STRATEGIC MANAGEMENT SERVICES

Guidance for Compliance Officers Assuming Responsibility for HIPAA Privacy

Richard P. Kusserow | March 2024

Key Points:

- **General Background**
- **Covered Entities vs. Business Associates**
- **HIPAA Privacy Compliance Checklist**
- **Options for Managing HIPAA Privacy Compliance**

General Background. The Health Insurance Portability and Accountability Act (HIPAA) created an outline of an organization's legal obligations concerning healthcare data management, including the right of patients to have privacy, the necessity for appropriate security controls to protect private data, and the requirements for addressing any breaches in the data by a third party. The HIPAA Privacy Rule establishes the national standard for patients' privacy and private information rights. Furthermore, it sets up the framework that dictates what electronic protected health information (ePHI) is, how it must be protected, how it can and cannot be used, and how it can be transmitted and stored. HIPAA enforcement has been assigned to the Department of Health and Human Services (DHHS) Office for Civil Rights (OCR). Although HIPAA has been in effect since 1996, HIPAA compliance remains a difficult problem for many healthcare organizations. In recent years, responsibility for HIPAA Privacy compliance has increasingly fallen under the Compliance Officer, creating a whole new set of duties and responsibilities, which, for many, has been a whole new learning area.

Covered Entities vs. Business Associates. One of the first compliance issues is identifying how HIPAA applies to the organization and the parties with whom the organization does business. The fundamental question is determining the difference between a Covered Entity and a Business Associate (BA). The difference between the two lies in the level of compliance controls needed. Under HIPAA, a Covered Entity includes health plans, clearinghouses, or health care providers

that submit electronic claims information, and organizations that transmit claims information electronically for healthcare activity for which they receive payment. As such, the question here would be whether the person, business, or agency furnishes, bills, or accepts payment for health care in the ordinary course of business. If so, they are a Covered Entity. Business Associates, in contrast, consists of third-party entities that assist Covered Entities and, in doing so, have access to the Covered Entity's Protected Health Information (PHI).

Additionally, a Covered Entity could be considered a BA to another covered entity. Any individual or organization that is a BA must comply with HIPAA rules; if they do not, they could be subject to financial penalties. BAs engaged by a Covered Entity must be documented and tracked, with specific contracts specifying what function the BA has been committed to perform and their acknowledgment that they must be HIPAA-compliant. The Covered Entity is responsible for ensuring that any BAs they engage comply with the HIPAA rules. While HIPAA does not explicitly mandate organizations to hire dedicated HIPAA compliance staff, it does require them to have a designated person (HIPAA Privacy Officer) responsible for overseeing the development, implementation, maintenance of, and adherence to privacy policies and procedures regarding the safe use and handling of protected health information (PHI) in compliance with HIPAA and other state and federal law regarding privacy. In fulfilling these responsibilities, the Privacy Office needs to develop, implement, and monitor the HIPAA Privacy program, ensure ongoing compliance, and investigate reported breaches in PHI. In determining responsibilities for protecting PHI, it is necessary to have a third-party gap analysis of required policies/procedures, security controls, and business processes.

HIPAA compliance requirements include the following:

1. Ensuring patients' rights to PHI;
2. Establishing and maintaining physical, technical, and administrative security measures;
3. Conducting prompt and complete investigations of any breach in PHI;
4. Taking proper steps in Breach Notification, if a breach occurs, and
5. Ensuring Business Associates comply with HIPAA.

The following is a summary checklist for HIPAA Privacy compliance:

1. Designate a Privacy Officer
2. Develop and implement written policies and procedures
3. Provide HIPAA training for the workforce
4. Keep track of all BAs
5. Obtain patient consent for certain disclosures
6. Maintain appropriate safeguards for protected PHI
7. Implement a system for reviewing and verifying requests for PHI
8. Respond to patient requests for access to PHI
9. Notify patients in the event of a breach of unsecured PHI
10. Assign unique identifiers to individuals and groups
11. Establish a process for disclosing PHI to BAs and other third parties
12. Promptly investigate potential data breaches
13. Establish a process for Breach Notification
14. Ensure Business Associates are complying with HIPAA
15. Establish proper steps in Breach Notification if a breach occurs

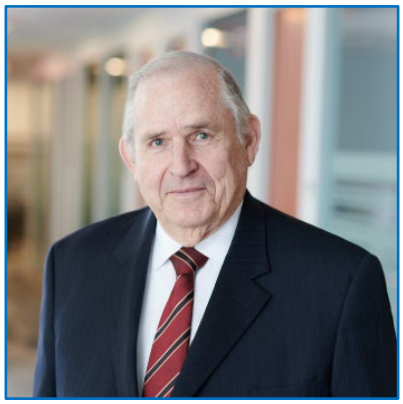
Options for managing HIPAA Privacy compliance. Compliance Officers assuming responsibility for HIPAA Privacy compliance must quickly implement all the actions, steps, assessments, processes, governing policies, and training needed for HIPAA compliance. To meet this challenge, there are several approaches the Compliance Officer can take to manage the function:

1. Have the existing HIPAA Privacy Officer report to them and continue existing operations. It is crucial to ensure that the individual has an in-depth understanding of HIPAA regulations, including the Privacy and Security Rules. Lack of expertise could result in misinterpretation or incomplete implementation of HIPAA requirements.
2. Assume the added title and responsibility as the Privacy Officer, which not only brings a whole new body of work but requires knowledge and expertise that may be lacking, to effectively manage the program. In its new "General Compliance Program Guidance," the OIG recognizes that many Compliance Officers now have the dual role of privacy officer and recommend that the entity ensure the Compliance Officer has sufficient staff and resources to perform the additional duties associated with the expanded role.
3. Hire a HIPAA Privacy Officer. Similarly, the person hired should have a strong understanding of HIPAA regulations, prior experience in that capacity, a deep understanding of security and privacy practices, and certifications such as Certified HIPAA Professional (CHP), Certified HIPAA Privacy Security Expert (CHPSE), or Certified in Healthcare Privacy and Security (CHPS).

4. Contract out the Designated HIPAA Privacy Officer to a HIPAA Expert Consultant on a temporary interim basis to bring the program up to standard and then either shift the position in-house or keep the expert consultant permanently. Consultants who are experts in HIPAA Privacy compliance can quickly address the complex data privacy laws and ensure alignment with rules. The work, by and large, can be performed remotely and could begin with the initial privacy assessment to identify gaps.

More information on this subject can be found at https://www.compliance.com/privacy-security/

You can also keep up-to-date with Strategic Management Services by following us on **LinkedIn**.



About the Author

Richard P. Kusserow established Strategic Management Services, LLC, after retiring from being the DHHS Inspector General, and has assisted over 2,000 health care organizations and entities in developing, implementing and assessing compliance programs.