SAI360
RISK FROM EVERY ANGLE

4th Annual

2025 HIPAA Benchmark Report

The current state of HIPAA compliance

SAI360
RISK FROM EVERY ANGLE

Introduction

The 4th National HIPAA Compliance Survey was conducted by SAI360 in collaboration with Strategic Management Services, LLC. The goal of the survey is to continue understanding how organizations structure, develop, implement, and maintain their HIPAA Privacy Programs and respond to increasing challenges in today's regulatory environment.

This report summarizes the findings from the 2024 National HIPAA Compliance Survey (HIPAA Survey) and covers topics such as:

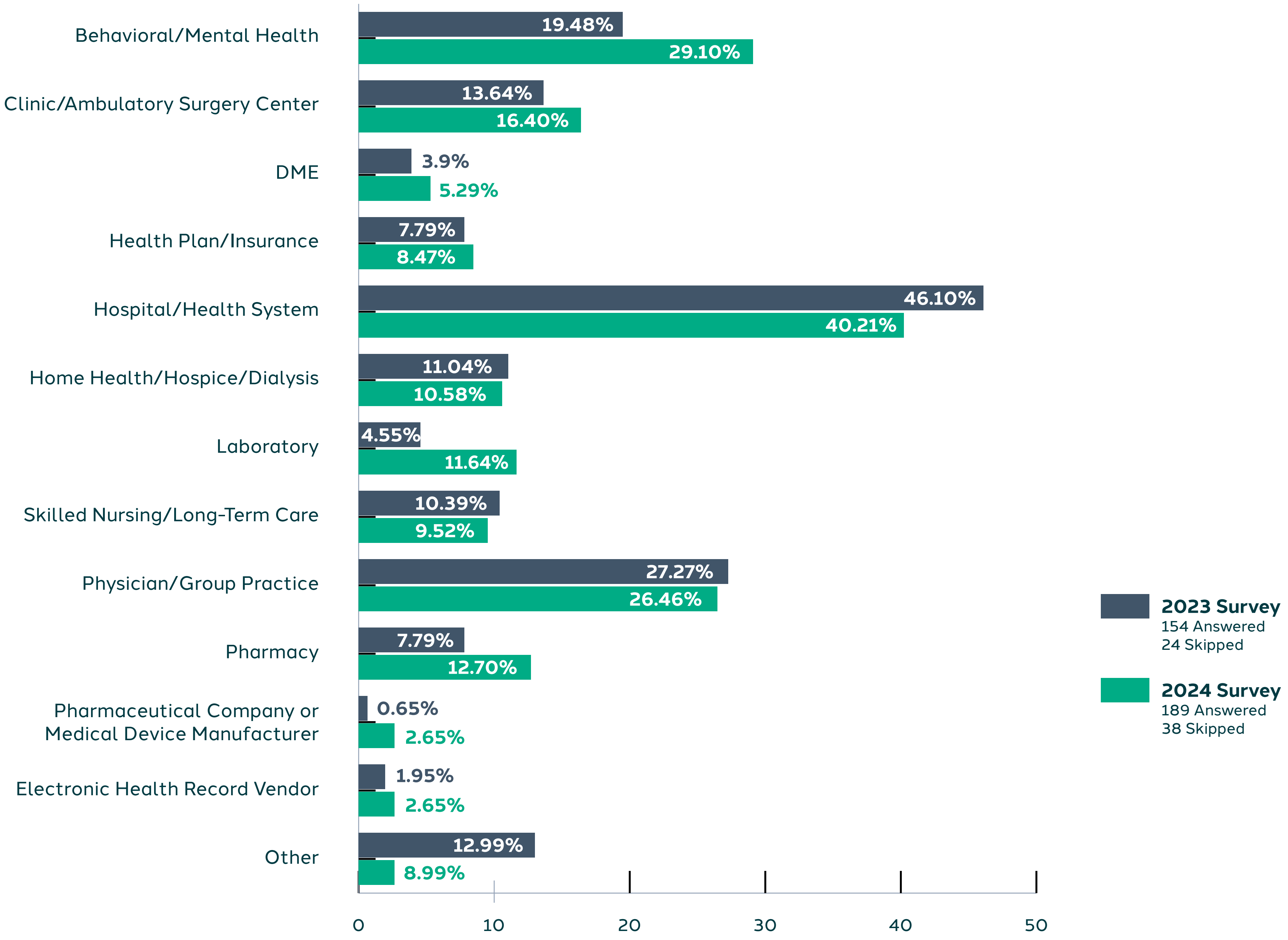
- HIPAA program structure - responsibility, and oversight
- Program operations – policies, training, and business associates
- HIPAA investigations, breach management, and audits
- HIPAA program planning, priorities, and resources
- Enforcement

The HIPAA survey was conducted among 227 respondents, which is a 22% increase over last year's survey response. Respondents are located within the United States and represent various provider types and business associates. As with prior year surveys, the majority of respondents reported being associated with a hospital or health system; however, the percentage of these respondents was lower than last year. This year's survey yielded a higher percentage of respondents associated with behavioral/mental health (29%), with physician/group practices a close third (26%), followed by clinic/ambulatory surgery center (16%), pharmacy (13%), laboratory (12%); and home health/hospice/dialysis (11%) rounding out the double-digit responses. The remaining respondents were dispersed over various healthcare provider types (e.g., skilled nursing-long term care, health plan/insurance, DME, etc.) or vendors.

The nearly 10% increase in respondents from behavioral/mental health entities is notable. In mid-February of 2024, the Department of Health and Human Services (HHS) finalized its regulatory requirements for the Confidentiality of Substance Use Disorder Patient Records (42 CFR Part 2). The final rule noted that the Coronavirus Aid, Relief and Economic Security (CARES) Act required HHS "to increase regulatory alignment between" Part 2 and the HIPAA Privacy, Breach Notification and Enforcement Regulations. While Part 2 does not explicitly require entities to have a privacy official, the percentage increase in behavioral/mental health participant may be a result of the new final rule.

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. In the case of multiple-response questions, percentages may add to more than 100%. It is also noted that not all respondents answered every question. Percentages are based on the number of respondents for the specific question.

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 continue to take HIPAA Privacy seriously and keep Executive Management and Board Members informed on HIPAA Privacy issues.

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 last year's survey results. Most respondents store their policies and procedures in a central computerized location either through an intranet or policy management system. 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 regarding who, between the Privacy Officer, the Compliance Officer, Legal Counsel, or a partnership thereof, is responsible for making final decisions on the necessity of a business associate agreement (BAA). Similar to the last survey, many recipients responded that HIPAA Privacy incidents are primarily found through employees reporting incidents to management or a Privacy/Compliance Officer, which indicates a continued positive trend that many organizations have a culture of compliance and workforce members feel comfortable reporting issues internally.

HIPAA INVESTIGATIONS, BREACH MANAGEMENT, AND AUDITS

Organizations continue to rely on employees reporting directly to management when there is a suspected privacy incident. A higher percentage of respondents monitor workforce/user access than the previous survey. Responses also indicated that organizations have a wide variety of items and issues on their audit work plans, with many noting that user access reviews remain a priority.

Almost half of respondents stated that they had some type of encounter with the Department of Health and Human Services Office for Civil Rights (OCR) within the last two years. Over 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, which is again a higher combined percentage from the last survey.

HIPAA Compliance Survey Highlights

HIPAA PROGRAM PLANNING, PRIORITIES, AND RESOURCES

Around one-third of participants responded that updating policies and procedures and conducting investigations take the most planning and resources. The top priorities for the organization's HIPAA Program in the coming year include incident response and reporting; reducing inappropriate/inadvertent disclosures of protected health information (PHI) by the workforce; monitoring improper access to PHI/snooping by the workforce; monitoring business associate agreements and activity; and breach notification management. These priorities are similar to the results from last year's survey. Overall, most respondents indicated that they are mostly or somewhat prepared for an OCR audit or investigation.

