2019 HIPAA Compliance Survey Report

STRATEGIC MANAGEMENT

SAI GLOBAL

Table of Contents

2019 HIPAA Compliance Survey Report

For the first time, a national HIPAA compliance survey conducted by SAI Global, in collaboration with Strategic Management Services, LLC, explored the current state of HIPAA compliance. Our goal was to better understand the nature and level of commitment that healthcare organizations have made to HIPAA compliance in 2019.

The report covers a wide range of topics such as:

- HIPAA program structure, responsibility and oversight
- Program operations
- Business Associate Agreements (BAA) management
- Program assessment and priorities
- Investigations, breaches, and disciplinary action and interactions with enforcement

The national survey was conducted among 352 respondents located in different states within the United States and representing various provider types. Over half of respondents reported being associated with a hospital or health system, with 9% working with a physician/group practice and 7% connected with a clinic or ambulatory surgery center. The remaining respondents were dispersed over a variety of health care provider types, health plans, and business associates (i.e., device manufacturer, pharmaceutical company, etc.). The range of entities represented by respondents evidences that HIPAA compliance is an issue that cuts equally across the entire healthcare spectrum.

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

HIPAA Compliance Survey Highlights

HIPAA Program Staffing and Oversight

Many organizations reported having relatively minimal staffing support for their privacy office operations and an inconsistent approach to HIPAA oversight. This finding suggests a lack of clear industry guidance as to where HIPAA accountability should lie. Including, to whom the Privacy Officer should report to and how top-level management and the Board of Directors should be involved or both, in HIPAA oversight.

HIPAA Program Policies and Training

A majority of healthcare organizations reported a basic understanding and attention to the HIPAA program requirements addressing the implementation of policies and procedures, as most respondents reported having at least five HIPAA policies in place, with others having twenty or more, that undergo a regularly scheduled review and revision process. Virtually all respondents noted that training is conducted on at least an annual basis. They stated that records of HIPAA compliance training are maintained documenting who attended the training when it occurred and what type of training took place.

High Priorities for HIPAA Programs

Survey participants largely agreed on their top five priorities for their HIPAA compliance program in the coming year included: reviewing and updating HIPAA compliance policies/procedures, developing/delivering HIPAA training programs, reducing inappropriate/inadvertent disclosures of PHI by workforce members, implementing processes for monitoring ongoing HIPAA privacy compliance, and tracking investigations and corrective actions to completion.

Encounters with Enforcement

Survey results suggest that organizations reporting breaches to Office of Civil Rights (OCR) are not alone. A majority of respondents have reported a HIPAA breach to OCR within the last five years, with a little less than half of those organizations reporting a breach within the previous year.

Identification and Management of Business Associate Agreements (BAAs) and Relationships

Many healthcare organizations reported having a single, uniform process for entering into and maintaining BAAs. Responses noted that the departments responsible for both determining when a BAA is necessary and for maintaining BAAs were closely divided between the following four departments: privacy office, compliance office, legal counsel and procurement/contracting department. A small percentage of organizations stated that their BAAs were maintained in the various departments, not in one central location. Where an organization's BAA process is not centralized, it is absolutely imperative that the Privacy Officer be able to identify, understand, and produce a listing of all BAAs in order to evidence compliance with the business associate related requirements.

Use of Vendors

A third of respondents indicated that their organizations hire a consultant or vendor to assist with HIPAA privacy and security program functions, such as conducting training, helping with policy development, and risk analysis. Organizations also indicated that they use outside assistance for HIPAA training, assessments and to address breaches. A small percentage of organizations outsource their entire HIPAA privacy officer function.

Demonstrating HIPAA Compliant Effectiveness

A little less than half of the organizations noted they have never had an independent effectiveness evaluation of their HIPAA privacy program. Having an outside organization conduct an independent assessment of a HIPAA privacy program may be particularly helpful for any organization to evidence the effectiveness of their HIPAA program and is particularly useful for small privacy and compliance workforces that only have the bandwidth to respond to day-to-day activities.

HIPAA Program Structure: Responsibility and Oversight

Q. What is the staffing level for the HIPAA privacy office function?

What We Found

67% of survey respondents indicated that they either have only one full-time or less than one full time person in their organization's HIPAA Privacy Office. The remainder of respondents specified that their HIPAA privacy office staff consists of more than one full-time individual.

What This Suggests

Results suggest that many organizations may have minimal staffing support for HIPAA privacy office functions. While it is expected that smaller organizations may have a Privacy Officer who also has other job responsibilities (i.e., may have only part-time responsibilities that are HIPAA related), these results indicate that some larger-scale healthcare organizations also may employ only one person who is tasked with HIPAA privacy responsibilities. Issues focused on compliance and HIPAA are both complicated and demanding. Having only one person responsible for HIPAA privacy related operations is unrealistic in medium and large size organizations, given the risks associated with failure to comply with HIPAA or other traditional healthcare compliance rules and regulations.

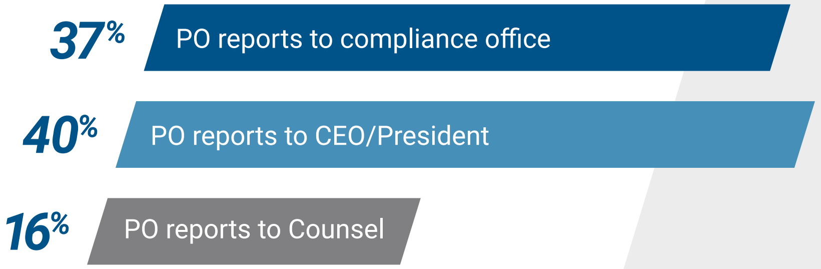
Q: To whom does your privacy officer report?

What We Found

About **37%** of our survey group stated that the Privacy Officer reports internally to the compliance office, with **40%** of Privacy Officers reporting directly to the CEO/President of the organization. To a lesser extent, about **16%** of respondents had Privacy Officers reporting directly to Legal Counsel, which is also not surprising given the increasing legal enforcement of HIPAA related to breach incidents by the Office for Civil Rights (OCR). A significant number of respondents also indicated that their Privacy Officer reported to other various parts of the organization, such as to the Chief Financial Officer (CFO), the Chief Operations Officer (COO), the Board of Directors (Board), Health Information Management, Information Technology, and Risk Management.

What This Suggests

It appears that, for many organizations, HIPAA privacy follows the same course as compliance by reporting directly to the CEO/President. Although the "2019 Healthcare Compliance Survey" showed that over half of respondents include HIPAA privacy functions as part of compliance operations, these survey results demonstrate that Privacy Officers may also have a reporting responsibility to higher authorities, beyond the compliance office. Survey results also show that top-level management and, in some cases, the Board of Directors, are becoming directly involved in the operational oversight of HIPAA.



