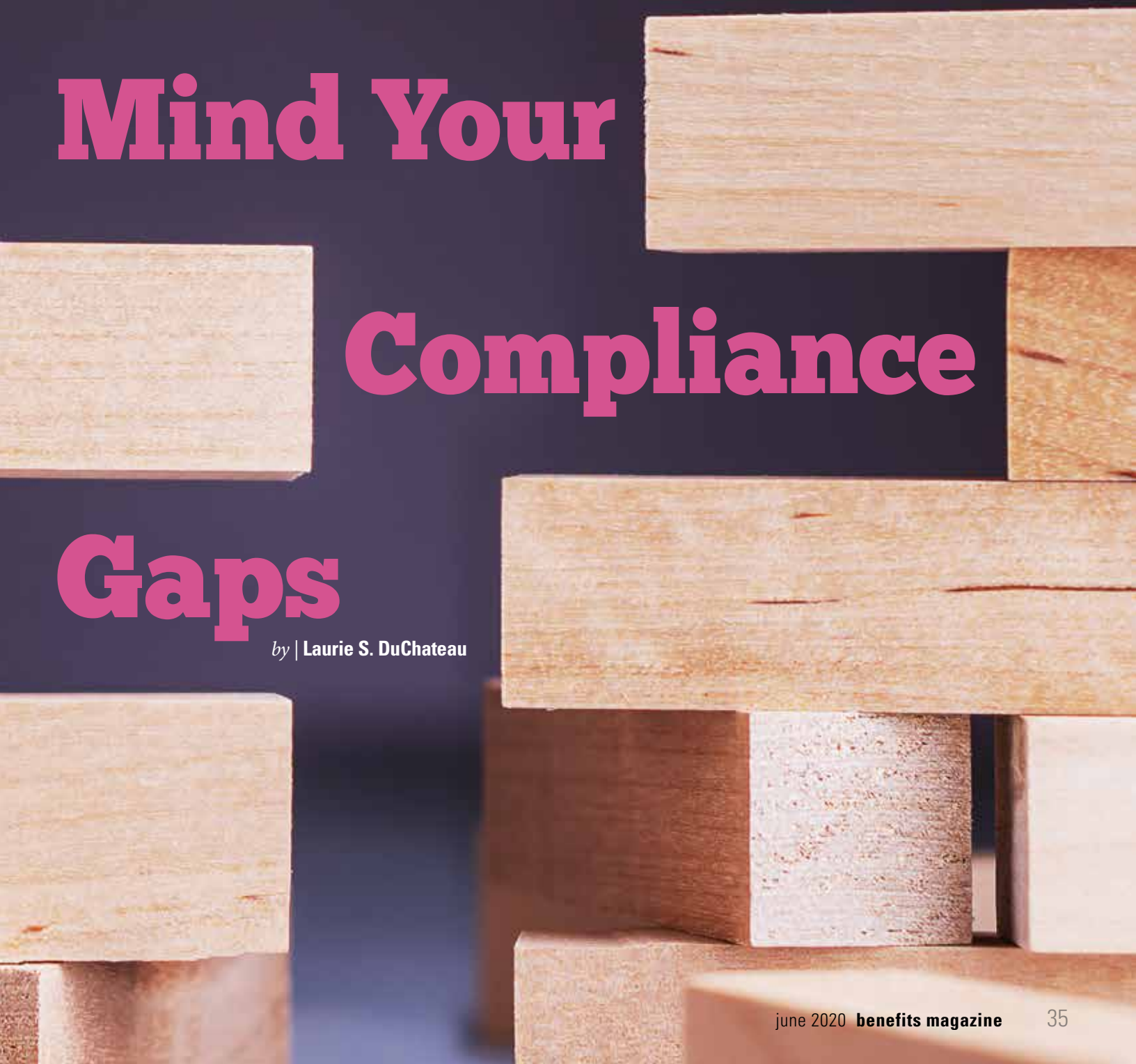
A breach of protected health information (PHI) could place group health plan sponsors at risk for fines for failing to comply with the Health Insurance Portability and Accountability Act (HIPAA). Risk analysis and workforce training are among the areas health plans commonly struggle with in their HIPAA compliance efforts.