ENFORCEMENT

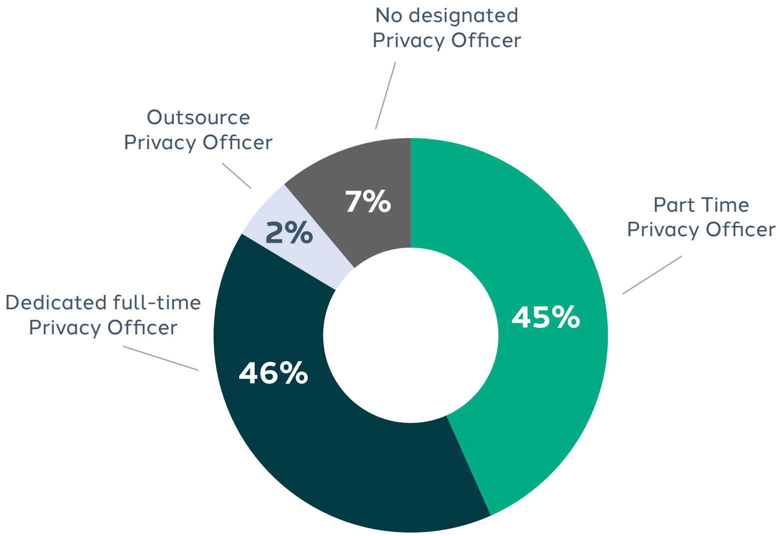
Almost half of respondents indicated that they had a breach reportable to the OCR within the last year. Nevertheless, almost half of respondents indicated they had no encounter with OCR over the past two years. More than half of respondents indicated they were very or mostly prepared for a HIPAA Compliance Audit or investigation.

HIPAA Program Structure, Responsibilities And Oversight

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

WHAT WE FOUND:

Similar to last year's survey, more than **46%** of respondents reported having a dedicated full-time Privacy Officer, followed closely by almost **45%** who reported having a Privacy Officer whose position is part-time or a secondary duty. Almost **2%** outsource the Privacy Office role and almost **7%** reported they did not have a designated Privacy Officer, which is a slight increase over last year.



WHAT THIS SUGGESTS:

The increase in respondents who indicated they do not have a privacy official is notable. As noted previously, the HIPAA Privacy Rule requires covered entities to designate a Privacy Official. 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 program to ensure they are meeting basic HIPAA privacy requirements. This remains important as OCR continues its enforcement and imposition of civil monetary penalties.

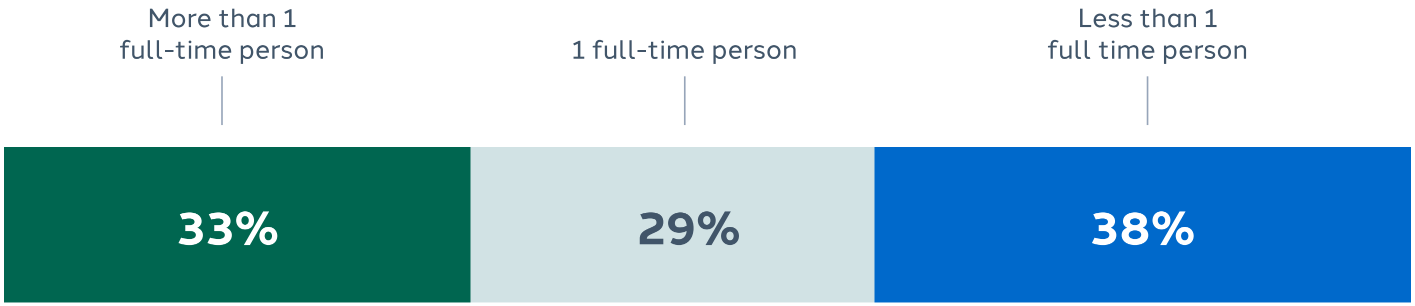
Q. WHAT IS THE STAFFING LEVEL FOR THE HIPAA PRIVACY OFFICE FUNCTION?

WHAT WE FOUND:

Only **33%** of respondents reported having more than one full-time person, which is about a 4% decrease from last year's survey. Almost **29%** of respondents reported having one full-time person, which is a very slight increase from last year. More respondents, almost **38%**, indicated they have less than one full-time position, which is again a higher percentage than our previous survey.

WHAT THIS SUGGESTS:

The HIPAA Privacy Rule requires a covered entity to "designate a privacy official 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 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 address privacy issues.



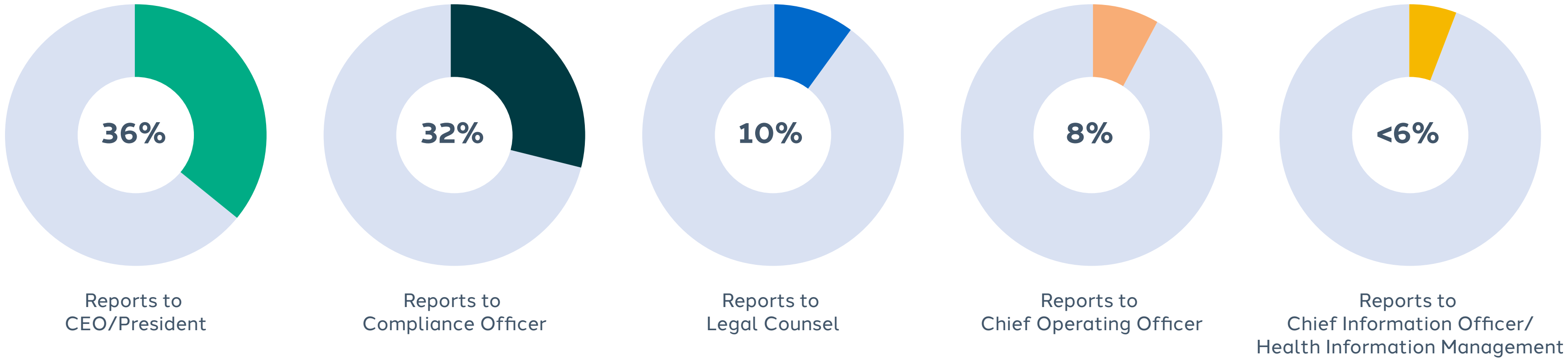
Q. TO WHOM DOES YOUR PRIVACY OFFICER REPORT?

WHAT WE FOUND:

- **36%** of respondents stated they report to the CEO/President, which is 4% lower than our previous surveys.
- Almost **32%** of respondents report to the Compliance Officer, which is 2% lower than our previous survey.
- Over **10%** report to Legal Counsel and over **8%** report to the Chief Operating Officer.
- Less than **6%** of respondents stated they report to the Chief Information Officer, Health Information Management, or to Human Resources, respectively.

WHAT THIS SUGGESTS:

Unlike compliance program guidance issued by the HHS Office of Inspector General, neither the 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 has a direct reporting relationship with the highest level within an organization. Therefore, the 4% reduction in those privacy officers reporting to the CEO/President is a significant change from last year's survey results. While they may report to a lower-level executive routinely, it is a best practice that Privacy Officers have a direct line to the highest officer in the organization, especially if a privacy event occurs.



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

WHAT WE FOUND:

62%

Over **62%** 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 our previous survey.

54%

54% of respondents reported that the Privacy Officer provides formal reports to the Executive-level Compliance Committee, which is significantly higher than our previous survey.