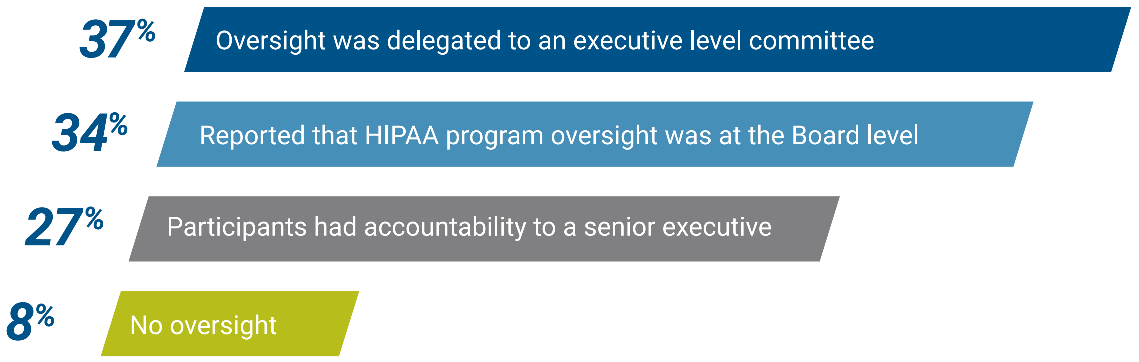
Q: Who is accountable for oversight of HIPAA operations?

What We Found

- **37%** noted that oversight was delegated to an executive-level oversight committee, either focused on compliance overall (i.e., Executive Compliance Committee) or directly on HIPAA privacy and security
- **34%** reported that HIPAA program oversight occurs at the Board level, either by a Board-appointed committee or the full Board of Directors
- **27%** of participants identified having accountability to a specific senior executive official like the CEO, Legal Counsel,
- or Chief Information Officer (CIO)
- **8%** of respondents stated that there is no oversight body for HIPAA

What This Suggests

A growing number of organizations appear to be appointing an executive-level compliance committee or Board level committee for HIPAA oversight, which is similar to guidance provided by the HHS OIG for compliance program oversight. The survey data also suggest that there may be ample opportunity to increase Board of Director's involvement in HIPAA oversight responsibilities, particularly for organizations that consider HIPAA a high-risk area, as as a minority of respondents reported as a minority of respondents reported board accountability.



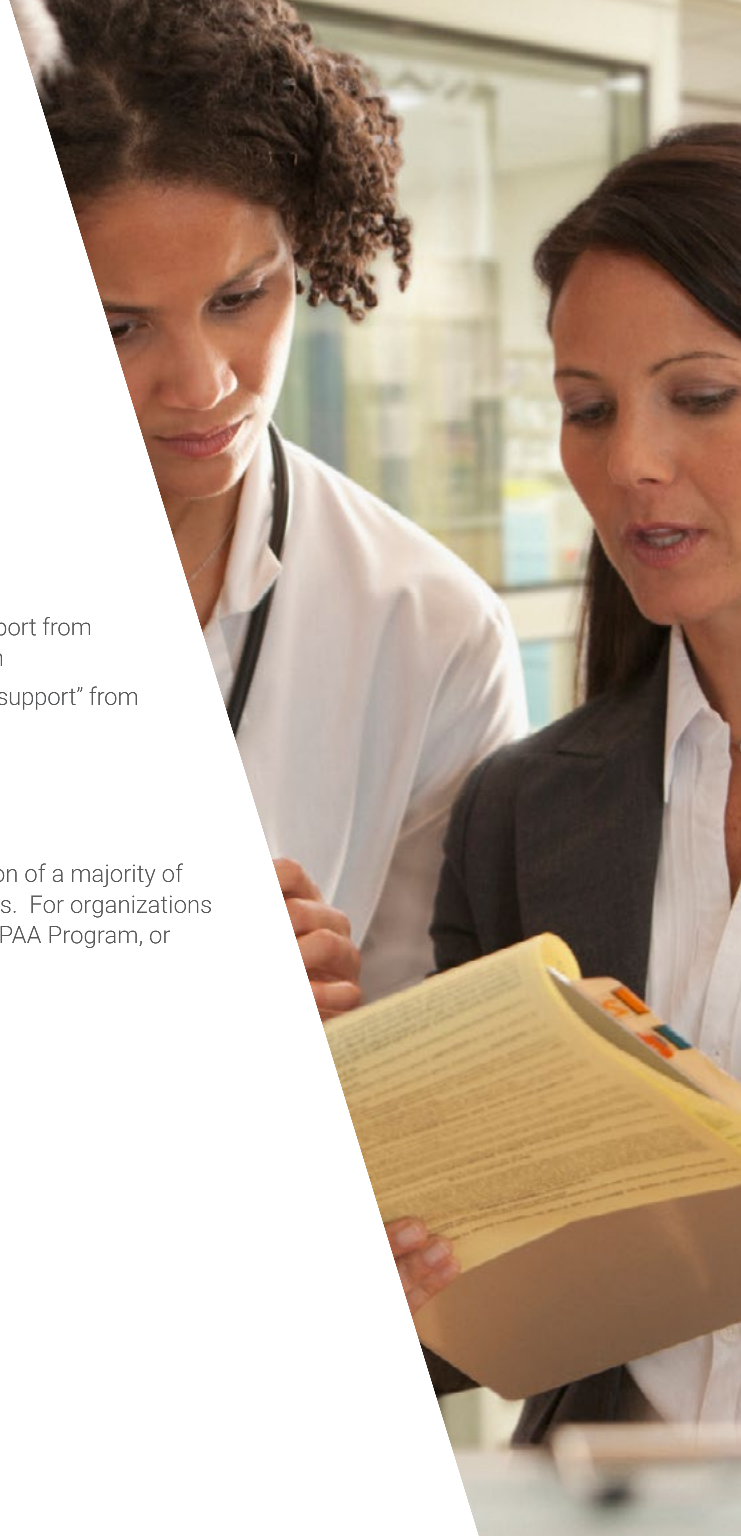
Q: Which of the following statements best describes the support received from your executive leadership and Board of Directors?

What We Found

- Approximately **80%** of respondents reported: "positive" support from executive leadership and the Board for their HIPAA program
- The remaining **20%** of respondents reported: "weak" to "no support" from executive leadership or their organization's Board

What This Suggests

Evidence strongly indicates that HIPAA has captured the attention of a majority of executive leadership and Boards across healthcare organizations. For organizations that do not have executive leadership, Board support for their HIPAA Program, or both, it is critical to find ways to correct this deficiency.



HIPAA Program Structure: Policies, Procedures and Training

Q: How many HIPAA related policies and procedures does your organization have?

