SAI360
RISK FROM EVERY ANGLE

3rd Annual

2024 HIPAA Benchmark Report

The current state of HIPAA compliance

Introduction

Strategic Management Services, LLC in collaboration with SAI360 conducted the 3rd Annual HIPAA Compliance Survey in November 2023 (the Survey). The goal of the Survey is to understand how organizations structure, develop, implement, and maintain their HIPAA Privacy Programs and how they respond to increasing challenges in today's regulatory environment.

This Report summarizes the findings from the Survey and covers the following HIPAA privacy-related topics:

- HIPAA program structure, staffing, and oversight;
- Program operations, including policies and training;
- Business associates and agreements;
- HIPAA investigations and audits; and
- HIPAA program priorities, planning, and resources.

There were 178 respondents to the survey located within the United States and representing various provider types. Nearly half of the respondents reported being associated with a hospital or health system, while 27% were associated with a physician/group practice, 19% in behavioral /mental health, 13% in a clinic/ambulatory surgery center, 11% in home health/hospice/dialysis, 10% working in skilled nursing/long term care, and almost 8% associated with a health plan/insurance provider. The remaining respondents were dispersed over various healthcare provider types or vendors (e.g., pharmacy, laboratory, DME, etc.). When comparing the representation of provider types to the previous year's survey responses, almost all of the respondent categories remained similar in number with a couple of exceptions.

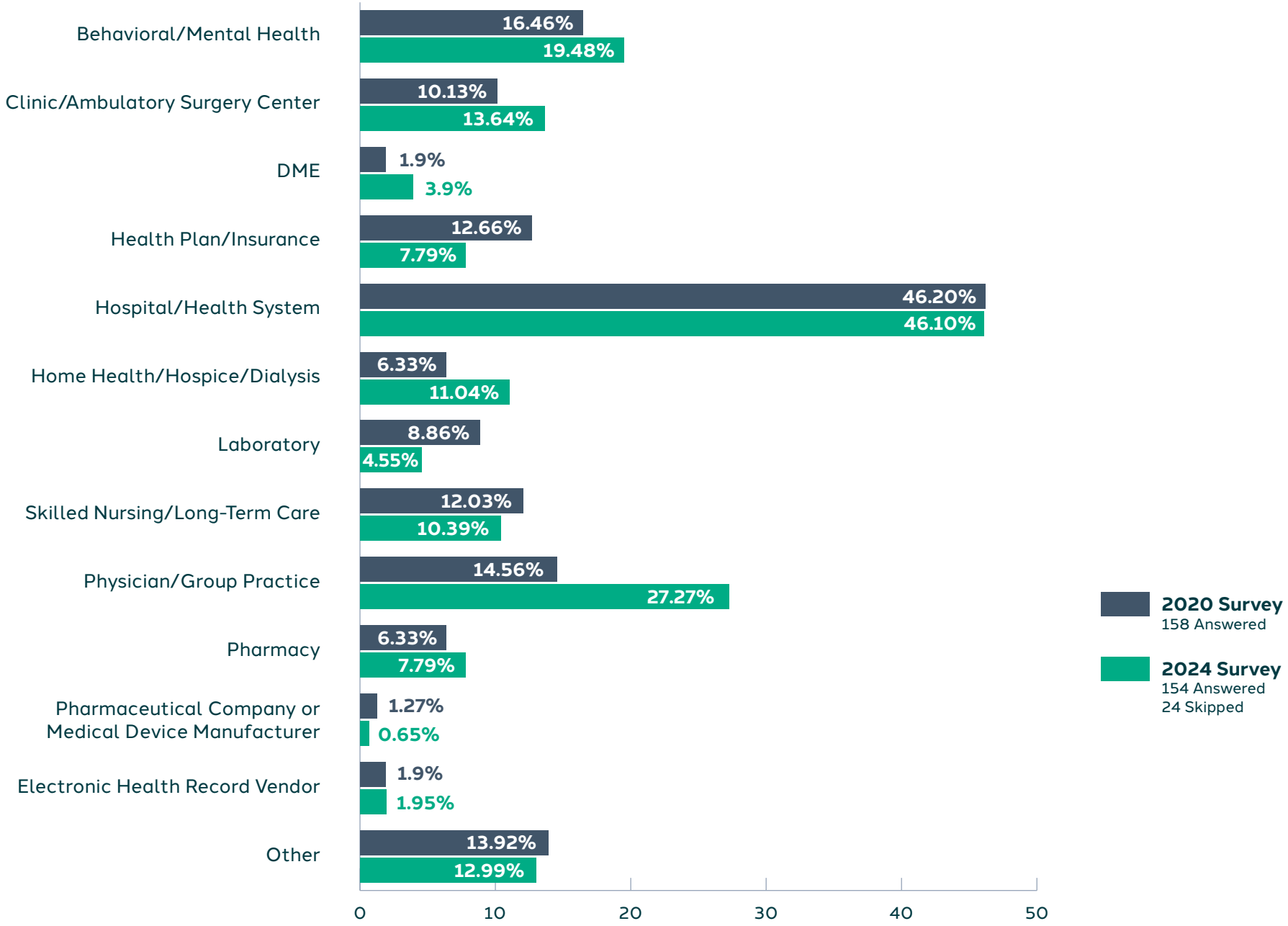
Survey results further indicated that most respondents were covered entities, with 84% healthcare providers/covered entities, almost 6% health plans/ covered entities, and 9% business associates.

It is important to note that the percentage of respondents associated with physician/group practices is much higher than in the previous year's survey. This increase may be reflected in some of the response percentages since physician/group practices tend to be smaller with staff sharing Compliance and HIPAA Privacy Officer duties and with fewer resources to devote to compliance in general. Additionally, there was a lower percentage of respondents associated with health plans and insurance companies than compared to the previous year's survey.

NOTE: Figures within the HIPAA Survey have been rounded and may or may not equal 100% due to weighting, rounding, and inclusion of "other" responses. Or, in the case of multiple-response questions, percentages may add to more than 100%.

We hope our assessment provides valuable insights into the current state of HIPAA Compliance and that it may inform your perspective on the time and money your organization invests in privacy programs. What we do next will shape our cultures for years to come.

What type of healthcare related provider best represents your organization (select all that apply):



HIPAA Compliance Survey Highlights

HIPAA PROGRAM STRUCTURE – RESPONSIBILITY AND OVERSIGHT

Consistent with prior survey results, many organizations receive positive support from their executive leadership and Board of Directors (Board) for the HIPAA Program. Further, most Privacy Officers report to the Board, an Audit/Compliance Committee of the Board, or an Executive-Level Compliance Committee. Also, the majority of respondents have at least one full-time person responsible for HIPAA Privacy. This highlights that most organizations take HIPAA Privacy seriously and keep Executive Management and Board Members informed on HIPAA Privacy issues. However, the majority of respondents noted that HIPAA duties are often secondary to their other job duties indicating a lack of prioritization for privacy compared to other responsibilities.

HIPAA PROGRAM OPERATIONS – POLICIES, TRAINING AND BUSINESS ASSOCIATES

The majority of organizations appear to have best practices in place for HIPAA Program operations, and responses generally aligned with the 2020 survey results. Most respondents have their policies and procedures in a central computerized location. In addition, most participants receive HIPAA compliance training during new employee orientation and annually and maintain adequate information on their HIPAA training.

Responses were split evenly regarding who, between the Privacy Officer, the Compliance Officer, and the Legal Counsel, is responsible for making final decisions on the necessity of a business associate agreement (BAA). Many recipients responded that HIPAA Privacy incidents are primarily found through employees reporting incidents to management or a Privacy/Compliance Officer, which indicates a positive trend that many organizations have a culture of compliance and workforce members feel comfortable reporting issues internally.

HIPAA INVESTIGATIONS, BREACH MANAGEMENT, AND AUDITS

Responses indicate that organizations have a wide variety of items and issues on their audit work plans, and they audit most large risk areas related to the HIPAA Privacy Rule. Around one-third of respondents stated they had never conducted an effectiveness evaluation of their HIPAA Privacy Program or did not know if one was ever completed.