21%

Almost **21%** noted that the Privacy Officer provides formal reports to the Executive-level HIPAA Privacy/ Security Committee. This is also higher than the previous survey.

8%

Over **8%** of respondents noted that their organization did not have an oversight body for HIPAA operations, which is a lower percentage than our previous survey.

WHAT THIS SUGGESTS:

The results in this year's survey are consistent with the results from our previous survey, in which most respondents stated that the Privacy Officer provided reports to the Board of Directors or Board Compliance Committee. There was also a significant increase in respondents stating the Privacy Officer has reporting obligations to an executive-level 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 8% of respondents indicating that their organization did not have an oversight body for HIPAA operations, it would appear that organizations and their leaders are continuing to take an interest in HIPAA privacy and ensuring their organizations remain in compliance with the regulatory requirements.

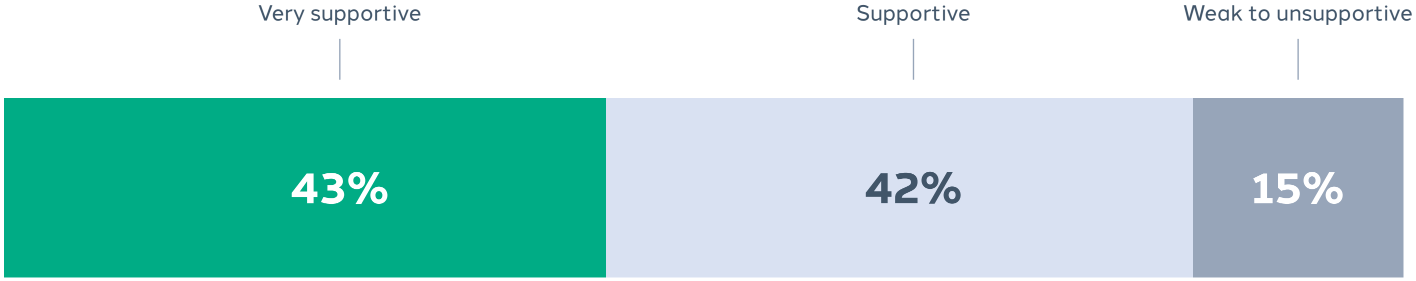
Q. WHICH OF THE FOLLOWING STATEMENTS BEST DESCRIBES THE SUPPORT RECEIVED FROM YOUR EXECUTIVE LEADERSHIP AND BOARD OF DIRECTORS?

WHAT WE FOUND:

- Respondents equally found their executive leadership and Board to be very supportive (almost **43%**) or supportive (almost **43%**) of the Privacy Program.
- A little over **15%** 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 decrease since our previous survey. Similarly, the combined percentage of weak or nonsupport is slightly higher. This is inconsistent with the other trends indicating that organizational leadership are taking HIPAA Privacy issues very seriously, which remains vital to reduce the potential for HIPAA Privacy violations and subsequent fines.



HIPAA Program Operations – Policies Training And Business Associates

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

WHAT WE FOUND:

28%

Almost **28%** have more than 20 HIPAA policies and procedures.

13%

13% have 16-20.

14%

Almost **14%** have 11-15.

17%

Over **17%** have 6-10.

15%

Over **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. The number of respondents who reported having at least 16 or more policies implies that they have a strong foundation for HIPAA Privacy compliance. Those who responded to having ten or fewer or were unsure of what they had may indicate that they are not fully addressing privacy rule requirements, which can lead to higher penalties in the event of a HIPAA violation and subsequent OCR investigation.

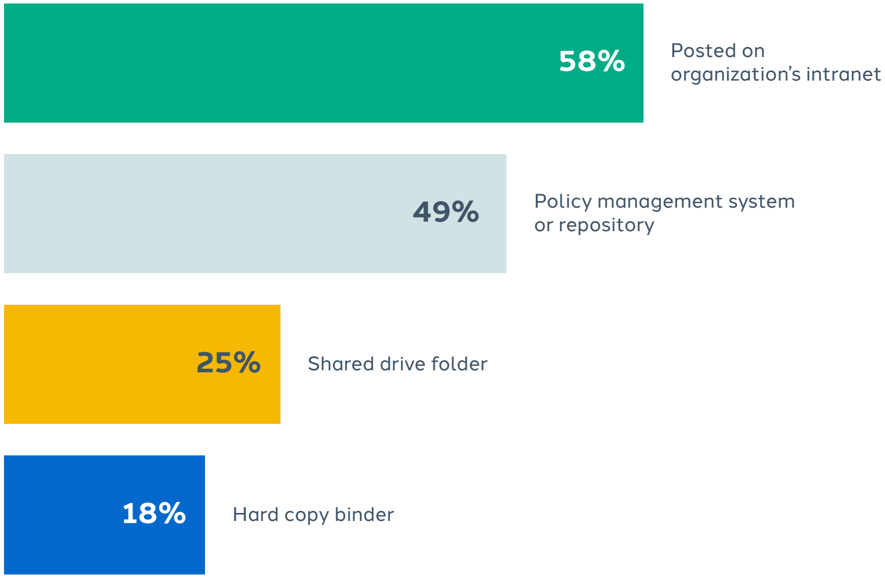
Q. HOW DOES YOUR WORKFORCE ACCESS HIPAA-RELATED POLICIES AND PROCEDURES?

WHAT WE FOUND:

- More than **58%** responded that their policies and procedures are posted on the organization's intranet.
- **49%** use a policy management system or repository.
- Almost **25%** use a shared drive folder.
- Over **18%** indicated that they use paper policies (i.e. a hard copy binder).

WHAT THIS SUGGESTS:

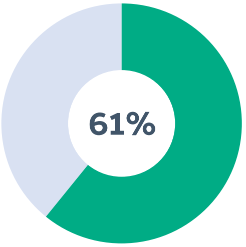
These survey results indicate that a majority of respondents rely on electronic means for employees to access HIPAA-related policies and procedures. This makes it easier for workforce members to access policies from almost any location and at any time. That being stated, there should also be a mechanism to avoid multiple electronic versions and duplication of policies. The percentage of respondents who continue to make policies available in paper format is a significant increase from our previous survey (6%). Reliance on a paper format may be a risk since employees may not have access to the most recent version of a policy and may instead be relying on outdated versions.



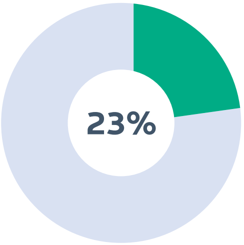
Q. HOW OFTEN DO YOU CONDUCT HIPAA COMPLIANCE TRAINING WITH YOUR EMPLOYEES?

WHAT WE FOUND:

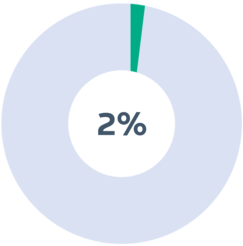
- More than **61%** of respondents reported conducting training at new employee orientation and annually thereafter.
- Only **23%** responded that they conduct training annually.
- Less than **2%** only conduct training at orientation.



At employee orientation and annually thereafter



Annually



Only at orientation

WHAT THIS SUGGESTS:

The responses are not significantly different from our last survey; however, there is a slight downward trend, which should be noted. The responses continue to evidence that organizations recognize that education is a key tool for communicating the importance of HIPAA and ensuring employee compliance 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 Rule does 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 that 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 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. Settlements with OCR continue to require organizations to implement new-hire and annual HIPAA training for employees as part of the mandated Corrective Action Plans.

Q. WHAT IS THE FORMAT OF THE TRAINING?

WHAT WE FOUND:

71%

More than **71%** of respondents reported using a learning module.

