Consulting

2019 HIPAA Readiness Survey

January 2020

BUCK

About Buck

Buck is an integrated HR and benefits consulting, technology, and administration services provider. Headquartered in New York City, with international operations, Buck is focused on helping its clients realize the best organizational performance for their business while driving positive health, wealth, and career outcomes for their people. Driven by best-in-class technology and leading analytics capabilities, our consulting solutions and easy-to-use administration platforms are helping the world's most forward-thinking companies re-envision and re-design the way that employees work and live.

HIPAA compliance is important for everyone.

Executive summary

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires healthcare providers, health plans, healthcare clearinghouses (covered entities) and business associates to adhere to rules for protecting health information. It ensures the confidentiality and privacy of an individual's health information.

Over the last few years, the U.S. Health & Human Services' (HHS) Office of Civil Rights (OCR – HIPAA's enforcement arm) has ramped up its investigations of reported breaches, resulting in some of the largest monetary settlements in HIPAA's history.

Buck conducted the 2019 HIPAA Readiness Survey to garner insight into HIPAA compliance awareness and areas that need to be addressed to be in full compliance with HIPAA.

The survey results show that organizations are not fully compliant with HIPAA rules nor are prepared for a HIPAA audit. In particular:

- **42%** of survey participants did not know when a risk/threat analysis was last conducted or last conducted one more than five years ago.
- **33%** of survey respondents either have not inventoried their business associates or did not know if they have done so; **16%** did not have current business associate agreements, or did not know if they had them.
- **35%** indicated they 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.

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 maintain up-to-date policies and procedures and periodically conduct operational reviews to determine that the policies are being followed.

Contact us

This survey was conducted by the Knowledge Resource Center at Buck. For additional information, contact **talktous@buck.com** or **800 887 0509**.

buck.com

HIPAA Readiness Survey results

HIPAA policies and procedures review

Under the HIPAA rules, covered entities must not only have processes in place to safeguard protected health information (PHI), they must also have HIPAA privacy and security policies in place, periodically review the procedures, and update or modify them as necessary.

Covered entities and business associates should evaluate HIPAA privacy and security policies and procedures whenever one or more of the following events occur:

- Changes in the HIPAA security regulations or privacy rules
- New federal, state, or local laws or regulations affecting the privacy or security of ePHI
- Changes in technology, environmental processes or business processes that may affect HIPAA security policies or procedures
- A serious security violation, breach, or other security incident occurs

HIPAA policies and procedures review – Breach Notification

All HIPAA covered entities and business associates must familiarize themselves with the HIPAA breach notification requirements and develop a breach response plan that can be implemented as soon as a breach of unsecured protected health information (PHI) is discovered.

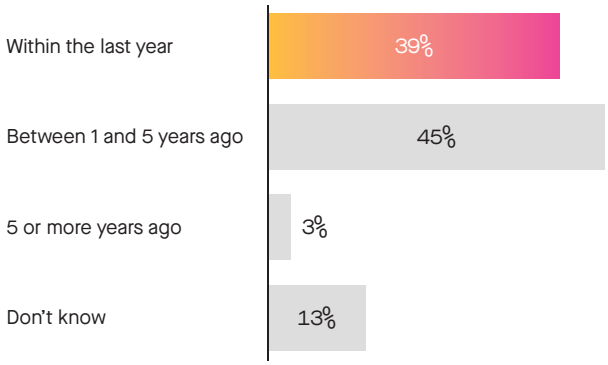
The HIPAA breach notification rule requires covered entities to notify affected individuals, Health and Human Services (HHS), and, in some cases, the media of a breach of unsecured PHI. The breach notification rule also requires business associates of covered entities to notify the covered entity of breaches at or by the business associate.

Failure to comply with HIPAA breach notification requirements can result in a significant financial penalty.