What We Found

- About **69%** of our survey group has enacted 10 or more policies, with **39%** percent of that group claiming to have more than 20 policies in place
- Approximately **24%** of the respondents reported having 10 or fewer policies, which is likely inadequate to address the HIPAA rule requirements adequately.
- Only **7%** reported that they did not know if their organization had HIPAA policies and procedures

What This Suggests

Considering the number of requirements that need to be addressed across the Privacy, Security, and Breach Notification Rule, adopting 20 or more reasonable and appropriate policies is good practice. It is also possible that some organizations may have "runaway" policies or a policy manual, which aim to address a multitude of issues in a single policy document. With that in mind, organizations with minimal HIPAA policies may wish to conduct a gap analysis of the policies they have against the HIPAA standards for Privacy, Security and Breach Notification to ensure that all applicable requirements are addressed.

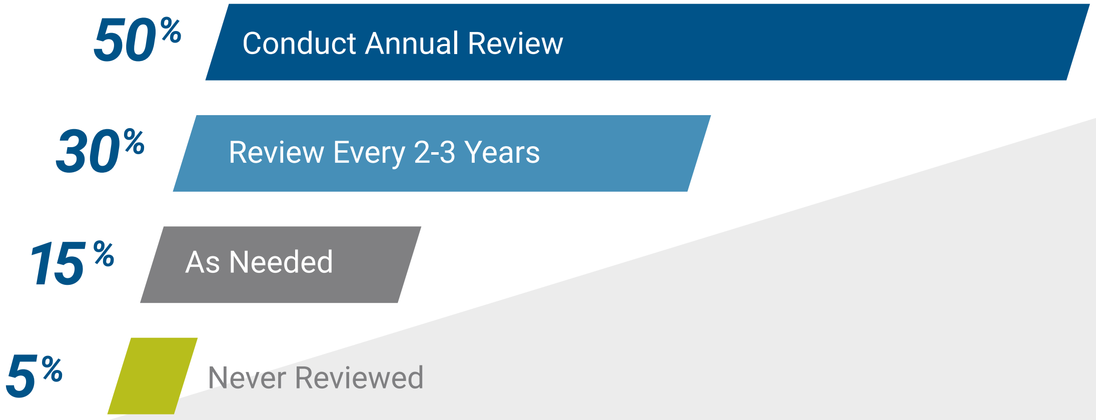
Q: How often are your HIPAA policies and procedures reviewed and updated?

What We Found

- The data revealed that **50%** of participants conduct an annual review of their HIPAA policies and procedures
- **30%** reported that reviews are completed every 2-3 years
- About **15%** of respondents reported reviewing and updating their policies only on an "as needed" basis
- Only **5%** responded not knowing when policies are reviewed or that they are never reviewed and updated

What This Suggests

Because the privacy and security regulatory environment is rapidly changing at both the federal and state level, most organizations should consider reviewing and updating their HIPAA policies and procedures at least once a year. This has been reinforced by OCR, in their recent Resolution Agreement Corrective Action Plans (CAP), where they require entities to conduct annual reviews of the policies and procedure required to be implemented by the CAP.



Q: How often do you conduct HIPAA compliance training with your employees?

What We Found

95% of survey respondents reported that they conduct HIPAA training on an annual basis. Most noted that HIPAA training was administered at both the time of hire and annually after that which is considered best practice. Only **2%** reported providing training at the time of hire only. The remaining **3%** were not sure.

What This Suggests

Results provide convincing evidence that organizations understand the HIPAA requirements for training, including the importance of using training as a tool for educating employees, outlining employee expectations and ensuring employee compliance with HIPAA requirements.

95%

CONDUCT HIPAA TRAINING ON ANNUAL BASIS

Q: Does your organization maintain a record of HIPAA compliance training that includes the following: when the training took place; who was trained; what was included in the training?

What We Found

Virtually all respondents indicated that they maintain HIPAA compliance training records, particularly documentation of who was trained when it took place and what was included in the training.

What This Suggests

This suggests that organizations in the healthcare sector have an adequate understanding of the training expectations outlined in the HIPAA Privacy and Security Rule requirements.

Q: How are employees within your organization made aware of methods to encrypt emails containing PHI?

What We Found

- About **86%** of respondents note that their organization has communicated encryption procedures to their employees. **46%** indicated employees are trained on encryption methods upon hire, with **25%** reporting that periodic communications are sent regarding encryption methods to their workforce
- Approximately **18%** noted that training of employees regarding encryption was provided "as needed" or no training was provided at all
- Only **5%** of organizations reported that they do not train employees regarding encryption and **3%** said that they do not utilize any solution for email encryption

What This Suggests

OCR has consistently emphasized the importance of having encryption processes in place for protecting electronically protected health information (ePHI), both while stored on devices (referred to as "data at rest") and when in transmission (i.e., sent via email or text). The HIPAA breach notification requirements explicitly state that organizations do not have to report instances where a device containing ePHI is misplaced or stolen if the data was encrypted. OCR has noted that it will not be sympathetic during breach investigations to organizations that do not encrypt their data, as it is a strongly suggested best practice.