HIPAA PROGRAM PLANNING, PRIORITIES, AND RESOURCES

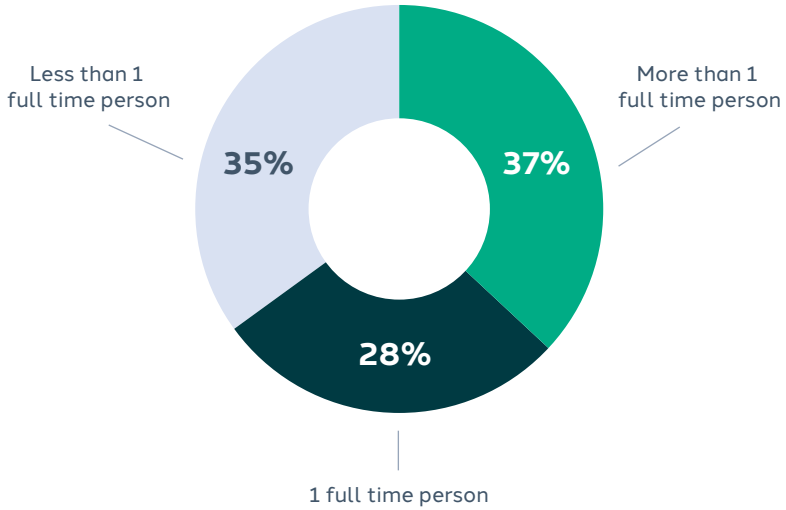
Around one-third of participants responded that updating policies and procedures takes the most planning and resources. Despite the reported increase in HIPAA-related responsibilities due to COVID-19, only a small percentage of respondents reported an increase in resources for the HIPAA Program, whereas a slightly higher rate reported receiving a decrease in resources. The top priorities for the organization's HIPAA Program in the coming year include incident response and reporting, reducing inappropriate/inadvertent disclosures of PHI by the workforce; monitoring business associate agreements and activity; breach notification management, and monitoring improper access to PHI/snooping by the workforce. These priorities are similar but slightly different than the results from last year's survey. Overall, most respondents indicated that they are mostly or somewhat prepared for an OCR audit or investigation.

HIPAA Program Structure, Staffing And Oversight

Q. What is the staffing level for the HIPAA Privacy Office function?

WHAT WE FOUND:

More than **37%** of respondents reported having more than one full time person, and **28%** have one full time person. Both percentages are slightly lower than the 2020 survey results. More respondents, almost **35%**, indicated they have less than one full time position, which is a higher percentage than the 2020 survey results.



WHAT THIS SUGGESTS:

The decreases in the percentage of full-time privacy officer function may be attributed to the higher percentage of respondents associated with physician/group practices, which typically do not have full-time compliance and privacy personnel. The HIPAA Privacy Rule requires a covered entity to "designate a privacy office who is responsible" for HIPAA compliance. The rule does not specifically require the level or the amount of time that this individual is expected to devote to their role as the HIPAA Privacy Officer. That being stated, given the increasing complexity of HIPAA privacy issues and the increased enforcement by the HHS Office for Civil Rights (OCR), the lack of a full-time HIPAA Privacy Officer is a risk, especially for larger organizations. In all organizations, regardless of size, it is advisable to have an individual with the expertise and bandwidth to properly deal with all privacy issues.

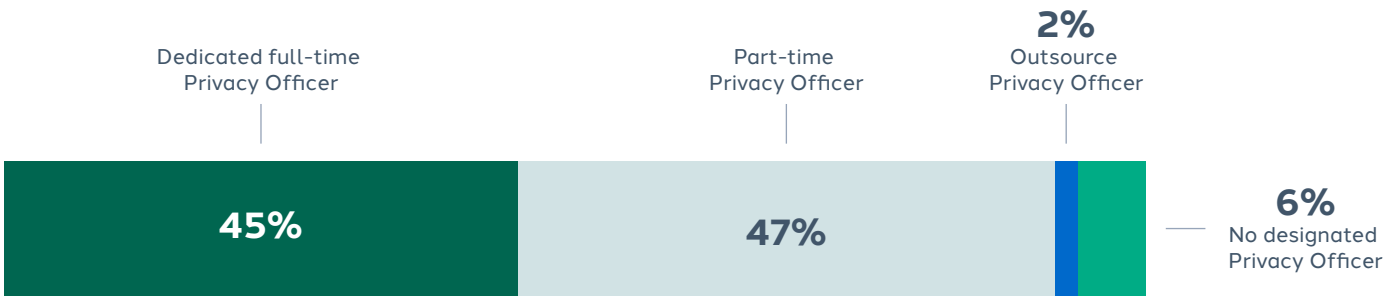
Q. WHICH BEST DESCRIBES YOUR HIPAA PRIVACY OFFICER SITUATION AT YOUR ORGANIZATION?

WHAT WE FOUND:

More than **45%** of respondents reported having a dedicated full-time Privacy Officer, but **47%** reported having a Privacy Officer whose position is part-time or a secondary duty. Almost **2%** outsource the Privacy Officer function and almost **6%** reported they did not have a designated Privacy Officer.

WHAT THIS SUGGESTS:

Again, it can be implied from the responses that the higher percentage of respondents indicating Privacy Officers have part-time or secondary duty positions may be associated with a percentage of physician/group practice participation in this year's survey. Nevertheless, melding the response from the question above and the response to this question indicates that HIPAA privacy is not necessarily front and center to many covered entities. As noted previously, the HIPAA Privacy Rule requires covered entities to designate a privacy officer. The OCR has stated that the privacy rule is "scalable" so that providers can tailor the program based on their size; however, providers are advised to be cautious in how they balance their Privacy Program to ensure they are meeting basic HIPAA Privacy requirements. This is especially important as OCR increases its enforcement and imposition of civil monetary penalties.



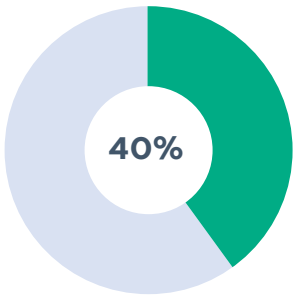
Q. TO WHOM DOES YOUR PRIVACY OFFICER REPORT?

WHAT WE FOUND:

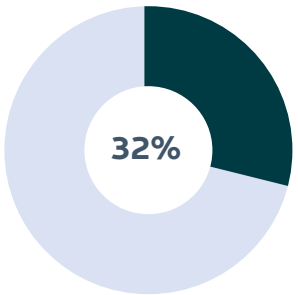
- **40%** of respondents stated that the Privacy Officer reports to the CEO/President, which is 4% higher than the 2019 and 2020 survey results.
- **32%** of respondents reported that the Privacy Officer reports to the Compliance Officer, which is 7% lower than the 2020 survey.
- Over **10%** reported that the Privacy Officer reports to Legal Counsel and over **7%** reported that the Privacy Officer reports to the Chief Operating Officer.
- Less than **3%** of respondents reported that the Privacy Officer reports to the Chief Information Officer or to Health Information Management, respectively.

WHAT THIS SUGGESTS:

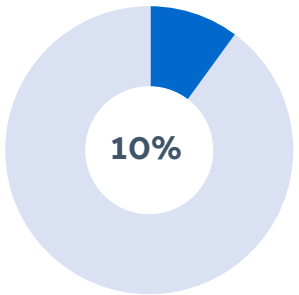
Unlike Compliance Program Guidance issued by the HHS Office of Inspector General, neither OCR nor the regulations specify to whom a privacy officer should report. Nevertheless, given the ramifications of a privacy incident, it is advisable that the Privacy Officer have a direct reporting relationship with the highest level within an organization. Based on these latest results, it appears that covered entities are heading this direction.



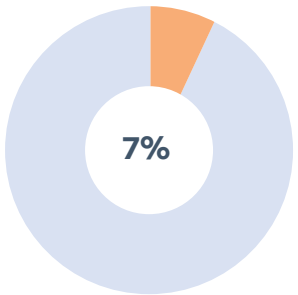
Reports to CEO/President



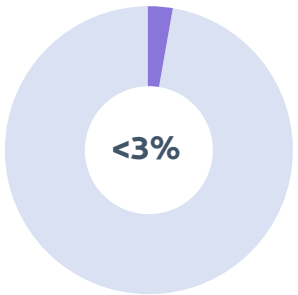
Reports to Compliance Officer



Reports to Legal Counsel



Reports to Chief Operating Officer



Reports to Chief Information Officer/ Health Information Management

Q. TO WHAT OVERSIGHT COMMITTEE DOES THE PRIVACY OFFICER PROVIDE FORMAL REPORTS?

WHAT WE FOUND:

61%

61% of respondents indicated that the Privacy Officer provides formal reports directly to the Board of Directors or Board Compliance Committee, which is a higher percentage than the 2020 survey results.

44%

44% of respondents reported that the Privacy Officer provides formal reports to the Executive-Level Compliance Committee, which is significantly lower than the 2020 survey results.

16%

Almost **16%** noted that the Privacy Officer provides formal reports to the Executive-Level HIPAA Privacy/ Security Committee.

12%

Over **12%** of respondents noted that their organization did not have an oversight body for HIPAA operations.

WHAT THIS SUGGESTS:

The results in this year's survey are almost opposite to the results from the 2020 survey in which most respondents stated that the Privacy Officer reported to the Executive-Level Compliance Committee. This year's survey found most respondents reporting directly to the Board of Directors or the Board Compliance Committee. Since respondents were invited to check more than one choice, it is also possible that respondents have multiple reporting obligations. This would ensure that any privacy issues are addressed at lower levels within the organization, with oversight at the highest level as well. With only a little more than 12% of respondents indicating that their organization did not have an oversight body for HIPAA operations, it would appear that organizations and their leaders are taking much more interest in HIPAA privacy and ensuring their organizations remain in compliance with the regulatory requirements.