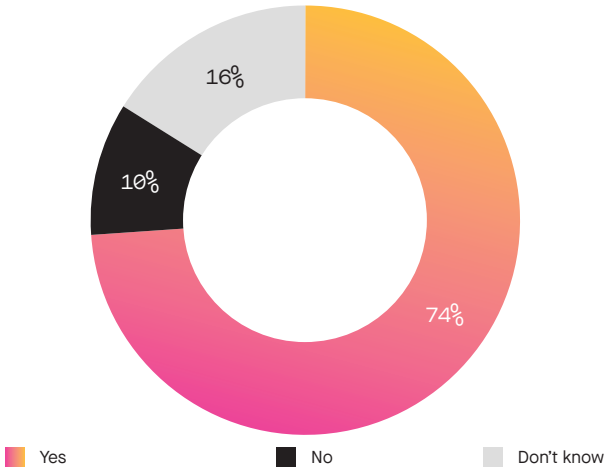
Risk/threat analysis

Not only does HIPAA require a risk/threat analysis to be performed, best practice dictates that one be conducted annually – especially with cyberattacks on the rise. Infrequent risk/threat analyses are one of the most common violations cited by OCR in their analysis of HIPAA audits.

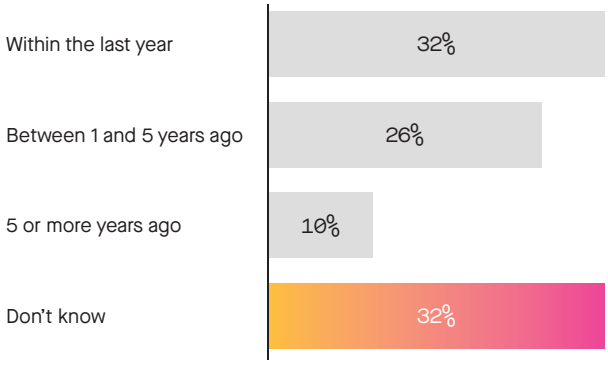
When was the last time your HIPAA privacy and security policies and procedures were reviewed and/or updated?



Do you have policies and procedures in place for breach notifications?



When was the last time you conducted a HIPAA risk/threat analysis?



Why perform risk analysis?

- It's required by the HIPAA security rule
- It's the key to cost-effective compliance
- Lack of a formal written risk analysis may result in a breach deemed as willful neglect
- Breaches considered as willful neglect carry the highest fines

Common risk analysis missteps:

- Missing, incomplete, or outdated risk/threat analysis
- Lack of consideration of all potential threats
- Lack of a consistent methodology to determine the frequency and/or cost/impact of potential threats
- Lack of ownership for HIPAA compliance/not including all parties in analysis
- Not limiting the scope of the risk analysis to protected health information only
- Incomplete, outdated or unavailable documentation of mitigating controls

Workforce training

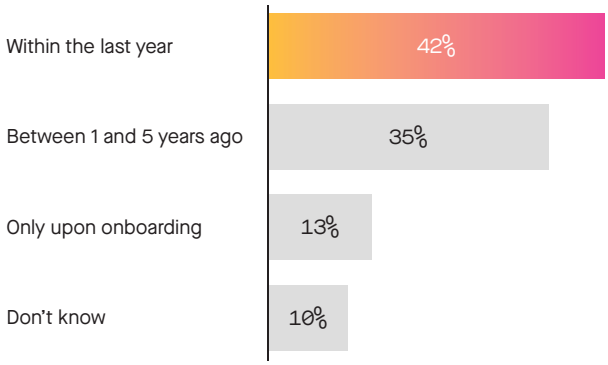
Lack of staff training for members of the workforce that are exposed to protected health information was cited as a primary area of concern by OCR in their audit reviews. The HIPAA Privacy Rule requires training for each staff member within a reasonable period of time after hire, or whenever there is a change in policies and procedures. The HIPAA Security Rule requires training periodically (common practice is annually) and whenever new guidelines or rules are issued by HHS. HIPAA training should be included during onboarding for any new employee with access to PHI. Additionally, attendance at all HIPAA training sessions should be documented.

Workforce training is important not only for preventing breaches, but also to create awareness of what constitutes a breach.