25%

Over **25%** responded that the training was provided live/in person.

33%

33% use a combination of live and virtual training.

2%

Less than **2%** of respondents reported they were not conducting any training.

WHAT THIS SUGGESTS:

This is a new question for this year's survey. Importantly, the percentage of those respondents who reported they did not conduct any training is low. While the use of a learning module may be a more efficient mechanism to ensure all employees participate in training in some fashion, it may not yield the intended learning results. In particular, learning modules do not always lend themselves to customization to ensure the specific entity's privacy policies, procedures, and challenges are addressed. Moreover, learning modules do not provide opportunities to ask questions. A combination of live and virtual training, of which 33% of respondents noted, may be a solution to ensure employee engagement. That being stated, live training is time consuming for the privacy officer, and therefore may not be feasible, especially if the position is part time. A solution to this challenge may be to train others, such as the HR Director, to lead live training sessions.

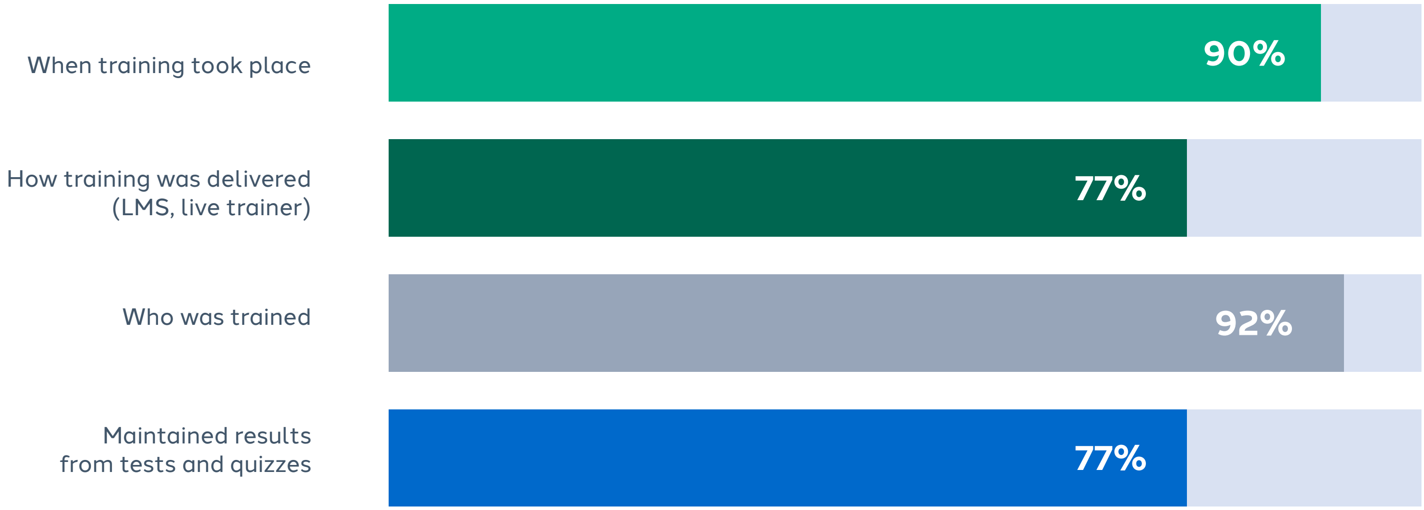
Q. WHAT TYPE OF INFORMATION DOES YOUR ORGANIZATION MAINTAIN FOR HIPAA TRAINING?

WHAT WE FOUND:

Respondents were invited to choose more than one response to this question. While response percentages varied from last year, there were responses of over **75%** for the following choices: when training took place **(90%)**, how training was delivered (LMS, live trainer) **(77%)**, and who was trained **(92%)**. In addition, **77%** of respondents indicated that they maintained results from tests and quizzes.

WHAT THIS SUGGESTS:

As with prior 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 items 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?)

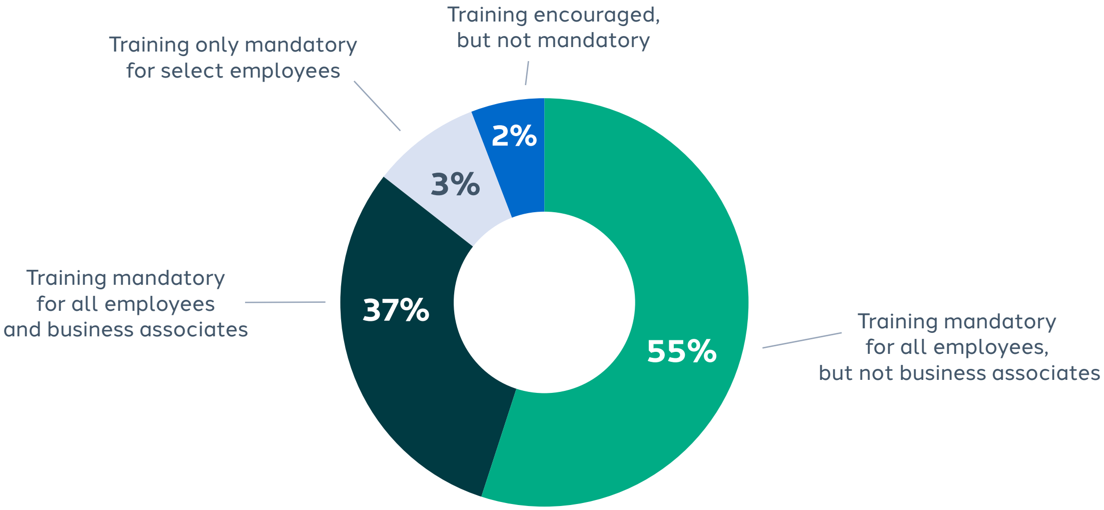
WHAT WE FOUND:

- 55% of respondents indicated that training is mandatory for all employees, but not business associates.
- 37% indicated that training is mandatory for all employees and business associates.
- Almost 3% indicated that training is only mandatory for select employees within the organization.
- 2% indicated that training is encouraged, but not mandatory.

WHAT THIS SUGGESTS:

This year's survey shows a 5% increase in requiring training for all employees and business associates, which may account for the decreased percentages in the other categories.

Almost 5% of respondents continue to indicate that training is not required of all employees. While this is lower than last year's responses, not requiring training is contrary to the HIPAA Privacy Rule and best practices.



Q. ARE THERE CONSEQUENCES IF AN EMPLOYEE OR BUSINESS ASSOCIATE DOES NOT COMPLETE TRAINING?

WHAT WE FOUND:

77%

77% of respondents indicated that employees may be disciplined for noncompletion of training.

22%

22% indicated that a business associate may be terminated for failure to evidence HIPAA training completion.

16%

16% indicated that employees do not face disciplinary action for failing to complete HIPAA training.

10%

Less than **10%** indicated that business associates are not terminated for failing to evidence completion of HIPAA training.

WHAT THIS SUGGESTS:

This is another new question for this year's survey. It was added as a reflection of regulatory expectations that all members of a covered entity's workforce receive training on applicable policies and procedures related to PHI. Business associates are considered part of the covered entity's workforce; therefore, business associate employees who provide services to the covered entity should complete HIPAA Privacy and Security training. Moreover, business associates should be able to evidence training completion to the covered entity.

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 (over 75%, a slight increase from last year) indicated they maintained such an inventory.

75%

WHAT THIS SUGGESTS:

As noted in previous years' surveys, 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 to conduct a random audit of the covered entity. When this occurs, OCR may 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, while the percentage is much lower than last year, an overwhelming majority of respondents (almost **72%**) answered yes to this question.

