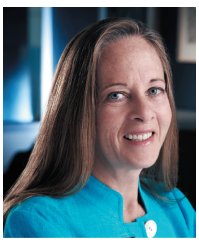
Bloomberg BNA

BNA's
Health Care Policy Report™

COMPLIANCE

PRIVACY

Practical Steps for Business Associate Compliance With the HIPAA Final Rule



BY DEBORAH GERSH AND JENNIFER ROMIG

On January 25, 2013, the Department of Health and Human Services ("HHS") published a final rule (the "Final Rule") modifying the regulations developed under the Health Insurance Portability and Accountability Act ("HIPAA") (21 HCPR 119, 1/28/13). Notably, the Final Rule modified the standards previously set forth in the Privacy Rule,[1] the Security Rule[2] and the Enforcement Standards.[3] Additionally, the Final Rule implements statutory amendments under the Health Information Technology for Economic and Clinical Health ("HITECH") Act by modifying the interim Breach Notification Rule.[4]

The Final Rule went into effect on March 26, 2013. Covered entities (that is, health care providers, health plans and health care clearinghouses), and business associates, such as certain third party administrators, consultants and accountants, have until September 23, 2013, to comply with its provisions. Because the Final Rule allows for the HHS Office for Civil Rights ("OCR") to regulate business associates for the first time, the financial and operational impact on business associates will be significant. Business associates and their subcontractors are now directly liable to OCR for violations of HIPAA and its underlying regulations. In addition, the Final Rule expands the definition of "business associate" to capture additional individuals and entities that have access to protected health information ("PHI"). Unlike traditional covered entities, such entities are likely to be smaller organizations lacking a HIPAA-compliant infrastructure. This article discusses how these two factors, in combination with a rapid timeframe for compliance, will create potential challenges for business associates, and provides practical steps

[1] The privacy standards, at 45 C.F.R. parts 160 and 164, subparts A and E.

[2] The security standards, at 45 C.F.R. parts 160, 162 and 164, subpart C.

[3] The enforcement standards, at 45 C.F.R. part 160, subparts C, D, and E.

[4] The final rule on Breach Notification for Unsecured Protected Health Information, at 45 C.F.R. part 164, subpart D.

Deborah Gersh is a partner in Ropes & Gray LLP's health care practice group. She is located in the firm's Chicago office and can be reached at Deborah.Gersh@ropesgray.com. Jennifer Romig is an associate in the health care practice group. She can be reached at Jennifer.Romig@ropesgray.com.

 ISSN 1068-1213

business associates can take to comply with the Final Rule by September 23, 2013.

I. The Final Rule Creates Direct Liability for Business Associates for Non-Compliance with HIPAA.

Prior to the implementation of the Final Rule, business associates did not face the current regulatory pressures for non-compliance with HIPAA because OCR did not have the authority to impose penalties for non-compliance. Instead, business associate liability was contractual, which limited business associate liability for any failure to comply with provisions contained in business associate agreements. As a result, prior to the Final Rule many business associates may have decided that the associated risk and costs resulting from any potential breach of contract did not justify the implementation of a robust HIPAA-compliant infrastructure. The cost-benefit analysis has materially shifted under the Final Rule, however, as business associates and their subcontractors are now directly liable for violations of HIPAA and its regulations. Consequently, there is a higher risk for those business associates who fail to comply with applicable HIPAA requirements.

In particular, the Final Rule clarifies that business associates are directly liable to OCR for:

- impermissible uses and disclosures of PHI;
- failure to provide timely breach notification to a covered entity;
- failure to provide access to a copy of electronic PHI to either the covered entity or the individual, as specified in the business associate agreement;
- failure to disclose PHI where required by the Secretary of HHS to investigate or determine the business associate's compliance with HIPAA and the regulations thereunder;
- failure to provide an accounting of disclosures, to the extent required under the business associate agreement;
- failure to comply with the administrative, technical and physical safeguards under the Security Rule, including conducting a risk analysis assessment of the business associate's systems and processes;
- failure to make reasonable efforts to limit PHI to the minimum amount necessary to accomplish the intended purpose of the use, disclosure or request; and
- failure to enter into business associate agreements with subcontractors that create or receive PHI on their behalf.