HIPAA: Mind Your Compliance Gaps

by | **Laurie S. DuChateau**



Protecting the sensitive personal health information of your group health plan participants is not only a legal obligation under the Health Insurance Portability and Accountability Act (HIPAA)—complete with hefty fines for breaches of that protection—it is part of building trust in your organization. As such, if your organization sponsors a group health plan that is subject to HIPAA, the plan is considered a *covered entity,*[1] and as the plan sponsor, you have a responsibility to assure compliance. Common but critical gaps in compliance with this law include the following.

- **Infrequent risk/threat analysis.** Employer plans should conduct a risk and threat analysis to be compliant. Although the Department of Health and Human Services (HHS) does not state how often this should be done, conducting an annual analysis is a best practice. The risk assessment should be readily available for management and auditors.
- **Missing or outdated business associate agreements (BAAs).** Employer plans should embed the BAA in the contract process and conduct annual inventories of current business associates and business associate agreements.
- **Inadequate workforce training.** Employer plans should conduct training on a regular basis for any employee or contractor who works with PHI.
- **Outdated privacy and security policies.**

Protected health information (PHI) and *electronic protected health information* (ePHI) maintained by group health plans are medical records and other individually identifiable data, such as Social Security numbers, diagnosis codes and treatment information. This information is highly personal and is afforded protections under HIPAA. Any unintended disclosure of PHI can have negative consequences for the individual involved, as well as for the group health plan that failed to have the appropriate protections and protocols in place to ensure this sensitive data was safeguarded.

Over the last few years, the U.S. Department of Health and Human Services Office of Civil Rights (OCR), which enforces HIPAA, has ramped up its investigations of reported breaches of PHI, resulting in significant monetary settlements. The largest settlements have involved health care providers. In 2018 (the latest figures available) the average settlement was $3.2 million. Common violations occur due to improper disposal of PHI, insufficient security controls to counter hacking, malicious software/malware, lost or stolen devices, and lack of training.

Investigations are typically spurred by complaints. To avoid an unintended breach of privacy, sponsors of group health plans must make a commitment to evaluate their need for and exposure to PHI and ePHI. Part of that commitment is taking an honest look at their compliance with HIPAA privacy and security rules.

Following are some areas that organizations struggle with when it comes to this law.

Infrequent Risk/Threat Analysis

HIPAA requires a risk/threat analysis to identify vulnerabilities that could impact the confidentiality, integrity and availability of PHI maintained by a covered entity or business associate. Best practice dictates conducting an analysis annually, especially with cyberattacks on the rise. Although HIPAA risk/threat analyses are often thought of as specific to HIPAA security, in conducting a full HIPAA review, risks and threats under the HIPAA privacy rule[3] would also be evaluated.

The Buck *2019 HIPAA Readiness Survey* found that 42% of survey respondents did not know when a risk/threat analysis was last conducted, or they last conducted one more than five years ago.[4]

Specifically, the HIPAA audit protocol, which addresses the elements of privacy, security and breach notification that was issued and updated by HHS in July 2018, recommends that the last two risk analyses or the two prior updates to the risk analysis be readily available to the HHS auditor. (In the author's experience, they are often not readily available.) Most of the risk/threat analysis documents do not specifically ap-

learn more

Education

HIPAA Privacy
E-Learning Course
Visit *www.ifebp.org/elearning* for more details.

39th Annual ISCEBS Employee Benefits Symposium
August 23-26, San Diego, California
Visit *www.ifebp.org/symposium* for more information.

From the Bookstore

HIPAA Privacy for Health Plans After HITECH
Reinhart Boerner Van Deuren. 2013.
Visit *www.ifebp.org/books.asp?8950* for more details.

ply to applications containing *HIPAA-inventoried PHI/ePHI* (any system, application or storage area where PHI is stored, maintained or transmitted from). Rather, they apply to protected information maintained within the entire organization, which often does not address HIPAA-specific requirements. (Organizations should expand existing security analyses to include HIPAA risks, and IT departments could include PHI in their own risk/threat analyses.) Moreover, if HIPAA-related risk analyses do exist, they frequently are dated between 2003-2005, when the HIPAA privacy and security rules first came out.