Q. WHICH OF THE FOLLOWING STATEMENTS BEST DESCRIBES THE SUPPORT RECEIVED FROM YOUR EXECUTIVE LEADERSHIP AND BOARD?

WHAT WE FOUND:

- The highest percentage of respondents find that their executive leadership and Board are very supportive (almost **48%**) or supportive (almost **42%**).
- A little over **10%** respondents indicated a weak to unsupportive executive leadership and Board.

WHAT THIS SUGGESTS:

The combined percentage of "very supportive" and "supportive" executive leadership and Board is a slight increase over the 2020 survey results. Similarly, the combined percentage of weak or nonsupport is slightly lower. This continues the trend of organizational leadership taking HIPAA Privacy issues seriously, which remains vital to reduce the potential for HIPAA Privacy violations and subsequent fines.

HIPAA Program Operations – Policies And Procedures

Q. HOW MANY HIPAA-RELATED POLICIES AND PROCEDURES DOES YOUR ORGANIZATION HAVE?

WHAT WE FOUND:

37% of the survey group stated they have more than 20 HIPAA policies and procedures

15.5% have 16-20

15% have 1-5

WHAT THIS SUGGESTS:

Based on HIPAA regulatory requirements, a covered entity is advised to have at least 15 single-topic policies to address the full range of HIPAA privacy requirements. Over half of respondents reported having at least 16 or more policies, which indicates a strong basis for HIPAA Privacy compliance. Those who responded to having 10 or fewer or were unsure of how many may indicate that the organization is not fully addressing the Privacy Rule requirements, which can lead to higher penalties in the event of a HIPAA violation and subsequent OCR investigation.

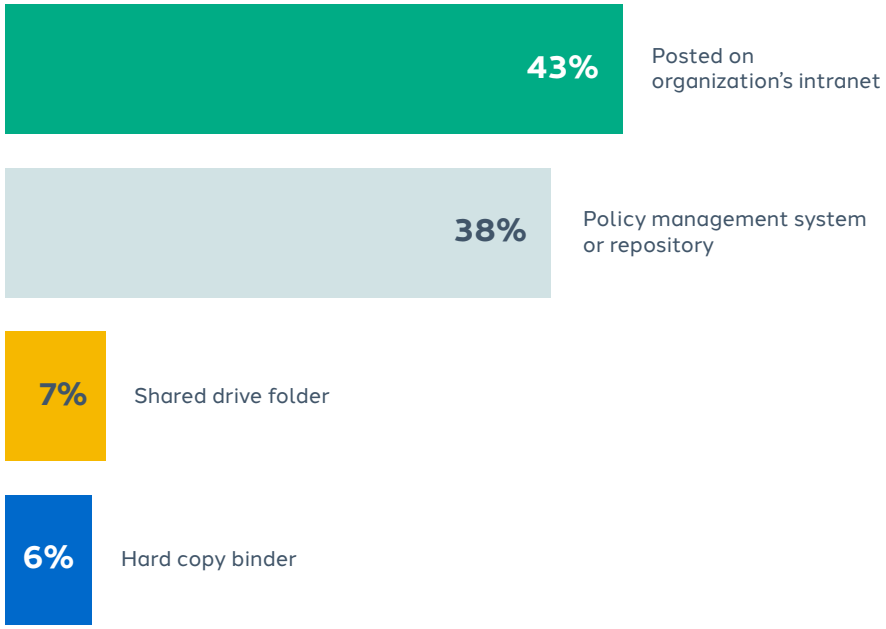
Q. HOW DOES YOUR WORKFORCE ACCESS HIPAA-RELATED POLICIES AND PROCEDURES?

WHAT WE FOUND:

- More than **43%** of the survey group responded that their policies and procedures are posted on the organization's intranet.
- **38%** of the participants access policies using a policy management system or repository.
- There were single-digit response percentages indicating the use of a shared drive folder (almost **7%**) or hard copy binder (**6%**).

WHAT THIS SUGGESTS:

These survey results indicated that a majority of respondents rely on electronic means for employees to access HIPAA-related policies and procedures. This makes it easier for workforce members to access policies from almost any location and at any time. The percentage of respondents who continue to make policies available in paper format is a significant reduction from our previous survey (20%). Limiting reliance on a paper format helps to reduce the risk of employees accessing outdated versions of the policies.

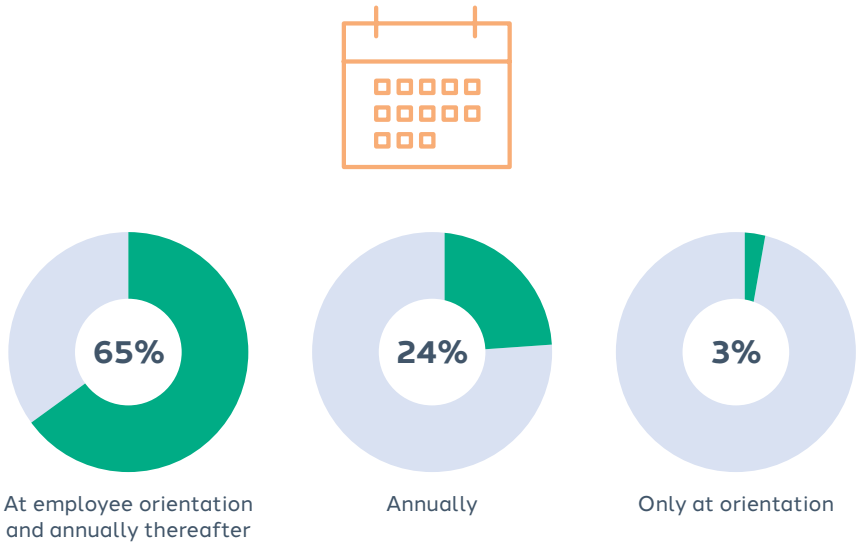


HIPAA Program Operations – Training

Q. HOW OFTEN DO YOU CONDUCT HIPAA COMPLIANCE TRAINING WITH YOUR EMPLOYEES?

WHAT WE FOUND:

- More than **65%** of respondents reported conducting training at new employee orientation and annually thereafter.
- Only **24%** responded that they conduct HIPAA compliance training annually.
- Less than **3%** only conduct HIPAA compliance training at orientation.



WHAT THIS SUGGESTS:

While slightly lower, the responses are not significantly different from the 2020 survey results. The responses continue to evidence that organizations recognize that education is a key tool for communicating the importance of HIPAA and ensuring that employees understand and comply with HIPAA requirements. That being stated, it is a best practice for organizations to provide workforce members with HIPAA training at the time of hire and at least annually. The Privacy Rules do not specifically address the cadence for training, stating only that new members of the workforce must receive training "within a reasonable period of time after the person joins the covered entity's workforce." There is also no specific regulatory requirement for annual training, only workforce members must be trained "as necessary and appropriate for the members of the workforce to carry out their functions within the covered entity." Nevertheless, it is a best practice that new workforce members receive HIPAA Privacy training before they access any PHI and annually thereafter, as well as when there is a change in regulation or covered entity policy. In fact, recent settlements with OCR require organizations to implement new hire and annual HIPAA training for employees as part of the mandated Corrective Action Plans.

Q. WHAT TYPE OF INFORMATION DOES YOUR ORGANIZATION MAINTAIN FOR HIPAA TRAINING?

WHAT WE FOUND:

Respondents were invited to choose more than one response to this question. While all response percentages were lower than the 2020 survey results, there were responses of over **80%** for the following choices: when training took place (**89%**), how training was delivered (LMS, live trainer) (**82%**), and who was trained (**87%**). In addition, **72%** of respondents indicated they maintained results from tests and quizzes.

WHAT THIS SUGGESTS:

As with prior year surveys, it appears that most respondents keep adequate documentation on HIPAA training, which remains important. The most important items to track include who has taken the training and when they completed the training since these evidence to regulators that the organization is conducting training. From a best practice perspective, organizations should consider maintaining records of test and quiz results to evidence understanding of the privacy rule and the organization's policies therein. The individual results can also be used as a factor during annual reviews.

Q. IS HIPAA TRAINING MANDATORY FOR ALL EMPLOYEES AND BUSINESS ASSOCIATES? (I.E., IS DISCIPLINARY ACTION TAKEN IF THE TRAINING IS NOT COMPLETED?)