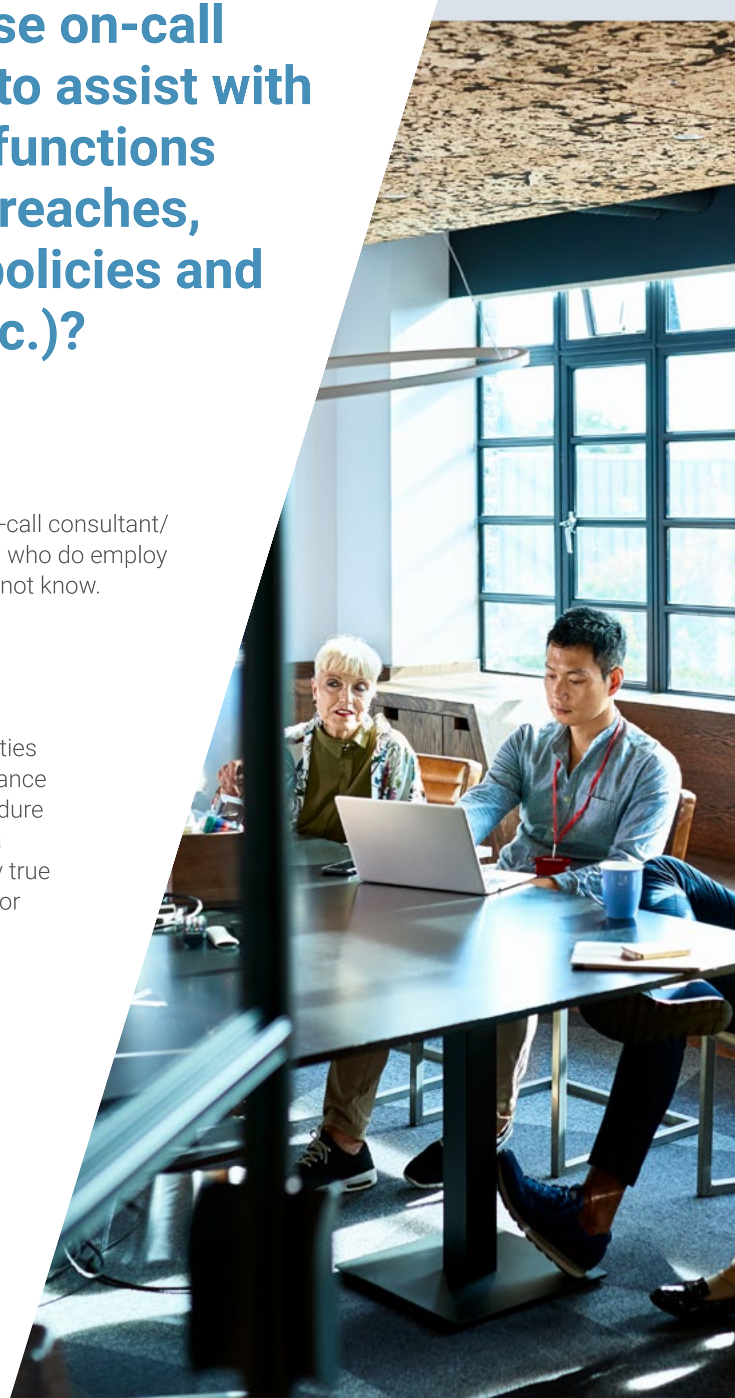
Q: Does your organization use on-call consultant/vendor services to assist with HIPAA privacy and security functions (i.e. training, investigation breaches, assisting with evaluations, policies and procedures, risk analysis, etc.)?

What We Found

Nearly **65%** of our surveyed group stated that they do not use on-call consultant/vendor services compared to approximately **30%** of respondents who do employ contractors to assist with HIPAA program functions. And **5%** did not know.

What This Suggests

The HIPAA Privacy and Security rules do not require covered entities or business associates to use outside vendors, but they can enhance your HIPAA operations by performing tasks like policy and procedure development and review, breach investigations and conducting a HIPAA risk analysis or HIPAA evaluation. This may be particularly true for smaller organizations that have limited personnel resources or technical expertise to perform these tasks adequately.



Business Associate Agreements

Q: Who determines if a business associate agreement (BAA) is needed with a third-party vendor?

What We Found

Participants answered evenly across the board that a combination of their Compliance Office, Privacy Office, Legal Counsel, or Procurement/Contracting Department oversee and are involved in the process of determining if a BAA is needed. There were **7%** of respondents who did not know who makes the determination.

What This Suggests

It appears that there is no standardized process for making BAA determinations, as it seems to differ widely throughout the survey population. Although there is no regulatory requirement that the Privacy Officer or Legal Counsel be involved in this process, it is recommended that they be available for review of the ultimate decision made, as it might not always be a straight forward determination. Many organizations rely on their Procurement or Contracting Department to make an initial determination of whether a BAA is necessary, with the final review of the BAA going to Legal Counsel, the Privacy Officer, or both. It is also particularly important to have the Privacy Officer, Legal Counsel, or both involved in the review of the BAA to ensure that specific provisions outside of the basic HIPAA requirements are included to adequately protect the organization from a liability standpoint (i.e., indemnity clauses and cybersecurity insurance guarantees).

Q: Who maintains your business associate agreements (BAAs)?

What We Found

Similar to the previous question, respondents noted that the responsibility to maintain BAAs is distributed among several departments:

- **32%** maintained in the Compliance Office
- **30%** maintained in the Privacy Office
- **26%** maintained in by the Procurement/Contracting Department
- **26%** maintained by the Legal Department

Notably, **13%** of respondents responded that their BAAs were not centrally held, as they are maintained in various departments.

What This Suggests

While the survey data shows a varied approach to the type of department that maintains BAAs, it also demonstrates that most organizations have centralized this responsibility. Nevertheless, there was a minority of respondents that stated that BAAs are kept in the various departments that hold the contract, not in one central location. When an organization discloses PHI to a business associate without a BAA in place, it creates a significant liability for both the covered entity and business associate, since having a BAA is a requirement under both the HIPAA Security and Privacy rules. In its last round of audits, OCR emphasized that it expects organizations to be able to produce a current list of all its BAAs to evidence compliance with the business associate related requirements. Organizations should strive to have a single, uniform process for entering into BAAs and should maintain the BAAs in one department or location. A centralized contracting and BAA process may reduce the risk of contracting with a vendor without a necessary BAA and allow for better monitoring and auditing of business associate activity.

HIPAA Program Assessment and Main Priorities

Q: When was the last time the effectiveness of your HIPAA privacy program was independently evaluated?

What We Found

44% of respondents commented that an independent party had evaluated the effectiveness of their organization's HIPAA privacy program within the last three years. **23%** of that group stating that the evaluation had occurred within the previous year. **8%** reported it had been at least three years since their last effectiveness review. The other **49%** of respondents indicated that either an effectiveness evaluation of their HIPAA privacy program had never been conducted or that they did not know if one was ever completed.

What This Suggests

Having an outside organization conduct an independent evaluation of a HIPAA privacy program may be particularly helpful for organizations with small privacy and compliance workforces that do not have the bandwidth to respond to day-to-day activities, as well as conduct retrospective reviews to ensure they are meeting all the HIPAA requirements and that their program is effective. It is also helpful for organizations that are not traditional healthcare providers and are newer to HIPAA, such as behavioral health organizations, medical device manufacturers, and health IT and application companies.

Q: Has your organization conducted a thorough assessment of the risks and vulnerabilities related to your ePHI (i.e., risk analysis)?

What We Found

70% of respondents indicated that their organization had conducted a thorough assessment of the risks and vulnerabilities related to electronic Protected Health Information (ePHI), with the remaining **30%** noting that either they had not conducted a Risk Analysis or that they did not know if one had been completed.

What This Suggests

Risk Analysis and Risk Management are two critical components of the Administrative Safeguards of the HIPAA Security Rule. Conducting an accurate and thorough Risk Analysis is not only crucial from a data security standpoint but also a HIPAA compliance standpoint as it is a required element of the Security Rule and a significant OCR enforcement priority. OCR has penalized covered entities and business associates that failed to meet the Risk Analysis requirement in more than half of their latest Resolution Agreements and have included a requirement for those entities to conduct an annual Risk Analysis within their related Corrective Action Plans.