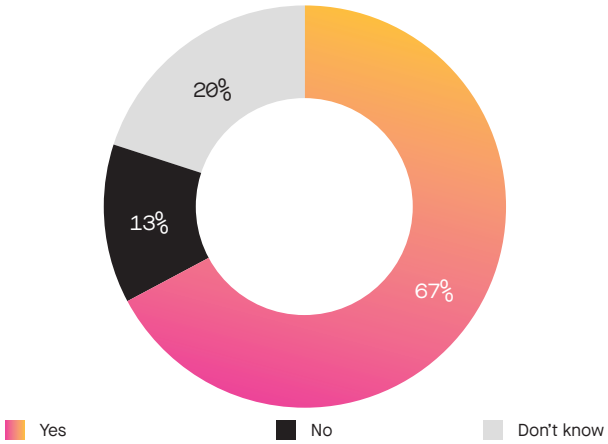
Business associates

A business associate (BA) is defined by HHS as "a person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity." BAs are directly liable for compliance with HIPAA Privacy and Security Rules. However, the entity with a BA agreement in place is required to take reasonable steps to ensure a breach or violation is corrected and may have to report the incident to OCR. OCR confirmed in their audit analysis that BAs had more compliance issues than clearinghouses or plans.

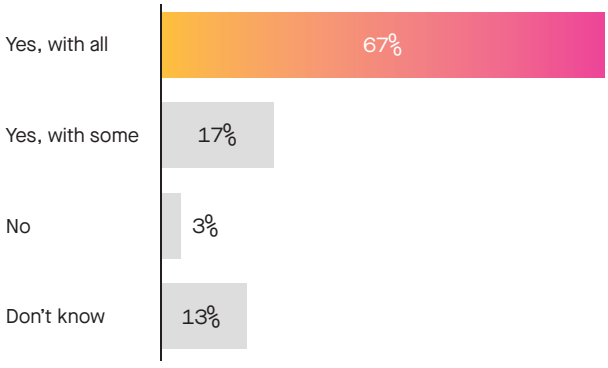
How often do you conduct HIPAA workforce training (for anyone who has access to PHI and/or ePHI)?



Do you have an inventory of all your Business Associates (e.g., insurers, consultants, off-site storage, copier/ shredding vendors, cloud providers)?



Do you have current Business Associate Agreements (as required under HIPAA) with your Business Associates?



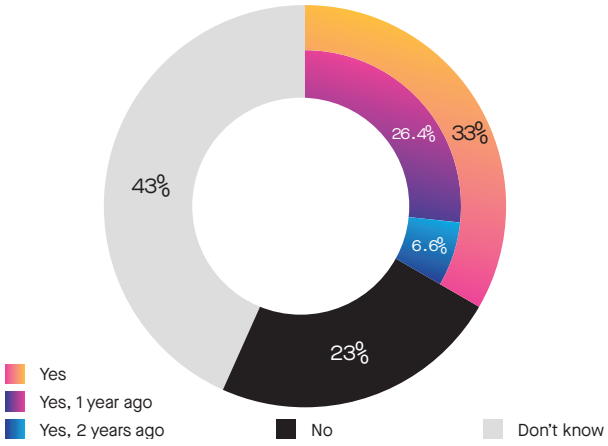
Business Associate Agreements (BAAs) are contracts that outline how different covered entities or business associates will handle PHI and the types of responsibilities that each covered entity or business associate assumes. Simply put, a BAA defines responsibility, and thus liability, with respect to the handling of PHI.

It is important to retain a list of all current BAs and to read and understand the language in your BAAs. The reality is when a breach or any other kind of security incident happens, you are at risk for what was declared in your BAA. In many ways, a BAA is a mechanism for transferring risk (and thus liability) from one entity to another.

Operational review

Clear, well-developed policies and procedures are vital and required under HIPAA. Equally important, and not to be overlooked, is the actual implementation of policies and procedures. Operational reviews evaluate if policies are being followed. Although organizations may have a strong governance program in place that protects information, specifically PHI or ePHI, it may not be implemented in day-to-day practices. On-site operational reviews and examinations of how HIPAA policies and procedures are being applied by staff members who handle PHI and ePHI every day can significantly reduce the likelihood of a breach.

Have you ever conducted an operational review to determine if areas covered in HIPAA training and within the policies and procedures are being followed?



Conclusions

The survey found three key critical gaps in compliance that need to be addressed.

- **Infrequent threat analysis:** 42% of those surveyed either did not know when a risk/threat analysis was last conducted, or indicated that the last one conducted was more than five years ago.
- **Missing or outdated business associate agreements:** 13% of respondents had not inventoried their business associates and only 17% had some — but not all — current business associate agreements in place.
- **Inadequate workforce training:** 35% of our respondents 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

HIPAA has always been a complex and evolving law. Understanding the rules and complying with them in a way that protects your organization is the best way to prevent a breach and the only way to emerge successfully from a HIPAA audit.