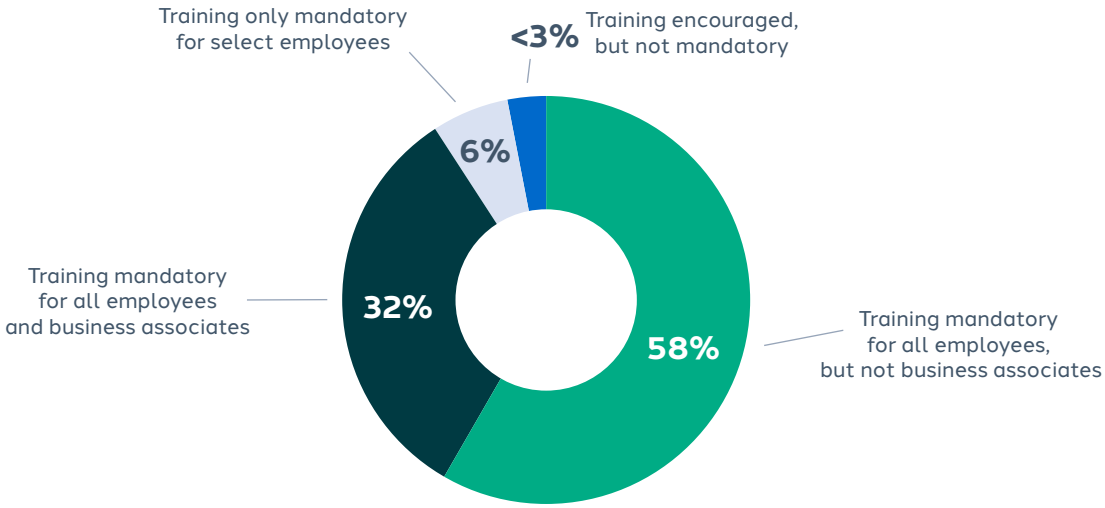
WHAT WE FOUND:

- **58%** of respondents indicated that training is mandatory for all employees, but not business associates.
- **32%** indicated that training is mandatory for all employees and business associates.
- **6%** indicated that training is only mandatory for select employees within the organization.
- Less than **3%** indicated that training is encouraged, but not mandatory.

WHAT THIS SUGGESTS:

Only one-third of respondents reported they require training for employees and business associates. If the entity does not or cannot provide training to their business associates, which can be resource-intensive, it is advisable that the covered entity require its business associate to evidence that training is required and provided by the business associate to its workforce.

Almost 10% of respondents indicated that training is not required of all employees. This is contrary to the HIPAA Privacy Rule and best practices.



Working with Business Associates

Q. DO YOU MAINTAIN AN INVENTORY OF ALL YOUR BUSINESS ASSOCIATES (E.G., INSURERS, CONSULTANTS, OFF-SITE STORAGE, COPIER/SHREDDING VENDORS, CLOUD PROVIDERS)?

WHAT WE FOUND:

An overwhelming majority of respondents (almost **75%**) indicated they maintained such an inventory.

75%

WHAT THIS SUGGESTS:

Maintaining a list of business associates is not a specific HIPAA requirement. However, it is a best practice and can save the covered entity a great deal of time in the event OCR chooses the covered entity for a random audit. When this occurs, OCR will ask the covered entity to identify their business associates with contact information.

Q. DO YOU EXECUTE/MAINTAIN CURRENT BUSINESS ASSOCIATE AGREEMENTS (AS REQUIRED UNDER HIPAA) WITH YOUR BUSINESS ASSOCIATES?

WHAT WE FOUND:

Again, an overwhelming majority of respondents (almost **81%**) answered yes to this question.

81%

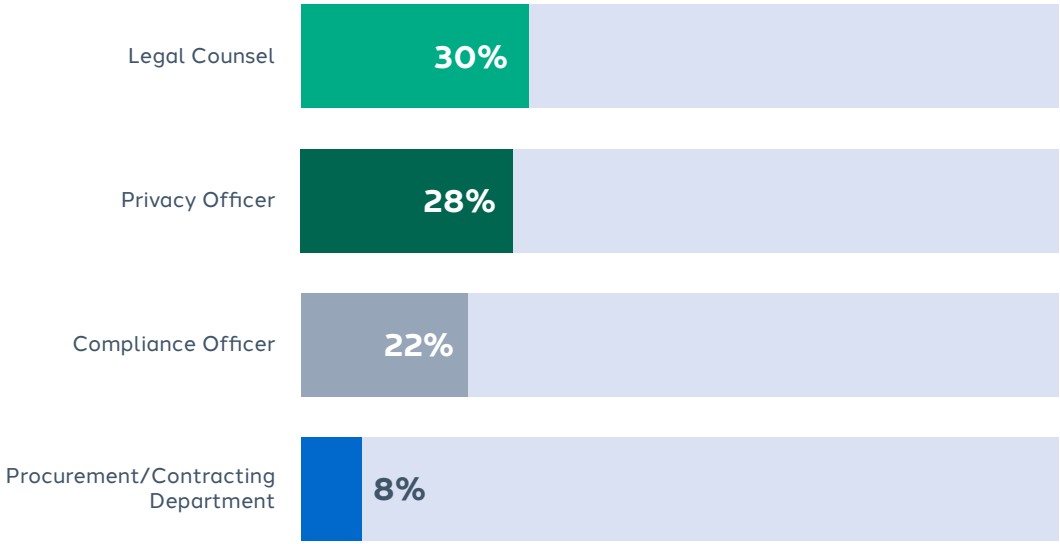
WHAT THIS SUGGESTS:

Having an agreement in place with identified business associates is important to protect against unauthorized disclosures of PHI. It is also a regulatory requirement and can lead to hefty fines. For example, in December 2020, an orthopedic clinic agreed to pay $1.5M to settle multiple HIPAA compliance failures, including failure to secure business associate agreements with multiple business associates. Covered entities are advised to have a checklist in place to identify which vendors meet the definition of a business associate and execute an agreement containing at a minimum, the requisite elements as listed in the regulation.

Q. WHO IS RESPONSIBLE FOR MAKING THE FINAL DETERMINATION OF WHETHER A BUSINESS ASSOCIATE AGREEMENT (BAA) IS NEEDED WITH A THIRD-PARTY VENDOR?

WHAT WE FOUND:

The responses were closely divided between Legal counsel (**30%**), Privacy Officer (**28%**), and Compliance Officer (**22%**). As with the 2019 and 2020 survey results, a little more than **8%** of respondents indicated that the procurement/contracting department was responsible for making the final determination.



WHAT THIS SUGGESTS:

While the HIPAA regulations are silent on this issue, as noted above, there are risks if vendors are not identified as business associates and agreements are not executed accordingly. Using a checklist to identify which vendors perform the duties of business associates will be helpful but it is a best practice that if the Privacy Officer is not a decision maker, they serve as consultants to the decision maker to ensure that a potential Business Associates is accurately identified. In many cases, this will be a straightforward determination, but in other cases, such as when a covered entity is acting as a Business Associate for another covered entity, the privacy officer's expertise and knowledge will be invaluable. If, as noted by the survey response, an organization's procurement/contracting department is responsible for making the determination, it is advisable that at least one person in that department has a thorough understanding of the HIPAA requirements and use the aforementioned checklist to support this understanding.

Investigations/Breaches/ Disciplinary Actions

Q. HOW ARE MOST HIPAA PRIVACY INCIDENTS DETECTED?

WHAT WE FOUND:

The top three responses included:

1. Employee reports directly to management/HIPAA/Compliance Office — **44%**
2. Monitoring of user access — **17%**
3. Patient reports/complaints — **9%**

WHAT THIS SUGGESTS:

While the percentage of respondents indicating that their organization learns of a HIPAA privacy incident through an employee report is slightly lower than in the 2020 survey, the response rate of almost 50% remains a positive. It infers that organizations continue to promote open communication, a key element of an overall effective Compliance Program, and that employees are feeling less ambivalent toward reporting HIPAA concerns with less fear of retaliation or reprisal. Nevertheless, relying solely on employee reports is not ideal since reporting may be delayed, thus delaying discoveries of potential breaches and mitigation steps therein. This year's survey results also revealed an almost 50% decrease in reports/complaints from patients, which may indicate that organizations are placing better controls to avoid errors in patient disclosures.

Program Assessments/Priorities

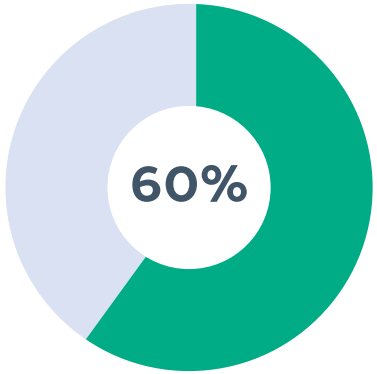
Q. WHICH OF THE FOLLOWING ITEMS ARE CURRENTLY ON YOUR HIPAA/COMPLIANCE AUDIT WORK PLAN?