72%

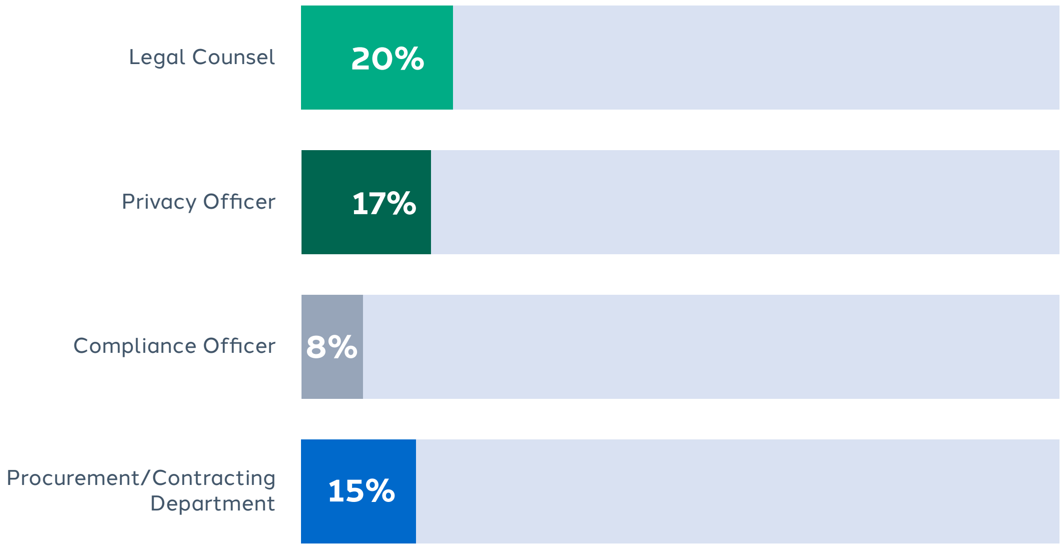
WHAT THIS SUGGESTS:

These results are lower than our previous survey (81%); however, it is a regulatory requirement to have an agreement in place with identified business associates to safeguard against unauthorized disclosures of PHI. Failure to have these agreements in place can lead to hefty fines. For example, just this past year, a physicians group agreed to pay $500,000 for failing to have a business associate agreement in place with its third-party billing company. Covered entities are advised to use a checklist 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:

While the overall results decreased from last year, the majority of respondents indicated that Legal Counsel (**20%**) is responsible for making the final determination for business associates. This was followed closely by the Privacy Officer (**17%**), and Compliance Officer (**17%**). As with our previous survey, a little more than **8%** of responses indicated that the procurement/contracting department was responsible for making the final determination. **15%** of respondents also indicated that the procurement/contracting department partnered with the Privacy Office to make 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 is helpful. Nevertheless, 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 potential business associates are 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, a procurement/contracting department is responsible for making the determination, it is advisable that at least one person in that department have a thorough understanding of the HIPAA requirements and use the aforementioned checklist to support this understanding as well as consult with the Privacy Officer.

HIPAA Investigations, Breach Management, And Audits

Q. HOW ARE MOST HIPAA PRIVACY INCIDENTS DETECTED?

WHAT WE FOUND:

The top five responses included (starting with the highest response):

1	Employee reports directly to management/HIPAA/Compliance Office	84%
2	Monitoring of user access	63%
3	Patient reports/complaints	62%
4	Hotline reports	62%
5	Reports from anonymous sources	53%

WHAT THIS SUGGESTS:

Since the previous survey, the percentage of respondents indicating that their organization learns of a HIPAA privacy incident through an employee report is significantly higher. This infers that organizations continue to promote open communication, a key element of an overall effective compliance program and employees continued to feel less ambivalent about reporting HIPAA concerns with less fear of retaliation or reprisal. The percentage of respondents receiving reports through the organization's hotline was also significantly higher. Nevertheless, relying solely on employee reports may not be ideal since reporting may be delayed, thus delaying discoveries of potential breaches and activating appropriate mitigation steps. Respondents' use of monitoring user access is much higher this year, which may infer a more proactive approach to ensure compliance with HIPAA requirements. A much higher percentage of respondents noted they detected privacy incidents through patient reports or complaints. This can be problematic, inferring a decrease in controls to avoid errors in patient disclosures, which can lead to complaints filed with the OCR.

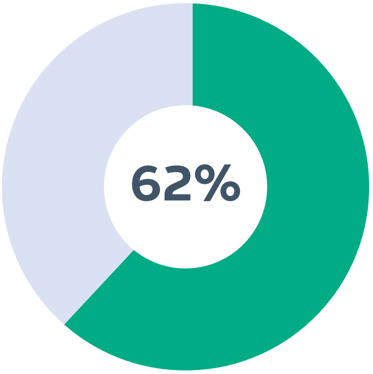
Q. WHICH OF THE FOLLOWING ITEMS ARE CURRENTLY ON YOUR HIPAA/COMPLIANCE AUDIT WORK PLAN?

WHAT WE FOUND:

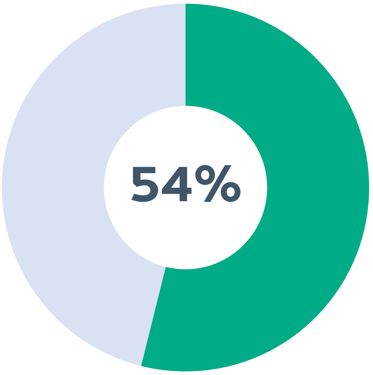
Respondents were asked to check all choices that applied to them. In this instance, user access review (of the EHR or other relevant applications) remained the top choice, garnering almost **62%** of the responses. Physical location reviews/walkthroughs came in second, but with a much lower percentage than last year (**54%** this year compared to almost **62%** last year). Individual Release of Information (ROI) request reviews (e.g., valid authorization form, received within required timeframes, etc.) received the third highest percentage of responses followed by Review of Business Associate activity.

WHAT THIS SUGGESTS:

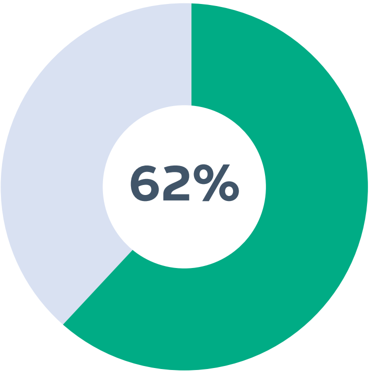
The responses continue to indicate that organizations have a wide variety of items and issues in their audit work plans. While best practices promote the use of audit work plans, smaller organizations may not have the resources to complete a formal audit. Nevertheless, organizations should consider a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



