JILLIAN BOWER / CAMELLA BOATENG

Meeting the Privacy Officer Challenge: Outsourcing Might Be the Answer

Jillian Bower, MPA, and **Camella Boateng**, MPH, are consultants and analysts with Strategic Management Services, LLC (SMS), a firm that has provided compliance advisory services to thousands of health care entities for 18 years. SMS has also worked with numerous clients of varying size to provide support to their HIPAA privacy compliance activities, including acting as the designated privacy officer for organizations. For additional information regarding Strategic Management Services, please contact Jillian Bower at jbower@strategicm.com or Camella Boateng at cboateng@strategicm.com.

Outsourcing Can Be Done in Various Ways to Meet the Specific Needs of an Organization

Imagine discovering an employee's laptop has been stolen that contained thousands of patient records with protected health information (PHI). Add to it that the laptop was not password protected or encrypted. Now you are faced with having to report the breach to the Department of Health and Human Services (HHS) Office for Civil Rights (OCR) who, among other things, will post your organization's name on its public Web site. Furthermore, you also will have to report the breach of PHI to all the patients affected, as well as explain the issue to the media.

For many the above scenario has become a reality. Under the Health Information Technology for Economic and Clinical Health (HITECH) Act, enacted as part of the American Recovery and Reinvestment Act of 2009, covered entities (CEs), such as hospitals, are mandated to report PHI breaches to the HHS OCR.[1,2] As of January 12, 2011, more than 200 covered entities each compromised the PHI of at least 500 patients, leading them to report the breach to HHS.[3]

A recent study reported that data breaches of patient information cost hospitals nearly $6 billion each year.[4] The study also found that protecting patient data is not a priority among hospitals and that the majority of health care organizations experience data breaches due to inadequate preparation and staffing.[5]

Think about how this costly mistake also will cause damage to your organization's image and reputation and ask yourself: (1) Are we ready to endure the cost of PHI breaches both in dollars and cents, as well as loss of reputation; and (2) if we do not want to avoid these problems, have we allotted enough resources to ensure that PHI is properly guarded and secured?

The enactment of the HITECH Act strengthens and expands the Health Information Portability and Accountability Act (HIPAA) privacy, security, and enforcement rules. Essentially, HIPAA protects patient's health information and establishes a number of administrative, physical, and technical safeguards for CEs to follow to ensure the integrity and availability of PHI.[6]

Under the HITECH Act, CEs face more requirements such as disclosing PHI breaches to patients and HHS, extending the HIPAA privacy and security rules to business associates, prohibiting the sale of PHI, and expanding individual rights to access his or her information while restricting certain disclosures of PHI to health plans, all to protect an individual's health information.[7] HHS also has the authority to conduct formal investigations and increase penalties applied to CEs who fail to comply with the new rules.[8,9]

According to HHS officials, the OCR plans to issue new rules regarding the HITECH provisions in 2011.[10] Thus, hospitals should stay tuned as more stringent rules concerning PHI are anticipated in the near future.

The Challenging Role of the Privacy Officer

To avoid negative press and financial loss associated with PHI breaches, hospitals need to designate a HIPAA privacy officer to oversee the organization's privacy compliance. The privacy officer can be a high-profile position that plays a critical role in maintaining and overseeing the integrity, security, and confidentiality of PHI. Since the HITECH Act creates serious consequences for hospitals when a privacy violation or security breach occurs, it is essential that hospitals have privacy officers who can be the first line of defense. Hospitals should take time to reexamine the position in relation to the needs of the organization and consider the best approach to address their HIPAA privacy needs.

In most hospitals, the HIPAA privacy officer and security officer are two separate roles; the former related more to program compliance and the latter to information technology operations. In many cases, hospitals have determined the privacy officer functions to be a part-time responsibility. Other hospitals roll the privacy officer function under the compliance officer. These decisions do not always create a solution.

The privacy officer function as a part-time activity is not very realistic, and compliance officers have a full plate of duties and responsibilities that may not lend them to taking on the added burdens of the privacy officer function. The end result is that often the privacy officer function is relegated to a secondary duty without provision of adequate attention.

The reality of the matter is that the privacy officer is expected to be the focal point for all privacy compliance-related activities, and responsibilities are significant and challenging. They include, but are not limited to, the following:

- implementing privacy policies and procedures;
- coordinating the development of privacy risk assessment policies and procedures;
- developing privacy and confidentiality consent, authorization forms, and information notices;
- developing, conducting, and ensuring delivery of privacy training and orientation to all covered persons;
- providing ongoing auditing and monitoring of the privacy program;
- conducting ongoing privacy compliance monitoring;
- ongoing compliance monitoring of all business associate agreements;
- performing initial and periodic information privacy risk assessments;
- reporting periodically to the board, chief executive officer (CEO), and others on the status of the privacy program;
- providing strategic guidance to corporate officers regarding information resources and technology;
- providing leadership in the planning, design, and evaluation of privacy and security-related projects;

- developing appropriate sanctions for failure to comply with the privacy policies and procedures;
- mitigating the effects of improper use or disclosure of PHI of the workforce or business partners;
- establishing an internal privacy audit program;
- periodically revising the privacy program in light of changes in laws, regulatory, or policy;
- coordinating with the compliance officer the documenting and reporting of privacy violations;
- serving as an information privacy consultant for all departments and appropriate entities;
- developing a system to track qualified individuals' access to review or receive PHI;
- promoting privacy awareness within the organization and related entities;
- acting as a liaison to the HIPAA security officer;
- working with those involved in any release of PHI to ensure compliance with policies;
- maintaining current knowledge of applicable PHI federal and state laws and accreditation standards;
- cooperating with the OCR and other legal entities in any compliance reviews or investigations;
- submitting periodic reports regarding the status of privacy compliance; and
- revising the privacy program to comply with changes to laws, regulations, and accreditation requirements.