WHAT WE FOUND:

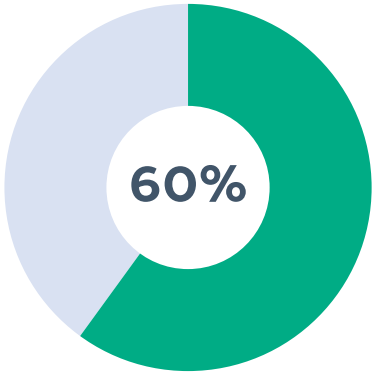
Respondents were asked to check all choices that applied to them. In this instance, user access review (of the EHR or other relevant applications), and physical location reviews/walkthroughs were the top choices each garnering **60%** or more responses. Review of Business Associate activity garnered **40%** of responses.

WHAT THIS SUGGESTS:

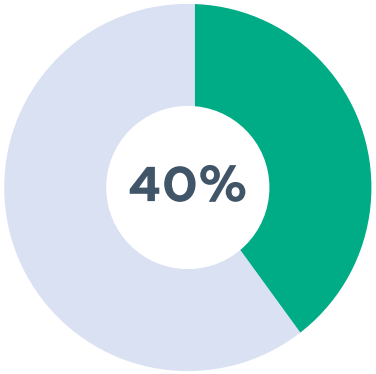
The responses continue to indicate that organizations have a wide variety of items and issues in their audit work plans. While best practices promote the use of audit work plans, smaller organizations may not have the resources to complete a formal audit. Nevertheless, organizations should consider a more streamlined approach to auditing, such as using reports from government enforcement and professional/trade press to inform their audits.



Access review



Physical location reviews/walkthroughs

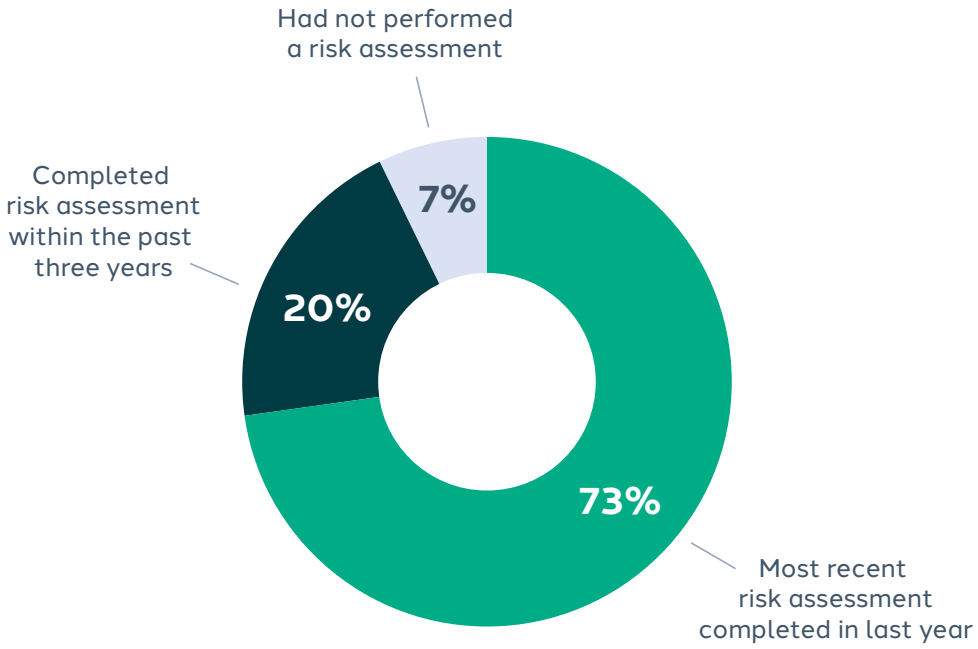


Review of business associate activity

Q. HIPAA REQUIRES PERFORMING A SECURITY RISK ANALYSIS TO IDENTIFY VULNERABILITIES THAT COULD RESULT IN A BREACH OF PHI.

WHAT WE FOUND:

In response to this question/statement, **73%** of respondents noted that their most recent risk assessment was completed in the last year. **20%** indicated that they completed an assessment within the past three years. Almost **7%** indicated they had not performed a risk assessment.

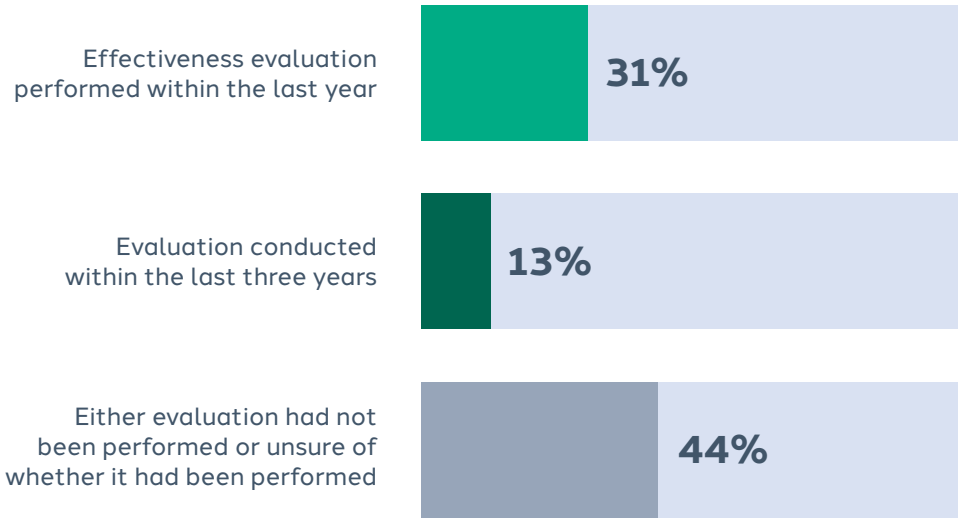


WHAT THIS SUGGESTS:

HIPAA requires covered entities or business associates to "[c]onduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronically protected health information held by the covered entity or business associate the rule does not specify the frequency of the assessment." The rule does not specify the frequency of conducting the assessment. OCR guidance states that the "risk analysis process should be ongoing" and OCR has noted that covered entities may perform the assessment annually, bi-annually or every three years, "depending on the circumstances of their environment." It is also important to note that in the event of a HIPAA incident, OCR investigators will most likely request data on the entity's most recent risk assessment.

Q. WHEN WAS THE LAST TIME THE EFFECTIVENESS OF YOUR HIPAA PRIVACY PROGRAM WAS INDEPENDENTLY EVALUATED?

WHAT WE FOUND:



WHAT THIS SUGGESTS:

The data for this year's survey is not much different from prior years' surveys. Conducting an effectiveness evaluation within the past year follows a best practice for measuring compliance with the HIPAA Privacy Rule. While the HIPAA Privacy Rule does not require covered entities to conduct independent reviews, it is an important tool. Outside independent evaluation of the program may be particularly helpful for organizations with small privacy and compliance workforces that do not have the time or personnel to be responding to day-to-day activities. Outside independent reviews can also be helpful tools if an organization is going through a transition that may impact HIPAA privacy, such as adopting a new EHR, expanding into different states, or merging with another covered entity.

Q. PLEASE SELECT THE TOP THREE PRIORITIES TO BE ADDRESSED BY YOUR HIPAA COMPLIANCE PROGRAM IN THE NEXT 12 MONTHS

WHAT WE FOUND:

The top four priorities included:

1. Incident response and reporting — 54%
2. Monitoring inappropriate access to PHI/snooping by workforce — 52%
3. Reducing inappropriate/ inadvertent disclosures of PHI by workforce — 50%
4. Monitoring Business Associate Agreements and activity — 44%

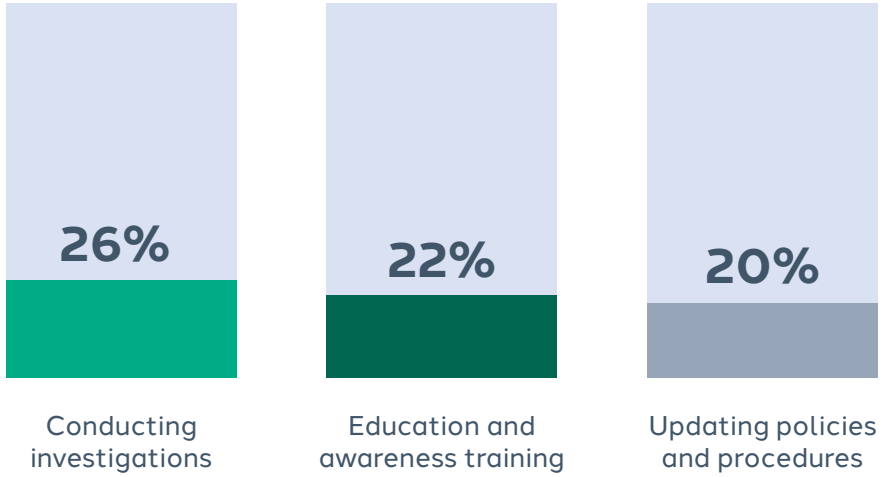
WHAT THIS SUGGESTS:

The priorities and associated percentages are similar to the 2019 and 2020 surveys. The top three priorities can pose risks to the organization's reputation among providers, patients, and the community at large, as well as financial risks in the form of lost revenue and potential fines since delayed remediation of privacy incidents can lead to larger fines. Almost half of respondents noted that reducing inappropriate/inadvertent disclosure of PHI by the workforce indicates a need for increased training and education about HIPAA Privacy Rules, increased monitoring of EHR access, and a need for greater controls over access to the EHR.