Access review



Physical location
reviews/walkthroughs

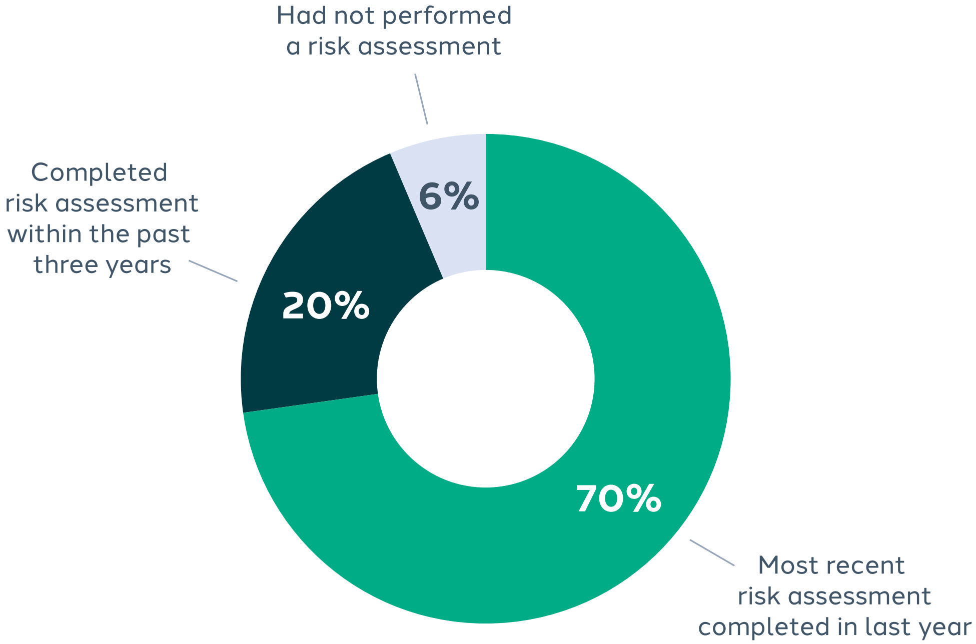


Review of
business associate activity

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, almost **70%** of respondents noted that their most recent risk assessment was completed in the last year, which is slightly lower than last year's survey response. **20%** indicated that they completed an assessment within the past three years. Almost **6%** indicated that 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 PHI held by the covered entity or business associate." The rule does not specify the frequency of conducting the assessment. OCR guidance states that the "risk analysis process should be ongoing." OCR also 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 YOUR ORGANIZATION HAD A HIPAA BREACH THAT HAS BEEN REPORTED TO THE OFFICE FOR CIVIL RIGHTS?

WHAT WE FOUND:

46%

Almost **46%** stated they reported a breach to OCR within the past year.

9%

About **9%** reported a breach within the past two years.

9%

Almost **9%** reported a breach between three and five years ago.

17%

Almost **17%** stated they had never had a breach reported to OCR.

WHAT THIS SUGGESTS:

About 64% of respondents indicated they reported a HIPAA incident to OCR over the past five years, which is a significant reduction from last year's results. As with last year's results, the majority of the HIPAA breaches were reported within the last 12 months. While it is impossible to prevent all breaches, training of the workforce, and early detection of potential incidents with an immediate investigation followed by remediation as needed will continue to contribute to managing breach identification and reduction. Organizations are advised to implement industry-accepted best practices to decrease the possibility of a data breach involving electronic PHI. This includes data encryption, multi-factor authentication, training, software updates, implementing role-based access for employees to access PHI, and removing access for employees who leave the organization. OCR is a good source for guidance.

HIPAA Program Planning, Priorities, And Resources

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 five priorities included (starting with the highest response):

1	Incident response and reporting	54%
2	Reducing inappropriate/ inadvertent disclosures of PHI by workforce	50%
3	Monitoring inappropriate access to PHI/snooping by workforce	45%
4	Breach notification management	40%
5	Monitoring Business Associate Agreements and activity	38%

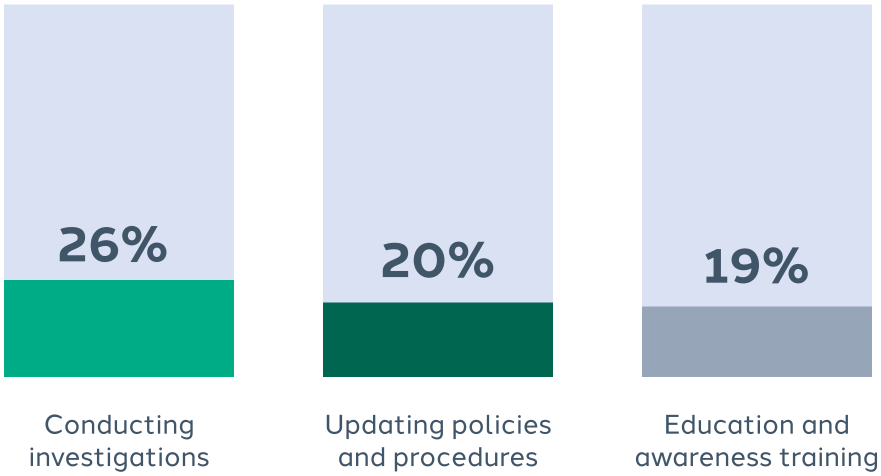
WHAT THIS SUGGESTS:

The priorities and associated percentages are similar to prior surveys; however, breach notification management took a higher priority than monitoring Business Associate Agreements and activity. Among the top three priorities, reducing inappropriate/inadvertent disclosures of PHI by the workforce was a higher priority this year than monitoring inappropriate access to PHI/snooping by workforce, which dropped by seven percentage points. Nevertheless, the results continue to demonstrate a need for increased training and education about the HIPAA Privacy Rule, increased monitoring of EHR access, and a need for greater controls over access to the EHR. Moreover, these 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.

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

WHAT WE FOUND:

- Almost **26%** of respondents indicated that conducting investigations took the most planning and resources.
- **20%** stated updating policies and procedures took the most planning and resources.
- **19%** stated that education and awareness took the most planning and resources.



WHAT THIS SUGGESTS:

The responses to this year's survey are not very different from the last survey; however, this year, updating policies and procedures was a slightly higher priority than education and awareness. Regardless, these results imply that organizations are using standardized processes and timelines for updating policies and procedures, thereby reducing the amount of time spent planning for this activity.

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 **61%** reported Incident Reporting Tool (i.e., HIPAA Hotline).

57% reported Learning/Training Management System.

42% reported Incident Tracking Software.

41% reported Policy Management Software.

Almost **35%** reported automated monitoring of users' access to PHI.

20% reported an automated review of audit logs and reports from the EHR system.

Almost **21%** reported Investigation Management Software.

WHAT THIS SUGGESTS:

All percentages are lower than last year; however, the percentage of organizations reporting that they did not use any type of software for their privacy program operations decreased by almost 50%. Software programs 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. Recognizing that not all organizations have the resources for elaborate expensive tools, even the use of spreadsheets to track audits, policies, breaches, and training will provide the critical documentation to evidence an effective HIPAA compliance program.

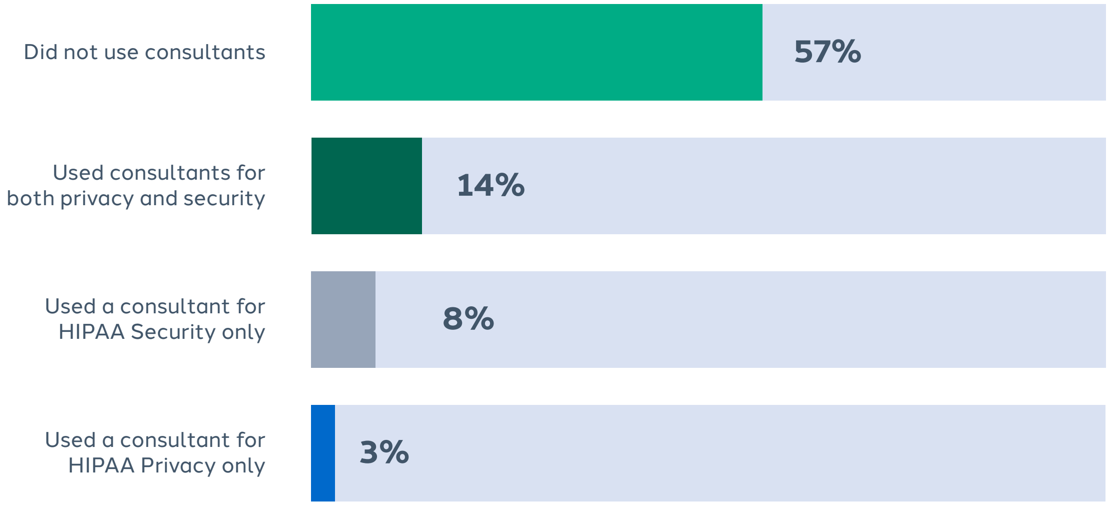
Q. DOES YOUR ORGANIZATION USE ON-CALL CONSULTANT/VENDOR SERVICES TO ASSIST WITH HIPAA PRIVACY AND SECURITY FUNCTIONS (E.G. TRAINING, INVESTIGATION BREACHES, ASSISTING WITH EVALUATIONS, POLICIES AND PROCEDURES, RISK ANALYSIS, ETC.)?