OCR may now directly impose civil monetary penalties (''CMPs'') on business associates who violate the above provisions. The Enforcement Rule provides for increasing penalties based upon a business associate's level of culpability for the violation, ranging from ''did not know,'' ''reasonable cause,'' ''willful neglect—corrected,'' to ''willful neglect—not corrected.'' OCR will consider the nature of the violation, the nature and extent of harm resulting from the violation, the business associate's history of prior compliance with HIPAA and the financial condition of the business associate prior to levying CMPs. CMPs can range from $100 to $50,000 per violation, with a cap of $1.5 million per year for multiple violations of identical HIPAA provisions in a calendar year. In addition, the business associate and certain employees, such as directors, employees or officers, may be subject to criminal penalties, which can include both financial penalties and imprisonment.

II. The Final Rule Expands the Definition of Business Associate.

The Final Rule also expands the definition of business associate to include persons who, on behalf of a covered entity or an organized health care arrangement (''OHCA''), ''create, receive, maintain or transmit'' PHI in order to perform certain functions or activities. In particular, this expanded definition of business associate captures:

- downstream subcontractors that create, receive, maintain or transmit PHI on behalf of business associates;
- health information organizations and other entities that transmit and require access on a routine basis to PHI (with an exception for entities that are mere conduits, such as Internet Service Providers);
- entities that, on behalf of a covered entity or an OHCA, handle PHI for patient safety activities carried out by or on behalf of a patient safety organization or a health care provider; and
- subcontractors that offer personal health records on behalf of covered entities.

Ultimately, this expanded definition captures persons not considered business associates prior to the implementation of the Final Rule. These new business associates are often smaller operations without existing HIPAA-compliant infrastructure. With such a short timeframe for compliance before the Final Rule goes into effect, each individual or entity whose functions or activities involve creating, receiving, maintaining or transmitting PHI must determine whether it is now a business associate under HIPAA. Importantly, compliance with the Final Rule is not determined based upon whether a business associate agreement is in place, but rather is determined based upon whether the organization is captured under the revised definition of ''business associate.'' As a result, the obligation to comply with HIPAA attaches even if an organization has no business associate agreements in place. It is each organization's responsibility to evaluate its access to PHI and the services it performs in order to determine whether it is a business associate in any of its relationships with covered entities or other business associates.

III. Practical Steps to Business Associate Compliance with HIPAA and its Underlying Regulations, including the Final Rule.

As the September 23, 2013, deadline for compliance with the Final Rule requirements grows near, business associates should take practical steps to ensure their

  HCPR ISSN 1068-1213

compliance responsibilities. The following are practical steps for compliance, both for new business associates captured by the expanded definition of business associate in the Final Rule, and for business associates seeking to ensure that their infrastructure is HIPAA-compliant, including their operational practices, policies and procedures, and business associate agreements.

1. Business Associates Should Ensure Their Operational Practices are HIPAA-Compliant.

Business associates should ensure their operational practices permit them to fully comply with applicable requirements of HIPAA and the HHS regulations promulgated thereunder. To begin, business associates should confirm they have complied with all applicable operational HIPAA requirements, such as appointing a Security Officer responsible for developing and implementing policies and procedures required under the Security Rule. In addition, business associates should consider whether it also needs to appoint other individuals (*i.e.,* a Chief Compliance Officer and/or Privacy Officer) to assist the business associate to achieve and maintain HIPAA compliance. Finally, business associates should review their technical systems to ensure that they are able to support the changes required to become HIPAA-compliant.

2. Business Associates Should Review Their Practices, Policies and Procedures Regarding the Investigation and Notification of Breaches of PHI.