Q. WHICH OF THE FOLLOWING HIPAA RESPONSIBILITIES TAKES THE MOST PLANNING AND RESOURCES FOR YOUR ORGANIZATION?

WHAT WE FOUND:

- A total of **26%** of respondents indicated that conducting investigations took the most planning and resources.
- Almost **22%** of participants stated that education and awareness training took the most planning and resources.
- A total of **20%** stated that updating policies and procedures took the most planning and resources.



WHAT THIS SUGGESTS:

The responses to this year's survey are markedly different from the 2020 survey when the highest percentage of respondents noted that updating policies and procedures took the most planning and resources. This may be an indication that organizations are finding standardized processes and timelines for updating policies and procedures, thereby reducing the amount of time spent planning for this activity. There was a 10% increase in respondents indicating that conducting investigations took the most planning and resources, which may be in response to an increase in government investigations and fines for HIPAA violations. There was also a 5% increase in respondents who stated that education and awareness took the most planning. This correlates to the response to an earlier question wherein more than 65% of respondents reported conducting training at new employee orientation and annually thereafter.

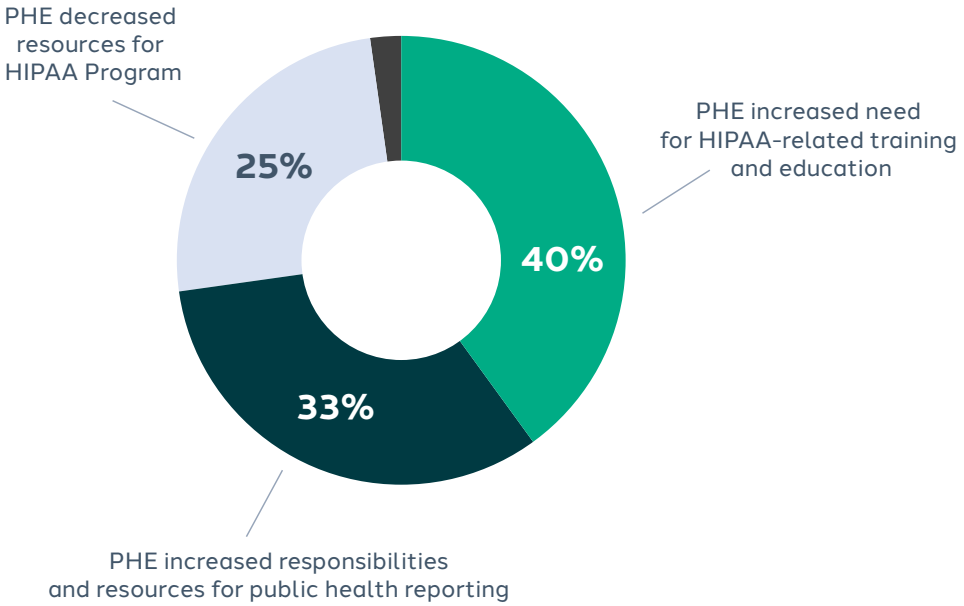
Q. WHAT TYPE OF IMPACT DID THE COVID-19 PUBLIC HEALTH EMERGENCY HAVE ON YOUR HIPAA PROGRAM?

WHAT WE FOUND:

- A total of **40%** of respondents indicated that the public health emergency (PHE) increased the need for HIPAA-related training and education.
- Almost **33%** noted that the PHE increased the responsibilities and resources needed for public health reporting.
- Almost **25%** noted that the PHE decreased resources for the HIPAA Program.

WHAT THIS SUGGESTS:

The increased need for HIPAA-related training and education is an indication that healthcare entities understood the need to continue safeguarding privacy during COVID-19. However, given the costs of treatment, and reduced workforce during this period of time, some covered entities may have needed to shift resources from HIPAA Privacy to other areas, such as patient care or public health reporting. With OCR's enforcement discretion of certain HIPAA-related violations having expired in May 2023, organizations are advised to return to pre-COVID-19 HIPAA privacy program priorities to avoid fines moving forward.



Q. WHAT TYPE OF SOFTWARE OR HARDWARE TOOLS DO YOU USE TO CARRY OUT THE PRIVACY PROGRAM OPERATIONS AT YOUR ORGANIZATION?

WHAT WE FOUND:

Almost **72%** of respondents reported using an incident reporting tool (i.e., HIPAA Hotline).

Almost **68%** use a learning/training management system.

A total of **50%** reported that they use an incident tracking software.

A total of **49%** reported using a policy management software.

A total of **41%** reported using automated monitoring of their users' access to PHI.

A total of **31%** reported implementing an automated review of audit logs and reports from the EHR system.

A total of **26%** reported using an investigation management software.

WHAT THIS SUGGESTS:

As with the prior survey, only a small number of organizations reported that they did not use any type of software for their Privacy Program operations. Software programs can help track investigations, train staff (e.g., an online learning management system), and keep track of policies to ensure currency of the policy, as well as facilitate access to the policies. It should be recognized that not all organizations have the resources for elaborate expensive tools. That being stated, even the use of spreadsheets to track audits, policies, breaches, and training will provide the critical documentation to evidence an effective HIPAA compliance program.

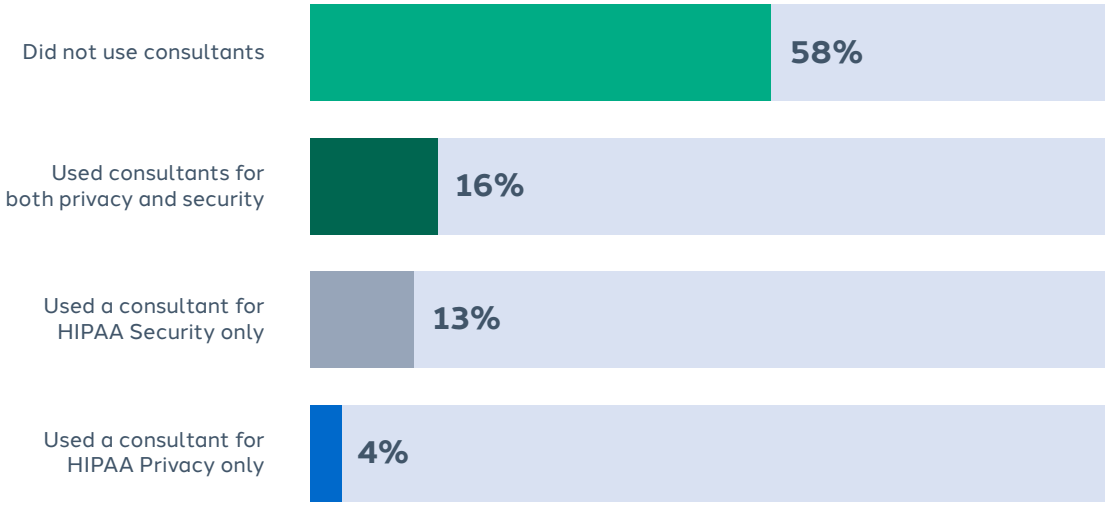
Q. DOES YOUR ORGANIZATION USE ON-CALL CONSULTANT/VENDOR SERVICES TO ASSIST WITH HIPAA PRIVACY AND SECURITY FUNCTIONS (E.G. TRAINING, INVESTIGATION BREACHES, ASSISTING WITH EVALUATIONS, POLICIES AND PROCEDURES, RISK ANALYSIS, ETC.)?

WHAT WE FOUND:

- More than **58%** of the survey group stated that they did not use consultants.
- Almost **16%** reported they used consultants for both privacy and security.
- Almost **13%** used a consultant for HIPAA Security only.
- Only **4%** used a consultant for HIPAA Privacy only.