Lessons Learned and Best Practices

HIPAA compliance is not a one-and-done exercise. A group health plan's risk/threat analysis needs to be reviewed regularly so the information remains current and the document provides a detailed understanding of the risks associated with maintaining the confidentiality, integrity and availability of PHI. The following triggers, among others, may necessitate a risk/threat analysis.

- New threats occur, such as the emergence of ransomware and phishing.
- ePHI-containing systems are replaced and/or updated.
- New PHI is introduced into the environment and is collected, stored, maintained and/or transmitted.
- New vendor relationships are established.
- Merger/acquisition activity occurs.
- Technology, environmental processes or business processes change.

The risk/threat analysis is most likely the first document auditors will request. Group health plans should use this information to identify, prioritize and manage potential security risks to protected information.

Missing or Outdated Business Associate Agreements (BAAs)

BAAs are contracts between covered entities and business associates (BAs). The BAA specifies each party's responsibilities, roles and liabilities when it comes to PHI. HIPAA requires covered entities to work only with BAs who assure complete protection of PHI, and it requires that BAs safeguard PHI. It is important to retain a list of all current BAs and to read and understand the language in BAAs. The reality is when a breach or any other kind of security incident happens, the plan sponsor is at risk for what was declared in the BAAs.

According to the Buck HIPAA survey, 33% of respondents either have not inventoried their BAAs or did not know whether they had done so.

Group health plans frequently do not have an updated inventory of their BAAs and/or the agreements are dated prior to September 2013, when the Health Information Technology for Economic and Clinical Health (HITECH) Act became effective. The HITECH Act was created to provide monetary incentives to U.S. health care providers for implementing electronic health records (EHRs) and supporting technology. This means that many of the BAAs do not reflect new obligations imposed upon business associates by HITECH.

Group health plan sponsors often have BAAs with the usual suspects, such as insurers (medical, dental, flexible spending account, etc.) and their health care consultants, but they too often fail to remember to secure or execute them for other entities, such as cloud providers (i.e., Microsoft), shredding companies, off-site storage, outside legal counsel, etc. Another problem that frequently crops up is the inability to find HIPAA documentation, including BAAs.

Lessons Learned and Best Practices

Keep an updated inventory of BAAs and continually review these documents. Store the inventory list and agreements in a place that is accessible and easily found. If your group health plan is audited, you'll need to turn these documents over to OCR within ten days. Finally, cast a wide net in thinking about who your BAs are beyond the obvious partners. Examples of BAs include:

- Answering services
- Billing companies
- Copier/printer/scanner vendors
- External benefit call centers
- Health benefit consultants
- Insurers
- External IT groups/support
- Medical transcription
- Off-site storage
- Outside legal counsel/auditors
- Shredding services
- Outsourced customer service/call centers
- Cloud providers.

Inadequate Workforce Training

In general, HIPAA privacy and security training should cover HIPAA definitions, patients' rights, the HIPAA Privacy Rule, disclosures of PHI, breach notifications, BAAs, the HIPAA

Security Rule, safeguarding ePHI, and violations and sanctions.

Workforce training is important not only to help prevent breaches, but also to create awareness of what constitutes a breach. Lack of staff training for members of the workforce who are exposed to PHI was cited as a primary area of concern by OCR in its audit reviews.

The Buck survey found that 35% of respondents last offered HIPAA training between one and five years ago, 13% provide training only during onboarding and 10% did not know when HIPAA training was last provided.

Training materials are often outdated, do not include both privacy and security components, or simply cannot be found. Often, organizations that sponsor a group health plan conduct training only for employees in the HR and benefits departments. However, it is just as critical to train the finance, payroll, legal, risk management and IT department staff as well as any temporary employees and contractors who have access to PHI.