30%

HAD NOT OR DIDN'T KNOW HOW TO CONDUCT A RISK ANALYSIS

Q: How confident are you that your organization is meeting the HIPAA privacy, security and breach notification rule requirements?

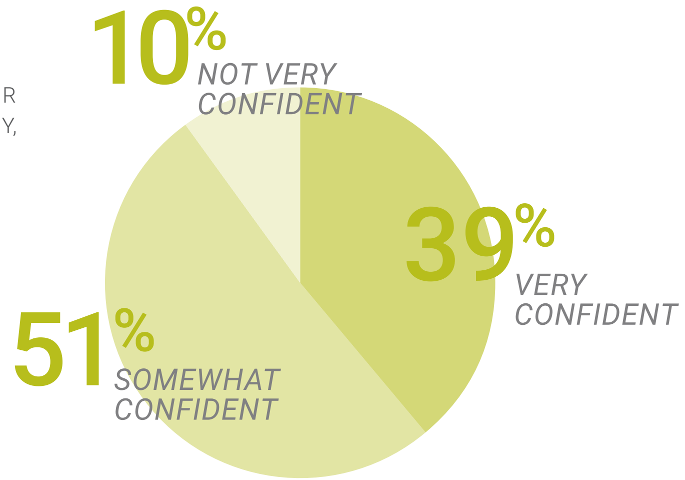
What We Found

Approximately **39%** of respondents answered that they were "very confident" that their organization was meeting HIPAA privacy, security and breach notification requirements. **51%** of respondents indicated they were "somewhat confident" of their HIPAA compliance, with **10%** noting that they were "not very confident" of meeting all HIPAA requirements.

What This Suggests

For organizations that lack confidence in whether they are meeting specific requirements, it may be beneficial to conduct a gap analysis of current processes against the various HIPAA rule requirements to identify and remediate areas that are causing concern.

RESPONDENTS CONFIDENCE WITH THEIR ORGANIZATION MEETING HIPAA PRIVACY, SECURITY AND BREACH NOTIFICATION REQUIREMENTS



Q: Which of the following describes how your organization is meeting the challenges of the fluctuation of HIPAA privacy needs?

What We Found

- **63%** of organizations noted that they have used outside assistance to conduct certain portions of their HIPAA privacy function
- **28%** of respondents indicated that no outside support had been needed to meet challenges within the HIPAA privacy function
- **26%** similarly responded that their organization seldom needed outside assistance for HIPAA privacy matters
- **1%** responded that the entire HIPAA privacy officer function had been outsourced

What This Suggests

Since the majority of the survey respondents are hospitals and health systems, these covered entities likely have personnel and resources to conduct most of these functions in-house. However, for other types of organizations or smaller providers, it may be more time and resource-efficient to obtain outside help with portions of their HIPAA operations (i.e., risk analysis, breach response, and training), particularly since forgoing these tasks or performing them poorly can create significant HIPAA compliance and enforcement risk.

Q: Please select the top three priorities to be addressed by your HIPAA compliance program in the next 12 months.

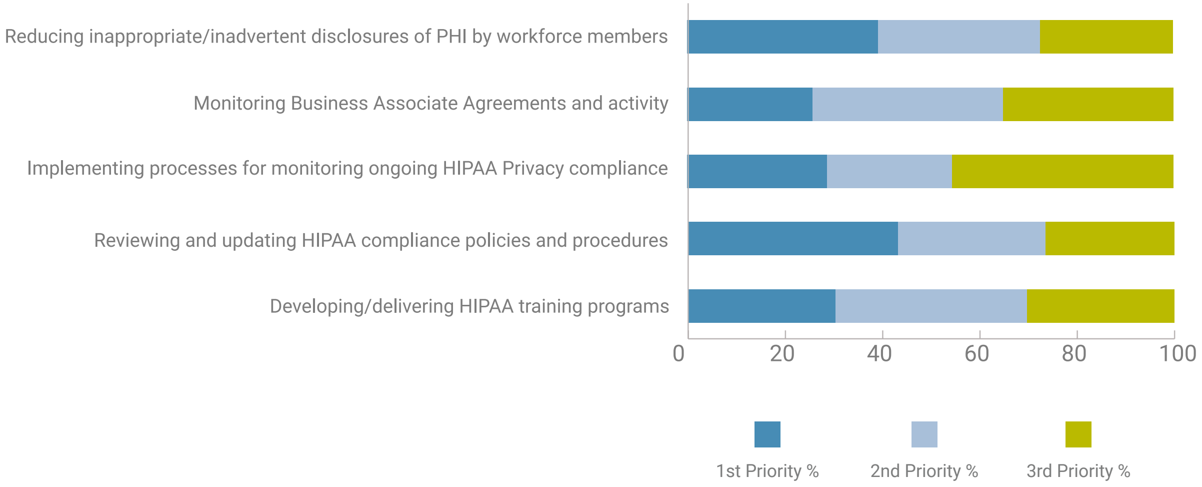
What We Found

When asked about their top three priorities for the coming year, a majority of survey participants largely agreed on the same 5 topics as their 1st, 2nd, and 3rd priorities. Overall, a large portion of survey respondents indicated that they also would be focusing on monitoring Business Associate Agreements and activity and monitoring inappropriate access to PHI.

What This Suggests

The responses indicate that organizations are understandably concerned and actively prioritizing these areas of HIPAA program operations, as OCR has identified many as legitimate risk areas. It is particularly telling that covered entities and business associates are concerned with addressing issues with monitoring business associate activity and reducing inappropriate disclosures by workforce members, as these continue to be a high compliance priority for OCR over the past few years.

Top Priorities for HIPAA Compliance Program



Investigations/Breaches/ Disciplinary Actions

Q: How are most HIPAA privacy incidents detected?

What We Found

- **64%** of respondents stated that their organization becomes aware of a HIPAA privacy incident because an employee reports the event to management or a HIPAA or compliance officer
- **37%** of respondents also said that patient-reported incidents or complaints are how most of their privacy incidents are detected
- **34%** of respondents reported that HIPAA privacy incidents are most often detected through monitoring of user access
- **39%** of respondents stated the events are identified via hotline reports or internal reporting system reports
- **15%** of respondents receive reports from anonymous sources

What This Suggests

The high percentage of privacy incidents identified through workforce members and the hotline indicates that organizations are successfully educating their workforce on the importance of reporting any HIPAA issues that they see or experience. It also appears that some organizations are effectively implementing automatic monitoring solutions to solutions to identify privacy incidents caused by inappropriate user access proactively.

Q: Do you conduct automated monitoring or audits of users accessing PHI?