WHAT THIS SUGGESTS:

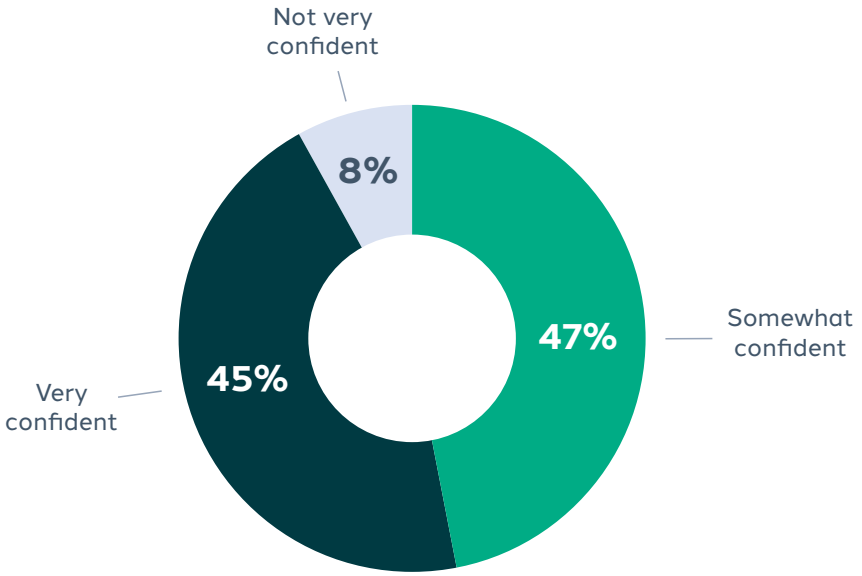
The responses to this year's survey are consistent with the 2020 survey results with percentages varying by just a few points, plus or minus. The HIPAA Privacy and Security Rules do not require covered entities or business associates to use external vendors; however, these professionals can be helpful for tasks like breach investigations and conducting a HIPAA risk analysis. An on-call consultant can also help respond to independent audits or conduct research to resolve a complicated regulatory question.



Q. HOW CONFIDENT ARE YOU THAT YOUR ORGANIZATION IS MEETING THE HIPAA PRIVACY, SECURITY, AND BREACH NOTIFICATION RULE REQUIREMENTS?

WHAT WE FOUND

- A total of **47%** of respondents stated they were somewhat confident that organization is meeting the requirements of the HIPAA Privacy, Security and Breach Notification Rules.
- Almost **45%** of respondents stated they were very confident.
- Only **8%** of respondents stated that they were not very confident.



WHAT THIS SUGGESTS

While the percentage of respondents who are only “somewhat confident” was higher than those who were “very confident,” compared to the 2019 and 2020 surveys, both responses show an increase in those who are “very confident” over those who are “somewhat confident.” Specifically, there was a 6% increase in respondents who were “very confident” and a 4% decrease in respondents who were only “somewhat confident.” The percentage of respondents stating they were not very confident also decreased by 2%. Organizations that are only “somewhat confident” or “not very confident” are advised to consider having a gap analysis conducted to identify those areas that are causing a lack of confidence.

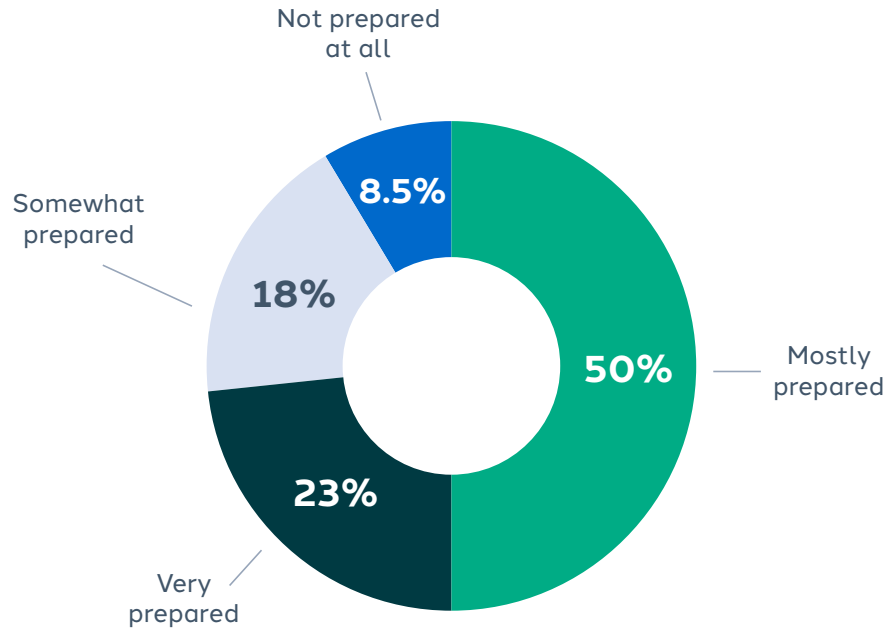
Q. HOW PREPARED IS YOUR ORGANIZATION FOR A HIPAA COMPLIANCE AUDIT OR INVESTIGATION FROM OCR?

WHAT WE FOUND:

- A total of **50%** of respondents stated that they were mostly prepared for a HIPAA audit or investigation.
- A total of **23%** of respondents stated they were very prepared.
- Almost **18%** of respondents felt they were somewhat prepared.
- Only **8.5%** of respondents stated they were not prepared at all.

WHAT THIS SUGGESTS:

The combined percentage of respondents who indicated they were "mostly" or "somewhat prepared" is a slight increase from the 2020 survey; however, the percentage of those stating that they were "very prepared" was 5% lower and the percentage stating they were "not prepared at all" was slightly higher. All organizations are advised to assess their preparedness with audits or investigations and document accordingly. Only through documentation of key HIPAA indicators such as training, policies and procedures, risk assessments, can an organization evidence to OCR that they have an effective HIPAA Privacy Program.



Q. WHEN WAS THE LAST TIME YOUR ORGANIZATION HAD A HIPAA BREACH THAT HAS BEEN REPORTED TO THE OFFICE FOR CIVIL RIGHTS?

WHAT WE FOUND:

47%

About **47%** of respondents stated that they reported a HIPAA breach to OCR within the past 12 months.

12%

Almost **12%** of respondents noted reporting a breach one to two years ago.

13%

A total of **13%** noted having a breach reported to OCR three to five years ago.

16%

A total of **16%** of respondents stated that they never experienced an OCR reportable HIPAA breach.

WHAT THIS SUGGESTS:

About 80% of respondents indicated that they experienced an OCR reportable HIPAA breach within the past five years; with nearly half of respondents stating they reported a HIPAA breach within the last 12 months. It is nearly impossible to prevent all breaches. Training the workforce and early detection of potential incidents with an immediate investigation followed by remediation as needed are key to managing breach identification and reduction. It is advised that organizations implement industry-accepted best practices to decrease the possibility of a data breach involving electronic PHI. Examples of industry best practices include encrypting data at rest, enabling multi-factor authentication, on-going education and training, implementing recommended software updates, and disabling access for terminated employees. We recommend reviewing OCR's non-technical guidance as a starting point.

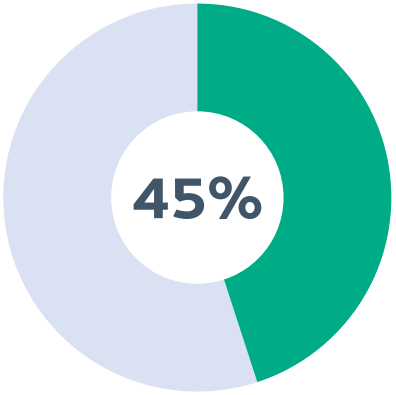
Q. WHAT TYPE OF ENCOUNTERS HAS YOUR ORGANIZATION HAD WITH OCR IN THE LAST 2 YEARS?

WHAT WE FOUND:

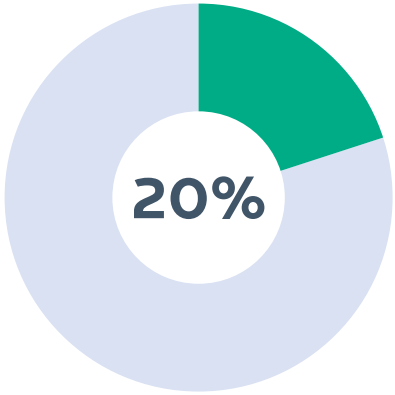
- Over **45%** of respondents indicated that they have not had any encounter with OCR over the past two years.
- Almost **20%** of respondents had an investigation/inquiry regarding a breach report for an incident involving less than 500 individuals.
- Almost **18%** of respondents had an investigation/inquiry regarding a breach report for an incident involving more than 500 individuals.

WHAT THIS SUGGESTS:

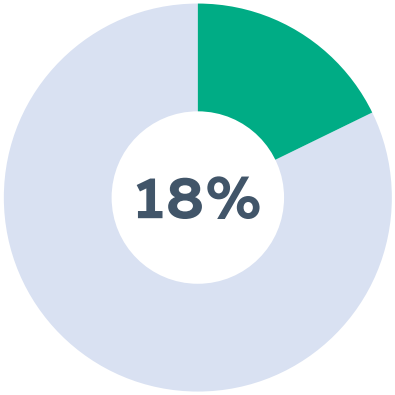
Almost half of the respondents reported having no encounter with OCR in the past two years. While the reasons for this may vary, it can be inferred that these organizations have strong HIPAA privacy and security practices in place, such as workforce training, data encryption, access controls, that protects the organization against breaches that result in an OCR encounter. Responses to this question correlate with the responses to a previous question that addressed how privacy incidents are detected. Almost 44% of respondents to that question indicated that employees report issues directly to leadership. Provided leadership forwards the issue to the Privacy Officer as quickly as possible, this type of direct reporting enables the Privacy Officer to investigate a potential issue to either avert or detect a breach sooner.