It is difficult to imagine how anyone could carry out all these things on a full-time basis, let alone part-time basis.

Outsourcing Privacy Officer Functions

In meeting the challenges of an effective privacy program, there are a number of approaches that can be considered. For example, hospitals that do not have the necessary internal resources to ensure the integrity, security, and confidentiality of PHI should consider outsourced assistance. This approach has been recognized by the Office of Inspector General (OIG) at a jointly sponsored roundtable with the Health Care Compliance Association. The OIG further noted in its Compliance Program Guidance that, *"[f]or those companies that have limited resources, the compliance function could be outsourced to an expert in compliance."* This same principle applies to a privacy officer function.[11]

One of the advantages of outsourcing the privacy officer function is economic. A firm providing privacy officer services can amortize all the effort of keeping current with the ever-changing laws, regulations, and accreditation requirements across a number of clients whereas this would be a significant burden for a hospital to do individually. There are also great advantages in having established experts available rather than trying to develop them internally.

Moving forward, hospitals may wish to consider the following questions when determining what functions of the privacy officer could be outsourced.

- How complex is the organization with respect to privacy and security systems?
- Is the privacy officer position currently vacant, either due to temporary leave (*i.e.*, maternity, extended medical) or turnover in the position?
- Has the organization experienced difficulties in recruiting a qualified person?
- Is the hospital equipped to handle a breach of PHI or other unexpected incidents involving PHI?
- How much time does the privacy officer dedicate to regulatory research in order to stay well informed of current and changing rules?
- Does the hospital system have a need for a corporate privacy officer as well as a privacy officer at the facility level?
- What are the privacy officer's responsibilities? Does the privacy officer wear "multiple hats" within the organization?
- Do the compliance officer's responsibilities overlap with the privacy officer's functions?

Answering these questions can lead your organization into deciding how much of the HIPAA privacy functions can be out-

sourced. For example, if the privacy officer wears multiple hats and divides his or her time, consider outsourcing certain privacy functions, such as development of policies and procedures and training. On the other hand, during any point of time when the privacy officer position is vacant, an organization should highly consider outsourcing until a permanent replacement is found.

Outsourcing is not an all or nothing choice; experienced consulting firms can provide a range of support services to help supplement the current work of an organization's privacy officer. Consider these options for outsourced assistance:

- *Option 1: Advisory Services.* Contract with an expert for a one-time engagement to handle certain duties related to HIPAA compliance, such as developing and updating HIPAA privacy policies and procedures (*i.e.*, controls on computers/laptops, access to electronic PHI, and proper disposal of PHI) or developing annual or refresher training modules.
- *Option 2: Remote Supplementary Interim Privacy Officer Services.* Outsource a portion of the responsibilities of the privacy officer on an ongoing basis to an experienced consulting firm.
- *Option 3: Engage an Onsite Interim/Designated Privacy Officer.* Hire an interim/designated privacy officer. In the absence of a permanent privacy officer, the hospital should considering hiring an interim privacy officer while looking to fill the position. The interim privacy officer can maintain the HIPAA privacy activities as well as provide a fresh perspective of the current activities within the hospital.

Take Home Message

Outsourcing can be done in various ways to meet the specific needs of the organization. A consulting firm can handle the daily duties of the privacy officer, including carrying out investigations of alleged privacy violations; handling privacy-related concerns and issues reported through the hot line; providing regulatory analysis on new and updated laws and rules; advisory and best practices support; and providing support of current duties of the privacy officer without necessarily being at the hospital. A designated or interim privacy officer can work either onsite or offsite.

Further, the role can be a full-time or part-time position or can just be available "on call" to support remaining compliance staff when needed. A final factor to consider is the relationship with the compliance officer and the strength of the current compliance program.

The authors have been involved in providing various levels of privacy services. In some cases, it is merely a matter of developing the infrastructure for the program, including developing privacy-related policies and procedures, risk assessment protocols, as well as the confidentiality consent, authorization forms, and information notices. In many cases, this extends to developing the necessary educational programs and briefing senior management and the board on what is required in an effective program. Some smaller hospitals prefer just outsourcing all the duties and responsibilities of the privacy officer function.

Endnotes

1. A covered entity is defined as a health plan, health care clearinghouse, or health care provider who transmits any health information in electronic form. Additional information concerning covered entities is available at www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/index.html.
2. American Recovery and Reinvestment Act of 2009, Pub. L. No. 11-005, 123 Stat. 226.
3. "Breaches Affecting 500 or More Individuals." Department of Health and Human Services Office for Civil Rights. 2011. Accessed 12 Jan. 2011. www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html.
4. "Benchmark Study on Patient Privacy and Data Security." Ponemon Institute. Nov. 2010.
5. *Id.*
6. 45 CFR Part 164.
7. *Supra.* n. 2.
8. 45 CFR Part 160.
9. *Supra.* n. 2.
10. "HITECH, HIPAA Rules to Launch Simultaneously in 2011." Health Leaders Media. 2011. Accessed 12 Jan. 2011. www.healthleadersmedia.com/content/

TEC-260186/HITECH-HIPAA-Rules-to-Launch-Simultaneously-in-2011.
11. "Building a Partnership for Effective Compliance. A Report on the HCC-OIG Physician's Roundtable." HCCA Conference in Philadelphia, PA. 24 Jul. 2000. Accessed 14 Jan. 2011. oig.hhs.gov/fraud/docs/complianceguidance/roundtable0700.pdf.

Reprinted from Journal of Health Care Compliance, Volume 13, Number 2, March-April 2011, pages 33-37, with permission from CCH and Aspen Publishers, Wolters Kluwer businesses.
For permission to reprint, e-mail permissions@cch.com.