What We Found

- **27%** of respondents stated that they proactively monitor user access and activity by conducting regular reviews, with **22%** noting that they use an automated system to monitor user access
- **19%** of respondents answered that they perform ad hoc user access reviews, likely when investigating an issue that has been reported
- **26%** of respondents reported that they do not conduct any automatic or manual surveys of user access to PHI and the remaining respondents were unsure

What This Suggests

There are several technical and administrative safeguard requirements under the Security Rule that address how organizations must monitor access, use and disclosure of PHI, including those related to information system activity review, log-in monitoring, security incident procedures and audit controls. Most of the respondents appear to understand that it is critical for HIPAA compliance that workforce access to PHI is monitored with some regularity (i.e., quarterly, monthly, annually). Conducting insufficient monitoring activities can result in significant HIPAA liability for an organization, as large scale instances of improper access that are not promptly identified and mitigated may result in substantial enforcement attention from OCR upon reporting.

26%

DO NOT CONDUCT AUTOMATIC OR MANUAL REVIEWS OF USER ACCESS TO PHI

Q: What type of software tools do you use to assist in identifying and managing privacy-related incidents?

What We Found

A majority of participants indicated that they use the software tool to identify and manage privacy-related incidents, with only **12%** reporting that they use no software at all. Of the respondents who do use software, **60%** utilize an incident reporting tool, **33%** use incident tracking software and **17%** employ an investigation management software. Additionally, **50%** of respondents reported using audit logs and reports from their Electronic Health Record (EHR) system and **31%** utilize a software tool to conduct automated monitoring of users accessing PHI.

What This Suggests

Automated incident response and investigation tools can help an organization examine an incident in a uniform, organized and timely manner and ensure that proper evidence is maintained for OCR to demonstrate that they took adequate steps to safeguard PHI and take corrective action where necessary. Automated software that identifies improper access to ePHI or produces audit logs of EHR access can also be useful in helping an organization quickly identify and investigate inadequate attempts to access ePHI, including those from workforce members or external threats. If the use of software for smaller organizations is cost-prohibitive, it is essential to ensure that any internal (or "homegrown") processes developed for identifying, managing and tracking privacy-related incidents are used uniformly, consistently and that they meet the requirements of the HIPAA privacy, security, and breach notification rules.

Q: Do you have a HIPAA breach response plan that is tested periodically?

What We Found

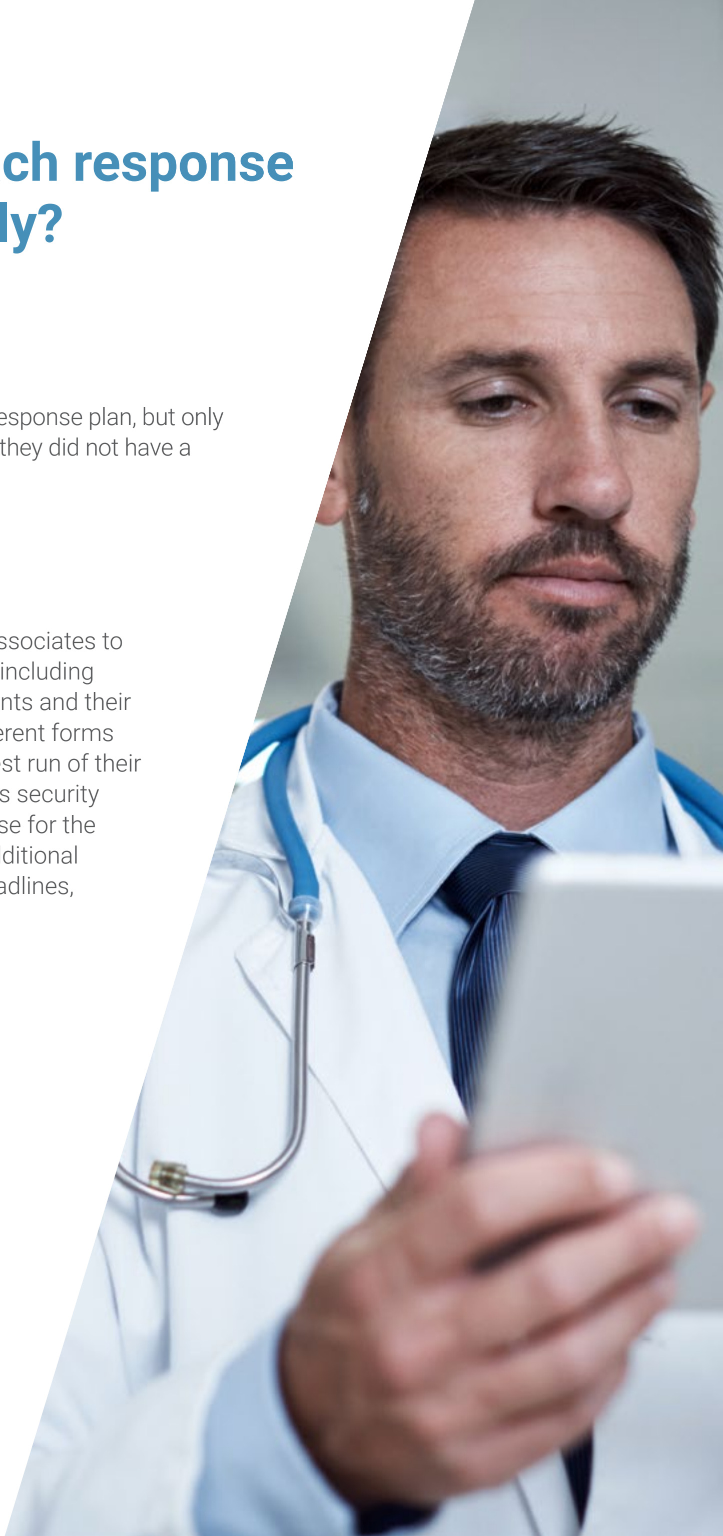
While nearly **73%** of respondents reported having a HIPAA breach response plan, but only **27%** indicated that they periodically test their plan. **13%** stated that they did not have a HIPAA breach response plan.

What This Suggests

The HIPAA Security Rule requires covered entities and business associates to implement policies and procedures to address security incidents, including that they identify, respond, mitigate, and document security incidents and their outcomes. As security incidents and breaches come in many different forms and unfold quickly, organizations will find it helpful to conduct a test run of their plan's process to prepare for the future occurrence of a high-stress security incident. Organizations should avoid testing their security response for the first time during an actual breach incident, as this could lead to additional data loss, potential HIPAA violations such as missed reporting deadlines, and in some cases patient safety issues (i.e., ransomware).