The Final Rule changes how business associates investigate breaches of PHI and make the required notifications associated with those breaches. A breach occurs under HIPAA if there is an acquisition, access, use or disclosure of PHI not permitted under the Privacy Rule, which compromises the security or privacy of the PHI. Prior to the implementation of the Final Rule, HIPAA had a ''risk of harm'' threshold—that is, in order to determine whether there was a breach, business associates assessed whether the use or disclosure posed a significant risk of financial, reputational or other harm to the individual whose PHI was acquired, accessed or disclosed. With the implementation of the Final Rule, there is now a rebuttable presumption of a breach if PHI has been acquired, accessed, used or disclosed in a manner that violates the Privacy Rule. The business associate may rebut this presumption if it can demonstrate, through a multi-factor assessment, that there is a low likelihood that an individual's PHI has been compromised. Alternatively, the business associate can accept the presumption that a breach has occurred, document the incident, and contact the relevant parties.

As a result of these changes, business associates must examine their current practices with regard to the investigation and notification of breaches of PHI. At a minimum, business associates should revise their investigation and notification practices, as well as their breach notification policies and procedures, to reflect the data breach standard implemented under the Final Rule. In addition, business associates should consider how they will conduct breach investigations and how they will train their workforce members on the new breach notification requirements.

3. Business Associates Should Review and Revise Their Policies and Procedures.

Business associates must update current policies and procedures to reflect additional changes imposed by the Final Rule. To start, business associates should conduct a HIPAA security risk analysis, in accordance with 45 C.F.R. 164.308(a)(1) of the Security Rule. The risk analysis assists business associates in assessing their potential risks and vulnerabilities to the confidentiality, integrity and availability of electronic PHI held by the business associate. After conducting a risk analysis, business associates should address any identified gaps in their policies and procedures, as well as in their operational practices and controls. Specifically, under the Final Rule business associates should add or make changes to the following:

- breach notification policies and procedures that incorporate the new method for analyzing breaches of PHI;
- policies and procedures related to the Privacy Rule, including policies involving fundraising, marketing, individual rights with regard to their PHI, and certain uses and disclosures; and
- policies and procedures related to the Security Rule, including policies involving business associate agreements.

4. Business Associates Should Review and Revise Their Business Associate Agreements.

Business associates should review and revise their current business associate agreements to reflect the changes imposed by the Final Rule. The HHS OCR website has a helpful tool here containing sample business associate agreement provisions (http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html). In particular, the Final Rule imposes additional obligations on business associates which should be included in business associate agreements with covered entities and subcontractors to require the business associate to:

- comply with the Security Rule regarding electronic PHI;
- report to the covered entity any breach of PHI of which the business associate becomes aware; and
- to the extent the business associate carries out a covered entity's obligation under the Privacy Rule, comply with provisions of the Privacy Rule that would apply to the covered entity in carrying out such obligations.

Business associates should also revise their business associate agreements with subcontractors to require subcontractors to agree to the same restrictions and conditions that apply to the business associate with respect to PHI created, maintained or transmitted on behalf of the business associate. For example, if a business associate does not have permission from the covered entity to aggregate PHI, it should ensure that the subcontractor does not have permission to aggregate PHI. In addition, business associates should review their relationships with vendors and other subcontractors more generally in order to determine whether any are now subcontractor business associates under the Final Rule.

Business associates should also consider whether to include provisions in subcontractor business associate agreements that would provide additional protection, such as requiring subcontractors to:

- provide adequate training to their workforce members;
- represent that neither the subcontractor, nor any of the entities or individuals that the subcontractor employs or contracts with, is excluded from participation in any federal health care program or listed by the HHS or the General Services Administration's Excluded Parties List System (now encompassed within the System for Award Management) as an excluded party;
- maintain insurance covering acts or omissions of the subcontractor or members of its workforce in violation of HIPAA or the regulations thereunder; and
- indemnify the business associate for any and all damages arising from subcontractor's acts or omissions with respect to subcontractor's responsibilities under HIPAA or its business associate agreement.

In many cases, business associates may face pushback from subcontractor business associates who are not accustomed to compliance with business associate agreements or these potentially broad provisions. However, as subcontractor business associate agreements are also now subject to HIPAA, subcontractor business associates must also implement required elements under the Final Rule.

Business associates will face challenges in implementing the required provisions under the Final Rule. These challenges may be both operational and fiscal, particularly for those business associates currently without existing HIPAA policies and procedures, refined business associate agreements and an internal computerized system that meets the requirements of the Security Rule.

  HCPR ISSN 1068-1213