and Human Services, $750,000 settlement highlights the need for HIPAA business associate agreements, (April 19, 2016).

In addition to the $750,000 payment, Raleigh Orthopaedic is required to revise its policies and procedures to: establish a process for assessing whether entities are Business Associates; designate a responsible individual to ensure Business Associate agreements are in place prior to disclosing PHI to a Business Associate; create a standard template Business Associate agreement; establish a standard process for maintaining documentation of a Business Associate agreements for at least six years beyond the date of termination of a Business Associate relationship; and limit disclosures of PHI to any Business Associate to the minimum necessary to accomplish the purpose for which the Business Associate was hired. Press Release, U.S. Dept. of Health and Human Services, $750,000 settlement highlights the need for HIPAA business associate agreements, (April 19, 2016).

HIPAA Business Associate Agreement Best Compliance Practices

Create a Template Business Associate Agreement

A written contract between a Covered Entity and a Business Associate must:

- (1) establish the permitted and required uses and disclosures of protected health information by the Business Associate;
- (2) provide that the Business Associate will not use or further disclose the information other than as permitted or required by the contract or as required by law;
- (3) require the Business Associate to implement appropriate safeguards to prevent unauthorized use or disclosure of the information, including implementing requirements of the HIPAA Security Rule with regard to electronic protected health information;
- (4) require the Business Associate to report to the covered entity any use or disclosure of the information not provided for by its contract, including incidents that constitute breaches of unsecured protected health information;
- (5) require the Business Associate to disclose protected health information as specified in its contract to satisfy a covered entity's obligation with respect to individuals' requests for copies of their protected health information, as well as make available protected health information for amendments (and incorporate any amendments, if required) and accountings;
- (6) to the extent the Business Associate is to carry out a covered entity's obligation under the Privacy Rule, require the Business Associate to comply with the requirements applicable to the obligation;
- (7) require the Business Associate to make available to HHS its internal practices, books, and records relating to the use and disclosure of protected health information received from, or created or received by the Business Associate on behalf of, the covered entity for purposes of HHS determining the covered entity's compliance with the HIPAA Privacy Rule;
- (8) at termination of the contract, if feasible, require the Business Associate to return or destroy all protected health information received from, or created or received by the Business Associate on behalf of, the covered entity;
- (9) require the Business Associate to ensure that any subcontractors it may engage on its behalf that will have access to protected health information agree to the same restrictions and conditions that apply to the Business Associate with respect to such information; and
- (10) authorize termination of the contract by the covered entity if the Business Associate violates a material term of the contract. Contracts between Business Associates and Business Associates that are subcontractors are subject to these same requirements. OCR guidance on what a Business Associate agreement should include: U.S. Dept. of Health and Human Services, Sample Business Associate Agreement Provisions (Published Jan. 25, 2013).

Develop Policies and Procedures Related to Business Associate Relationships

Covered Entity should develop policies and procedures that:

- (1) designate one or more individual(s) who are responsible for ensuring that Covered Entity enters into a Business Associate agreement with each of its Business Associates, as defined by the HIPAA Rules, prior to Covered Entity disclosing protected health information (PHI) to the Business Associate;
- (2) create a process for assessing Covered Entity's current and future business relationships to determine

whether each relationship is with a Business Associate, as defined by the HIPAA Rules, and requires Covered Entity to enter into a Business Associate agreement;

■ (3) create a process for negotiating and entering into Business Associate agreements with Business Associates prior to disclosing PHI to the Business Associates;

■ (4) create a process for maintaining documentation of a Business Associate agreement for at least six years beyond the date of when the Business Associate relationship is terminated; and

■ (5) limit disclosures of PHI to Business Associates to the minimum necessary amount of PHI that is reasonably necessary for Business Associates to perform their duties.

Distribute Policies and Procedures Related to Business Associate Relationships

Covered Entities should distribute or otherwise make available on a corporate intranet HIPAA privacy and security policies and procedures related to Business Associate relationships. At the time of distribution of such policies and procedures, Covered Entities and Business Associates should obtain a signed written or electronic compliance certification from all workforce members and Business Associates stating that such workforce members and Business Associates have read, understand, and shall abide by such policies and procedures.

Update Business Associate Agreements and Policies and Procedures

Covered Entities and Business Associates should assess, update and revise, as necessary, the policies and procedures at least annually. Covered Entities and Business Associates should distribute such revised policies and procedures to all workforce members and business associates, and obtain new compliance certifications.

Provide Employee Training and Education

Provide training to Covered Entity and Business Associate workforce regarding Business Associates and their respective obligations under the HIPAA Privacy Rule and Security Rule. Covered Entities and Business Associates should remind employees about their HIPAA obligations on a regular basis, and document those reminders.

Conduct Employee Discipline

When protected health information is improperly accessed, used or released, or when an individual fails to comply with HIPAA Policies and Procedures; an individual may be disciplined based on the individual's classification. The specific discipline administered will depend on the nature and severity of the violation. Covered Entities and Business Associates should notify the Privacy Officer of any employee related violations of its policies and procedures related to Business Associate relationships

Audit and Monitor Business Associates

Covered Entities and Business Associates should audit and monitor their Business Associates for compliance with the HIPAA Privacy Rule and Security Rule; and the Covered Entity Business Associate Agreement. Under the HIPAA Privacy Rule and Security Rule, Business Associates now are required to:

■ (1) enter into HIPAA compliant business associate agreements with their subcontractors;

■ (2) use and disclose PHI only as permitted by their Business Associate Agreement;

■ (3) comply with the minimum necessary rule;

■ (4) notify the Covered Entity in case of a security breach;

■ (5) no sale of PHI without individual authorization or exception;

■ (6) provide access to a copy of the electronic PHI in their possession to either the Covered Entity, the individual, or the individual's designees; and

■ (7) provide the information needed for an accounting of disclosures;

■ (8) provide access to their records and PHI to DHHS for investigatory purposes.

The Office of Civil Rights has made it clear that failure to enter into Business Associate agreements as required will result in significant fines and penalties.

Business Associates are also required by law to comply with the Security Rule, and to safeguard electronic PHI in accordance with the HIPAA Security Rule.

Retain Compliance Documentation

Covered Entities and Business Associates should prepare and maintain a well-documented record of all HIPAA compliance activities. All documentation required for compliance review should be maintained for a period of six years.

Conclusion

The recent OCR enforcement actions/settlements emphasize the importance that Covered Entities and Business Associates enter into Business Associate agreements with their third-party vendors prior to allowing such vendors to create, receive, maintain or transmit PHI on behalf of the Covered Entity or Business Associate. In most cases, Business Associate agreements should be executed simultaneously with the contract for the third-party vendor services. OCR has made it clear that failure to enter into Business Associate agreements as required will result in significant fines and penalties.

In light of the recent enforcement actions and OCR's focus on HIPAA Phase 2 Audits in 2016, Covered Entities and Business Associates should implement HIPAA privacy and security policies, and re-examine third party vendor relationships and confirm they have up-to-date Business Associate Agreements in place where required.

  PVLR ISSN 1538-3423

OCR compliance auditors will check to make sure that Covered entities and Business Associates have compliance Business Associate agreements with third-party vendors. Thus, Covered entities and Business Associates should maintain ongoing monitoring, evaluation, audit, and compliance programs in place to ensure that HIPAA policies and procedures (including Business Associate Agreement provisions) are being complied with. Business Associate agreements are important because they document the Business Associate's contractual obligation to adopt appropriate administrative, physical and technical safeguards.