13%

RESPONDENTS STATED THAT THEY DID NOT HAVE A HIPAA BREACH RESPONSE PLAN



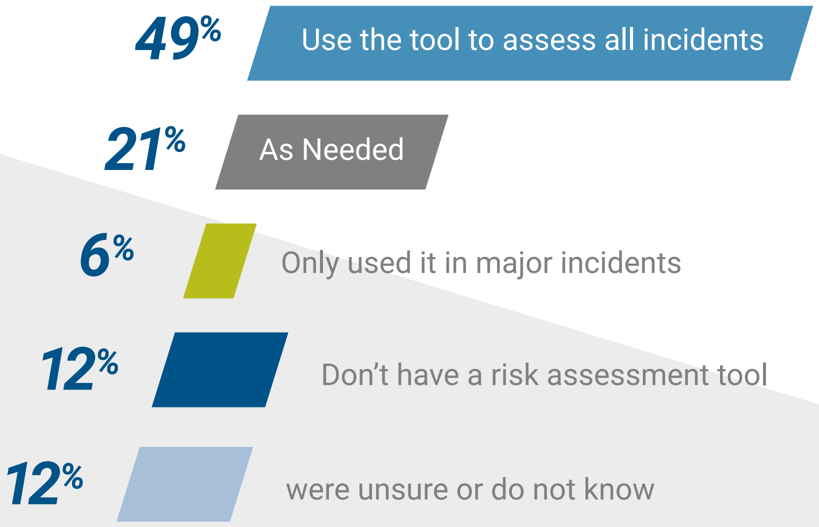
Q: How often do you use a breach risk assessment tool to assess privacy or security incidents?

What We Found

- **76%** of respondents reported using a breach risk assessment tool, with **49%** of that group indicating that their organization uses the tool to assess all privacy and security related incidents
- **21%** reported that their organization uses a risk assessment tool after most events, with **6%** noting that they only use it for significant incidents
- **12%** stated that they did not have a breach risk assessment tool and **12%** were unsure or did not know

What This Suggests

The HIPAA Breach Notification Rules require covered entities and business associates to utilize a breach risk assessment process to demonstrate whether there is a low probability that PHI has been compromised during a potential breach incident. The results indicate that a majority of organizations have taken the time to develop a risk assessment tool and that the device is used to assess potential breach incidents. While employing a breach risk assessment process can be time-consuming and particularly burdensome for some, adequate attention should be spent to ensure that there is a process in place that is scalable and consistently utilized where required by the HIPAA requirements.



Q: Are disciplinary procedures for HIPAA incidents applied consistently throughout the organization (i.e., for people at all levels of the organization)?

What We Found

Just over **52%** of survey participants commented that disciplinary procedures following a HIPAA violation are used always across the organization. Meanwhile, **34%** said that disciplinary actions are only sometimes applied consistently, with **3%** reporting that disciplinary action related to HIPAA issues are never applied uniformly throughout the organization. **11%** did not know or were unsure.

What This Suggests

Ensuring that disciplinary procedures are applied consistently is a constant struggle for organizations of all shapes and sizes. Organizations that can evidence a tone of support for the HIPAA program, from both a Board of Directors and executive-level management level, as well as an active executive level HIPAA or Compliance Committee that discusses HIPAA violations and their correlating corrective action results, may have a better chance of ensuring that disciplinary measures are applied consistently. Once implemented, these factors may also reduce future HIPAA violations and emphasize the importance of a HIPAA compliance culture at an organization.

Enforcement

Q: How prepared is your organization for a HIPAA compliance audit or investigation from OCR?

What We Found

- Over **71%** of respondents indicated that they are mostly or somewhat prepared for an OCR audit or investigation
- **18%** stated that they are very prepared
- **11%** noted that they believed their organization was not well prepared for an OCR audit or investigation

What This Suggests

Answers indicate that most organizations are well prepared for a HIPAA investigation and understand the importance of implementing a response plan, policies and procedures, and other tools to be able to to demonstrate the organization's HIPAA compliance efforts to OCR adequately. With that in mind, it is also essential that organizations assess their preparedness for interactions with OCR on a routine basis, as OCR investigations and audits are exceptionally resourced intensive. Although OCR has remained silent as to whether they will be conducting any further rounds of HIPAA audits, the agency is still consistently investigating HIPAA incidents relating to privacy and security.

Q: What type of encounters has your organization had with OCR in the last 5 years?

What We Found

- **46%** of interviewees reported having no encounters with OCR over the last five years
- **32%** stated that their organization had an encounter with OCR following a breach, with the responses split evenly among offenses involving less than 500 individuals and breaches involving more than 500 individuals
- **22%** reported encounters with OCR related to a privacy investigation
- **9%** reported encounters with OCR related to a security investigation
- **5%** reported being subject to an OCR HIPAA Phase 1 or Phase 2 audit

What This Suggests

For the significant number of respondents who reported having no recent interactions with OCR, this may indicate those organizations have implemented various positive HIPAA practices, such as comprehensive HIPAA training and enterprise-wide use of encryption, resulting in a decrease in breach reporting. However, it should also be noted that organizations that function as business associates were also included in the survey respondent group and that they are less likely to have direct interactions with OCR (as the communication would go through the contracted covered entity), which might have an impact on the survey results here.

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

- **48%** of respondents reported a HIPAA breach to OCR within the last twelve months
- **16%** noted having a reportable breach within the timeframe of one to five years ago
- **3%** indicated they had experienced breaches that were reported to OCR more than five years past
- **24%** of respondents reported that their organization had never experienced an OCR reportable HIPAA breach
- **10%** did not know or were not sure if their organization had reported a breach

What This Suggests

Survey results indicate that organizations reporting breaches to OCR are not alone, as most respondents have reported a HIPAA breach to OCR. Data breaches continue to be a severe issue, particularly in the healthcare industry. It will continue to be essential to report breaches to OCR within the required timeframe and guidelines.

48%

REPORTED A HIPAA BREACH TO OCR IN THE LAST 12 MONTHS

Q: What type of impact has enforcement of state and local laws concerning patient privacy had on your privacy program?

What We Found

Only **3%** of participants reported having an interaction with state and local laws or enforcement entities that have significantly impacted their Privacy Program. About **32%** of respondents indicated that they would be adjusting their Privacy Program planning efforts and training in anticipation of new and revised state and local laws. **64%** reported that they had not felt any impact from state or local privacy laws to date.

What This Suggests

Survey results from this question indicate that most organizations have not felt the impact of state-specific actions and legal mandates related to information privacy. This might suggest that a majority of local authorities have yet to implement their own laws and regulations that interact with the HIPAA privacy, Security and Breach Notification Rules. However, responses also suggest that Privacy Programs may have to significantly adjust their risk and planning processes in the future where states do enact their own privacy laws, for example, following in the footsteps of California with the California Consumer Protection Act. As privacy legislation continues to be a hot topic, both on a national and local level, Privacy Officers must continue to be informed on changes in the regulatory landscape that impact their organization and the patients they serve. It is important to keep in mind that state Attorneys General are also allowed to enforce HIPAA if a breach affects individuals in their state, which has become an increasing trend in the past few years.