Had no encounter with OCR over past two years



Had an investigation/inquiry regarding a breach report for an incident involving less than 500 individuals



Had an investigation/inquiry regarding a breach report for an incident involving more than 500 individuals

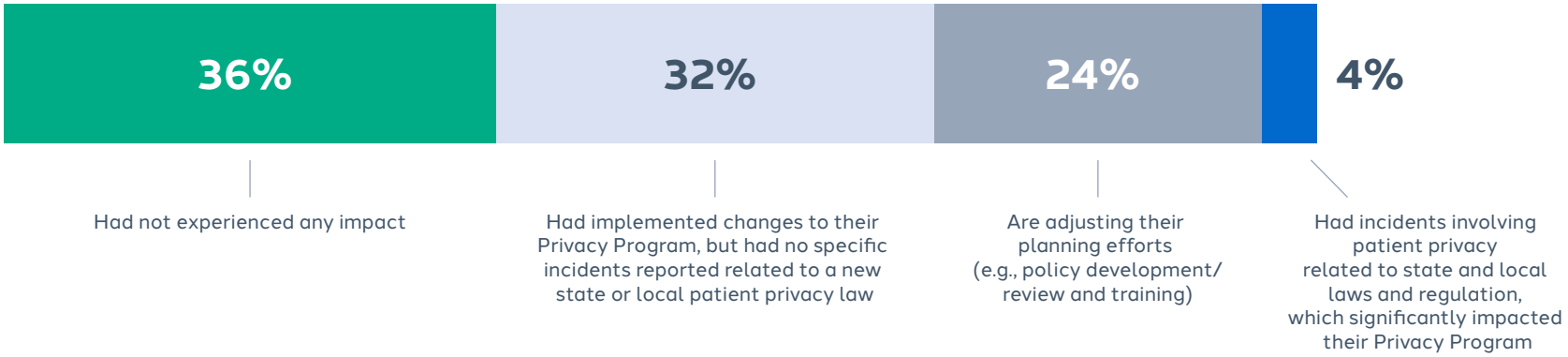
Q. WHAT TYPE OF IMPACT HAS THE IMPLEMENTATION OF PATIENT PRIVACY-RELATED STATE AND LOCAL LAWS HAD ON YOUR PRIVACY PROGRAM?

WHAT WE FOUND:

- About **36%** of respondents indicated they had not experienced any impact.
- Almost **32%** indicated they had implemented changes to their Privacy Program, but had no specific incidents reported related to a new state or local patient privacy law.
- A total of **24%** of respondents are adjusting their planning efforts (e.g., policy development/review and training).
- Less than **4%** had incidents involving patient privacy related to state and local laws and regulation, which significantly impacted their Privacy Program.

WHAT THIS SUGGESTS:

Results from this question suggest that most organizations continue to not feel the impact of state actions and mandates related to patient privacy matters. Nevertheless, more than 50% are adjusting their planning efforts or implementing changes to their Privacy Program, ostensibly to prepare for new state or local patient privacy laws. Even though states are enacting privacy laws, many are exempting those organizations that are subject to HIPAA privacy and security requirements. Still, covered entities should be mindful of state breach reporting requirements which may be more stringent and may require reporting to a state's top legal department, such as the attorney general, rather than a designated office within the state's department of health.



Conclusion

This HIPAA Survey Results Report provides a detailed breakdown of the responses to the 2023 HIPAA Compliance Survey and an analysis of the results, as well as a comparison to the 2020 HIPAA Compliance Survey results. Notably, there was a marked increase in the percentage of respondents representing physician provider offices, which may indicate an increasing recognition of the important of safeguarding patient privacy and value of a HIPAA Privacy Program. However, there was a marked decrease in the number of respondents representing health plans and insurance companies. As with the prior HIPAA Compliance Surveys, results indicate that many organizations have HIPAA Privacy Programs that are supported by organizational leadership, with most Privacy Officers reporting to the CEO or Compliance Officer, and providing formal reports to the Board of Directors and the Executive-Level Compliance Committee. Engagement by an organization's leadership is an essential component of creating a strong culture of compliance. As privacy regulatory requirements continue to evolve, Privacy Programs must continue to keep its staff, executive leadership, and board-level management informed of the changing regulatory landscape and any emerging HIPAA-related risk areas, as well as HIPAA privacy incidents.

Most organizations appear to have implemented operations to address HIPAA requirements, such as policies and procedures maintained in a central computerized location and providing HIPAA compliance training to new and existing employees. These operational elements are highly recommended and an industry best practice. Additionally, most organizations appear to maintain adequate documentation of their HIPAA training efforts, which is beneficial since OCR may ask for this documentation during an investigation.

The survey results also revealed that organizations are auditing a wide variety of items and issues with user access at the top of their list. This is important given the number of incidents in which employees have been terminated for "snooping" into medical records of patients for whom they had no need to know. Around one-third of respondents stated that an effectiveness evaluation of their HIPAA Privacy Program had never been conducted and another third of respondents did not know whether an effectiveness evaluation was ever completed. Although the HIPAA Privacy Rule does not require covered entities to conduct independent reviews, an evaluation is an important tool for detecting compliance failures with HIPAA Privacy Rule requirements. An independent review of the Privacy Program is also an important tool for executive management and the Board to stay abreast of the organization's Privacy Program and privacy-related matters.

Overall, most respondents indicated that they are mostly prepared or somewhat prepared for an OCR audit or investigation. Additionally, it was reported that most organizations do not use on-call consultants or vendor services. Even for organizations that can perform many HIPAA privacy functions in-house, having an on-call consultant, especially in the evolving regulatory environment, can help conduct independent audits, research more complicated HIPAA-related questions, or focus on changing state laws as needed.

More than three-quarters of respondents stated that the COVID-19 public health emergency had increased HIPAA-related training and education, research inquiries, policies, breach activity, responsibilities, and public health reporting. This is markedly different from our last survey, which was conducted in 2020, the beginning of the public health emergency. While the public health emergency may be waning, it is highly recommended that organizations continue to recognize the importance of safeguarding patient privacy and having a fully operational HIPAA Privacy Program. This includes incorporating HIPAA requirements into topics such as the increased use of telemedicine given that oversight flexibilities in this area have expired with the official end of the public health emergency.

STRATEGIC MANAGEMENT SERVICES

Privacy is challenging because, in addition to the federal HIPAA legislation and regulatory mandates, many states have implemented state privacy and consumer laws that health care organizations are required to comply with. It takes Privacy experts with a comprehensive understanding and practical operational experience with federal and state law to assess the organization's risks, train and education the workforce, and develop practical and effective policies, procedures and processes that address HIPAA Privacy.

Successfully addressing and complying with HIPAA Privacy and state privacy laws can be overwhelming. Strategic Management has worked with hundreds of health care organizations, and their Compliance and Privacy Officers, to assist them, specifically, in meeting the challenges of complying with the HIPAA Privacy Rule and state health care privacy laws.

Strategic Management empowers its clients to meet their regulatory compliance requirements by providing specialized products and services developed by proven industry experts. Founded in 1992 by Richard Kusserow, the former Inspector General of the U.S. Department of Health & Human Services, Strategic Management was the first healthcare consulting firm to focus on corporate compliance and ethics initiatives. Today, we are the undisputed industry leader, having helped more than 3,000 health care organizations with highly-specialized, actionable regulatory compliance services.

Connect with us at Compliance.com to learn how we can help you.

Interested in learning more about how SAI360 can help your organization?

Request a demo.

Our unified approach to risk sets us apart

Today's complex risk landscape demands more. SAI360 leads the way with an integrated GRC platform and Learning solution that spans the entire risk spectrum.

Risk Management Solutions

- Enterprise & Operational Risk Management
- Regulatory Change Management
- Policy Management
- Third-Party Risk Management
- Internal Control
- Internal Audit
- Incident Management
- Conflicts of Interest (COI) Disclosure Management
- IT & Cybersecurity
- Business Continuity Management

Ethics & Compliance Learning Solutions

- Anti-Bribery & Anti-Corruption
- Competition & Anti-Trust
- Conflicts of Interest
- Data Protection & Privacy
- Information Security
- Exports, Imports & Trade Compliance
- Harassment & Discrimination

SAI360
RISK FROM EVERY ANGLE

SAI360 is giving companies a new perspective on risk management. By integrating Governance, Risk, Compliance (GRC) software and Ethics & Compliance Learning resources, SAI360 can broaden your risk horizon and increase your ability to identify, manage, and mitigate risk. See risk from every angle. Visit www.sai360.com.

143550 0124