Lessons Learned and Best Practices

Be diligent about whom to include in training. Ensure that all employees with access to PHI and ePHI are trained to mitigate the likelihood of a breach, the potential of fines and the need for corrective action plans. Provide refresher training at least annually and upon onboarding for any new employee with access to PHI. Be prepared to demonstrate that employees were trained.

Other Common Compliance Gaps

Other common compliance gaps include the following.

- Privacy policies and procedures, as well as security policies and procedures, have not been updated in many years.
- Encryption is not implemented for ePHI on removable media, network drives or email transmissions, and security controls or updated virus protection were not present on personal devices used to access ePHI. (Workplaces that have bring-your-own-device (BYOD) policies introduce additional risks.)
- The review of permissions for, and access to, PHI/ePHI is insufficient, along with termination procedures for workforce members with access to PHI/ePHI.
- Documented policies and procedures are not adequately communicated and therefore not followed.
- Privacy and/or security officials are not designated.

Review HIPAA Compliance Regularly

HIPAA compliance must be addressed continuously. It is not something that can be considered once and then put on the shelf. In fact, HIPAA policies and procedures should be widely shared and accessible to all employees. Doing so demonstrates the organization's commitment to data privacy and security. Ensuring their visibility also means that the information won't be lost with inevitable changes in personnel.

Furthermore, while employees handling PHI receive more detailed training that specifically addresses how to handle data associated with the group health plan, it's definitely worth considering providing a basic level of privacy and security training to all employees.

Strong Governance

Strong governance is essential to protecting information. Clear, well-developed and implemented policies and procedures are vital and required under HIPAA. The best way to significantly reduce the likelihood of a breach of the rules is to perform a review of group health plan policies and procedures annually, and adjust when there are changes in the environment, staff, threats or the law. This will help you stay on top of your HIPAA compliance obligations and greatly reduce the risk of exposing the data that employees and their families have entrusted to you.

takeaways

- The U.S. Department of Health and Human Services Office of Civil Rights (OCR) has ramped up its investigations of breaches of protected health information (PHI) in recent years.
- Under the Health Insurance Portability and Accountability Act (HIPAA), group health plans are required to protect PHI and electronic PHI (ePHI).
- Common HIPAA compliance gaps include failing to regularly conduct a risk/threat analysis, having outdated or missing business associate agreements (BAAs), inadequate training, and out-of-date privacy and security policies and procedures.
- HIPAA compliance should be addressed continuously, and HIPAA policies and procedures should be widely shared and accessible to all employees.

Endnotes

1. *A covered entity* is a health care provider (doctors, psychologists, clinics and so on) that transmits any information in electronic form related to a transaction such as medical claims. Health plans (health maintenance organizations, insurers, company health plans and government programs such as Medicare, Medicaid and others that pay for health care), covered entities and business associates (a person or entity working on behalf of a covered entity whose services involve the use or disclosure of protected health information) are subject to and must comply with Health Insurance Portability and Accountability Act (HIPAA) privacy rules. See www.hhs.gov.
2. *Protected health information (PHI)* is individually identifiable health information, including demographic information, collected from an individual, that (1) is created or received by a health care provider, health plan, employer or health care data clearing house and (2) relates to the past, present or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present or future payments for the provision of healthcare to an individual.
3. The HIPAA Privacy Rule addresses the use and disclosure of individuals' health information—called PHI—by covered entities, as well as standards for individuals' privacy rights to understand and control how their health information is used. See www.hhs.gov.
4. Buck, *2019 HIPAA Readiness Survey:* https://buck.com/wp-content/uploads/2020/01/buck_pub_survey_hipaareadiness2019_report_web.pdf.

bio

Laurie S. DuChateau is the principal and leader of the U.S. compliance consulting practice at Buck, where she is responsible for the firm's cross-practice compliance consulting, publications, research and training. She joined Buck in 2011 and has more than 25 years of experience in the area of employee benefits. Before joining Buck, DuChateau was an employee benefits attorney in private practice for more than 20 years representing numerous Fortune 250 clients. She holds a J.D. degree from Duquesne University School of Law and a bachelor's degree in political science from Westminster College. She is also a member of the Allegheny County Bar Association.

benefits MAGAZINE

pdf/620