Methodology

Implementation. 31 survey participants completed an online questionnaire. A final data cleaning process was conducted after all data was received. Responses were collected from April 29, 2019 through May 17, 2019.

Data cleaning and quality control. All questionnaire responses were carefully reviewed. Statistical software was used to identify outliers and other unusual data points and a final quality control review was conducted.

Rules for descriptive statistics. To protect the confidentiality of individual respondents data, averages, quartiles and medians were presented only where there were at least five (5) data points. Prevalence information displayed in pie charts, bar charts or non-statistical tables required a minimum of three (3) data points to display any data. Due to rounding procedures, totals in this report may not always equal 100%.

Understanding the data. The data presented in this survey represents the actual responses of survey participants. Buck is committed to providing you with the information needed to make the best possible use of the results. You are encouraged to contact us with any questions.

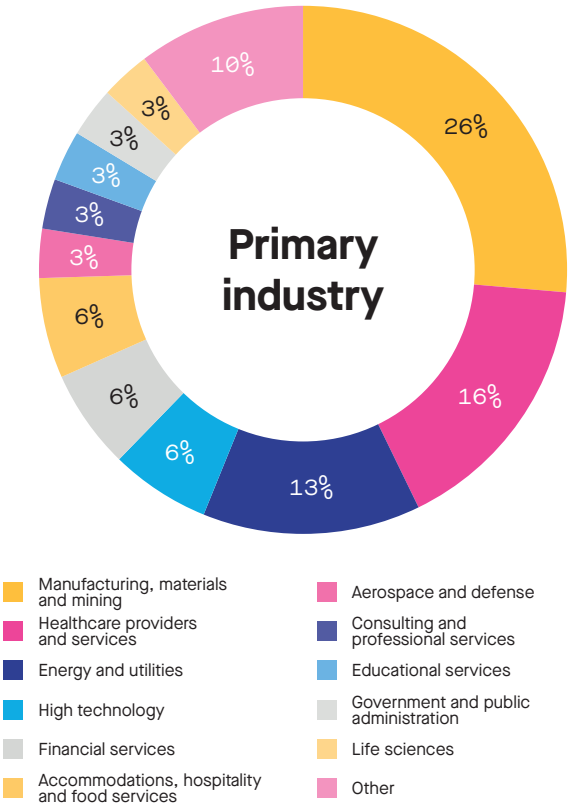
Survey participants

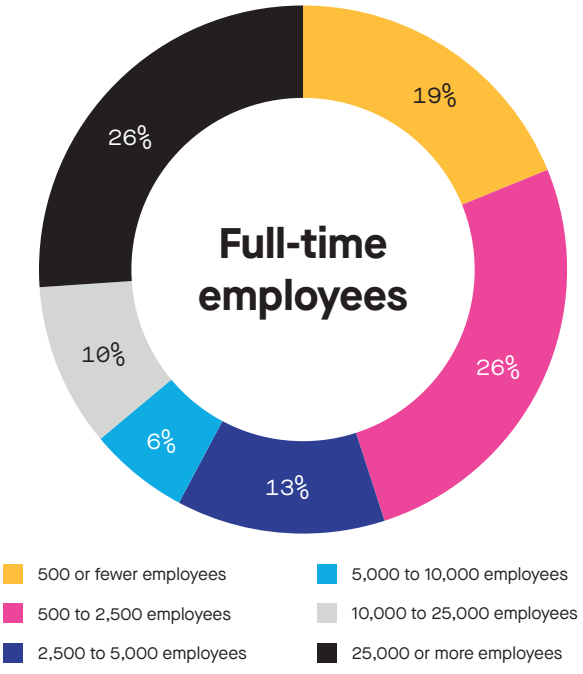
Responses were received from organizations representing a broad range of industries – primarily manufacturing, materials and mining, and life sciences – with 500 or more full-time employees. Organizations responding to the survey represented the following sectors:

- Publicly traded: 52%
- Privately held: 35%
- Not-for-profit: 10%
- Governmental: 3%

Survey participant profile

The majority (77.4%) of survey respondents identified as sponsors of group health plans. The balance of survey participants did not provide a response to this question.





Consulting