WHAT WE FOUND:

- **57%** of the respondents stated that they did not use consultants.
- **14%** reported they used consultants for both privacy and security.
- Almost **8%** used a consultant for Security.
- Only **3%** used a consultant for HIPAA Privacy.

WHAT THIS SUGGESTS:

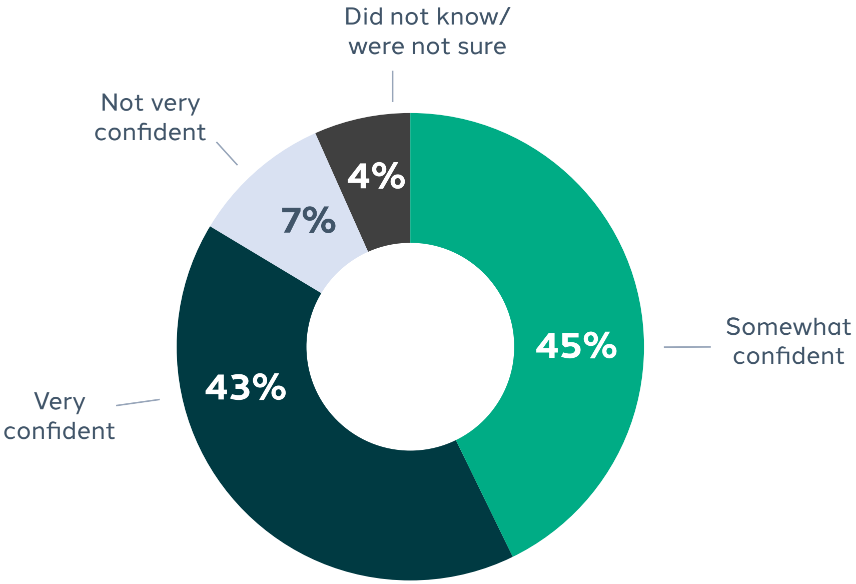
The responses to this year's survey are slightly lower than last year's survey with percentages varying by just a few points. Notably, respondents using a consultant for security functions were five percentage points lower than last year. The HIPAA Privacy and Security Rules are silent on the use of consultants to meet the HIPAA requirements. 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

- **45%** stated that they were somewhat confident.
- Almost **43%** stated that they were very confident.
- **7%** stated that they were not very confident.
- **4%** stated that they did not know/were not sure if they were meeting regulatory requirements.



WHAT THIS SUGGESTS

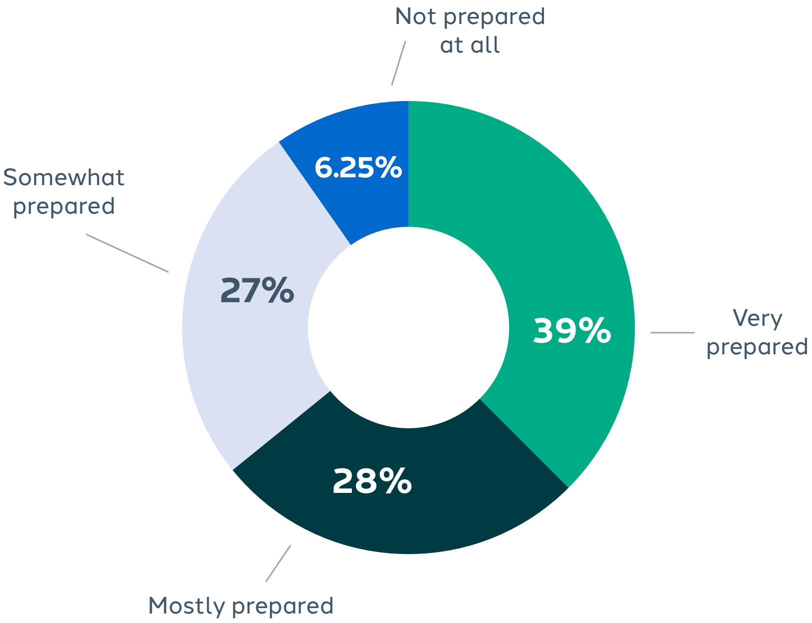
There continues to be a two-percentage point gap between respondents who are “somewhat confident” and those who are “very confident.” Both responses show a decrease from last year’s survey response. There was a decrease in the number of respondents who were not very confident. Of note, 4% of this year’s respondents indicated that they did not know or were unsure if their organization was meeting the requirements. Last year, none of the respondents indicated as such. Organizations that do not have sufficient confidence that their program is meeting regulatory requirements are advised to consider conducting a gap analysis to identify those areas that are causing a lack of confidence.

Enforcement

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

WHAT WE FOUND:

- Almost **39%** stated they were very prepared.
- About **28%** stated they were mostly prepared.
- Almost **27%** felt they were somewhat prepared.
- **6.25%** stated they were not prepared at all.



WHAT THIS SUGGESTS:

The combined percentage of respondents who indicated that they were prepared is a slight increase from last year's survey. The percentage of respondents stating they were mostly prepared was significantly lower than last year, while the percentage of those stating they were very prepared was much higher. There was an almost 10 percentage point increase in respondents who felt they were somewhat prepared. Notably, the percentage stating they were not prepared at all fell by more than two percentage points. All organizations are advised to continue 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, etc., can an organization evidence to OCR that they have the foundation for an effective HIPAA compliance program.

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

WHAT WE FOUND:

29%

Almost **29%** of respondents stated that an effectiveness evaluation had been performed within the last year.

12%

Almost **16%** had an evaluation conducted within the last three years.

43%

43% stated that either an evaluation had not been performed, or they were unsure of whether it had been performed.

WHAT THIS SUGGESTS:

The data for this year's survey is not very different from prior surveys. Conducting an effectiveness evaluation 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. WHAT TYPE OF ENCOUNTERS HAS YOUR ORGANIZATION HAD WITH OCR IN THE LAST 2 YEARS?

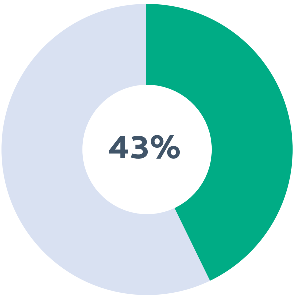
WHAT WE FOUND:

- Over **43%** of respondents indicated that they had not had any encounter with OCR over the past two years.
- **18%** had an investigation/inquiry regarding a breach report for an incident involving under 500 individuals.
- **13%** had an investigation/inquiry regarding a breach report for an incident involving more than 500 individuals.
- More than **14%** indicated their interaction with OCR was for Technical Assistance.

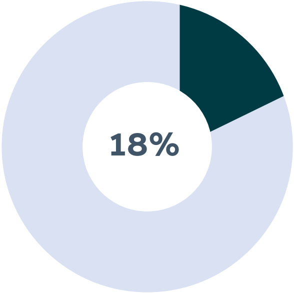
WHAT THIS SUGGESTS:

While the percentage of respondents reported having no encounter with OCR in the past two years decreased by 2% this year, it can still be inferred that the organizations have strong HIPAA Privacy and Security practices such as training, data encryption, access controls, etc., in place to protect against breaches resulting in an OCR encounter. It should also be noted that the percentage of respondents noting that their encounter with OCR was for Technical Assistance slightly increased this year, which may be reflection of OCR's focus on helping covered entities improve their processes rather than take punitive actions. These percentages should also be balanced against the almost 46% of respondents stating that they reported a breach to OCR within the past year.

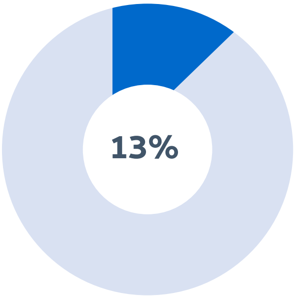
Responses may also correlate to the responses to our question about how HIPAA Privacy incidents are detected wherein almost 84% of respondents indicated that employees report issues directly to leadership. This allows the HIPAA Privacy Office to investigate a potential issue to either avert or detect a breach sooner and report according.



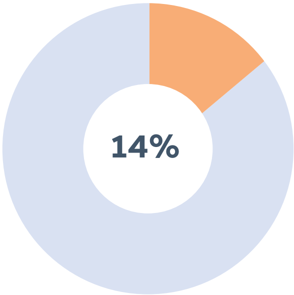
Had no encounter with OCR over past two years



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



Indicated their interaction with OCR was for Technical Assistance

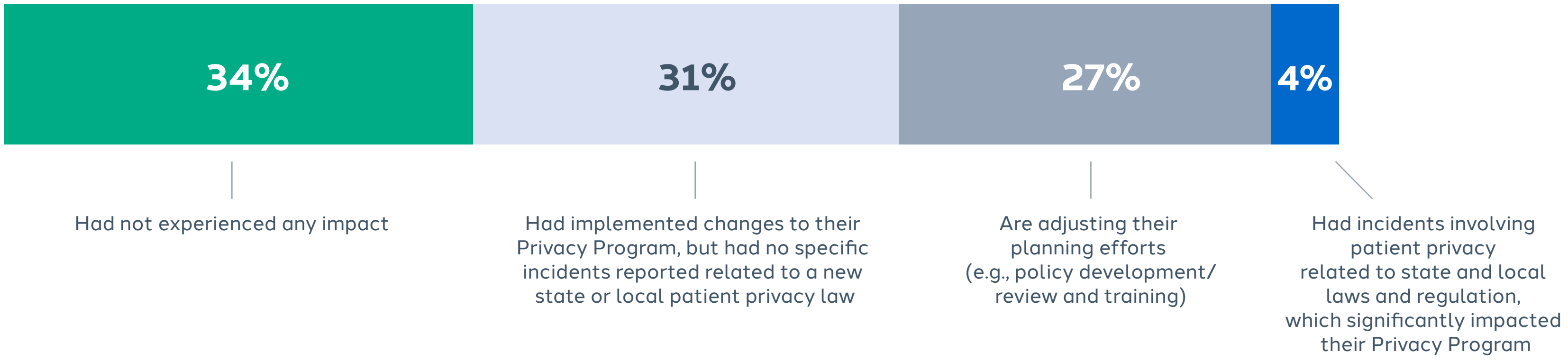
Q. WHAT TYPE OF IMPACT HAS THE IMPLEMENTATION OF PATIENT PRIVACY-RELATED STATE AND LOCAL LAWS HAD ON YOUR PRIVACY PROGRAM?

WHAT WE FOUND:

- Almost **34%** indicated they had implemented changes to their program, but no specific incidents were reported related to any new state or local patient privacy law.
- About **31%** of respondents indicated they had not experienced any impact.
- Almost **27%** are adjusting their planning efforts.
- A little more than **4%** had incidents involving patient privacy related to state and local laws and regulations, which significantly impacted their privacy program.

WHAT THIS SUGGESTS:

This year's survey indicated a slight increase in the percentage of respondents who had implemented changes to reflect state or local laws. This may be indicative of increased state legislative and regulatory changes to safeguard patient privacy. While many state privacy laws continue to exempt organizations that are subject to HIPAA privacy and security requirements, covered entities should continue to monitor state policy makers for changes. They should also continue to 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 privacy office with the state department of health.



Q. HAVE YOU BEGUN CHANGING YOUR NOTICE OF PRIVACY PRACTICES AND REVISING EXISTING OR CREATING NEW POLICIES AND OTHER DOCUMENTS TO REFLECT THE NEW REQUIREMENTS CONTAINED IN THE OCR'S LATEST FINAL RULE RELATING TO PART 2 AND REPRODUCTIVE HEALTH?

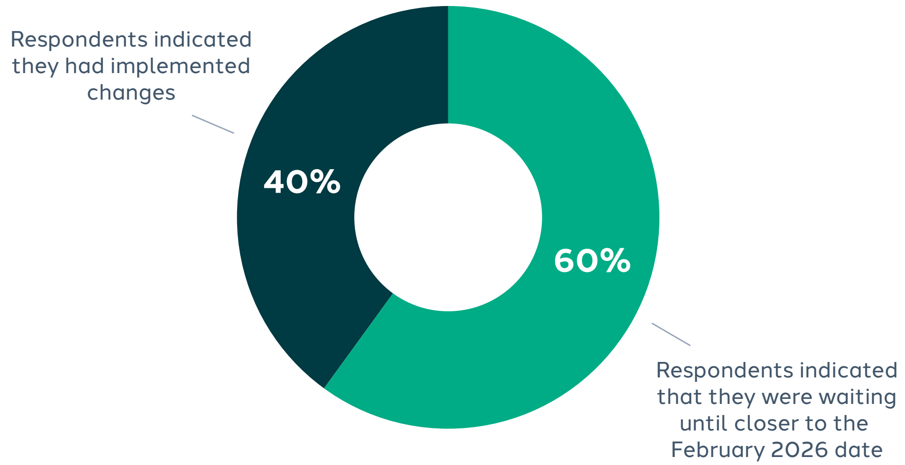
WHAT WE FOUND:

60%

A little more than **60%** of respondents indicated that they were waiting until closer to the February 2026 date.

40%

Almost **40%** of respondents indicated they had implemented changes.



WHAT THIS SUGGESTS:

This was the last of our new questions for this year's survey. It is usually a best practice to implement changes to final requirements sooner rather than later. Given that the changes are not effective for another year, it is not out of the question to wait to ensure there are no other changes prior to the effective date. Nevertheless, the requirements should remain on the Privacy Officer's workplan for implementation before the current 2026 effective date.

Conclusion

As in years past, this report provides a summary of responses from this year's survey, as well as an analysis of how answers compare to the prior HIPAA survey that was administered in 2023 as reported in 2024. Notably, there was an increase in the percentage of respondents representing behavioral mental health entities, which may reflect the connection between the Health Resources and Services Administration and the Office for Civil Rights in safeguarding the privacy of individuals with substance use disorders. There was also a slight increase in the number and associated percentage of respondents representing health plans and insurance companies. As with our prior 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 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 the workforce, 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.

The majority of organizations surveyed appear to have implemented operations to address HIPAA requirements, with policies and procedures maintained in a central computerized location, and HIPAA compliance training provided during new employee orientation and annually thereafter. These 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.

Survey results also show that organizations are auditing a wide variety of items and issues with user access at the top of the 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 did not know whether one 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 other HIPAA Privacy Rule requirements.

Overall, the majority of respondents indicate that they are mostly or somewhat prepared for an OCR audit or investigation. Additionally, it was reported that most organizations do not use on-call consultant/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.

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.

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.