Conclusion

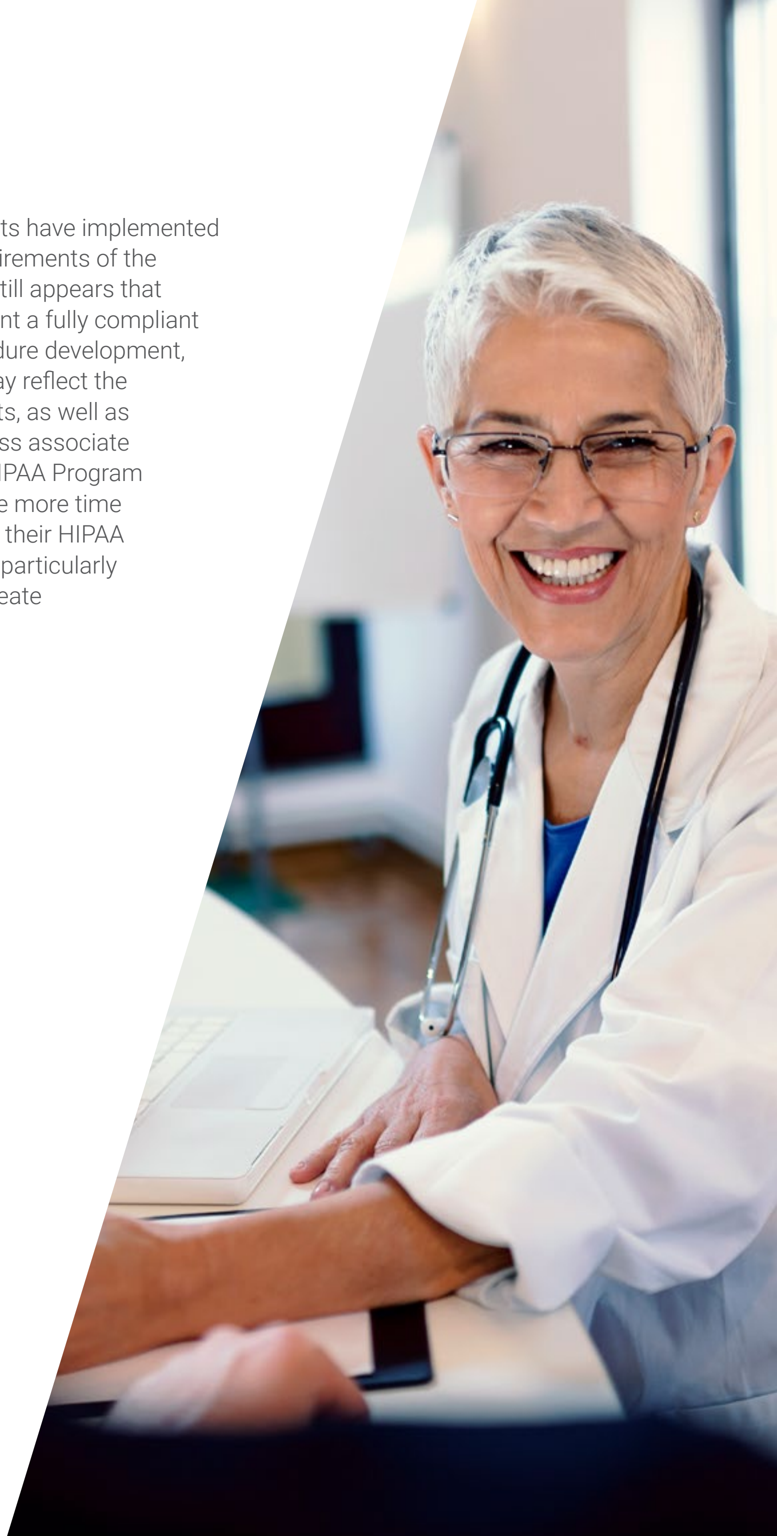
Conclusion

It appears that many organizations have focused significant time, resources and attention to their HIPAA program operations, with many respondents designing their HIPAA program infrastructure similar to what is observed for health care industry compliance programs in terms of reporting and oversight. Evidence strongly suggests that HIPAA has captured the attention of executive leadership and Boards across healthcare organizations, with HIPAA oversight cascading through both levels of many respondent organizations. Organizations should continue to engage their executive and board-level management regarding their HIPAA related risk areas, as it does not appear that HIPAA enforcement will decrease in the coming years, particularly since state Attorneys General are beginning to enforce at a local level.

A positive development is that most organizations have enacted more than 15 HIPAA policies and procedures that are reviewed regularly and almost all organizations maintain compliance with documenting HIPAA training. This suggests that organizations in the healthcare sector have an adequate understanding of the administrative and training expectations outlined in the HIPAA privacy and security rule requirements. Adequate training and communication are further evidenced through the response that most organizations become aware of a HIPAA privacy incident because an employee reports the incident to management or a HIPAA or compliance officer. Having documented policies, procedures and training to address all the HIPAA requirements are particularly important when interacting with OCR, as the department will almost always ask to review these materials when investigating HIPAA related issues.

While answers indicate that most organizations are well prepared for a HIPAA investigation and understand the importance of implementing a response plan, many organizations reported that they do not test their breach response plan. Organizations should avoid testing their security response for the first time during an actual breach incident, as this could lead to additional data loss, potential HIPAA violations such as missed reporting deadlines, and in some cases patient safety issues (i.e., ransomware). With approximately half of the organization respondents reporting a HIPAA breach to OCR within the last twelve months, organizations will find it helpful to conduct a test run of their breach response plan in order to prepare for the eventual occurrence of a high-stress security incident, breach, or both.

Overall, the survey results show that a majority of respondents have implemented solid HIPAA compliance programs that aim to meet the requirements of the Privacy, Security and Breach Notification Rules. However, it still appears that there is a minority of organizations who have yet to implement a fully compliant HIPAA program, with gaps noted related to policy and procedure development, risk analysis, encryption, and security incident plans. This may reflect the different sizes, business lines and types of survey participants, as well as the differences in whether they hold covered entity or business associate designation. For smaller organizations who are initiating a HIPAA Program or struggling to keep up with HIPAA responsibilities, it may be more time and resource-efficient to obtain outside help with portions of their HIPAA operations (i.e., risk analysis, breach response, and training), particularly since forgoing these tasks or performing them poorly can create significant HIPAA compliance and enforcement risk.



About Strategic Management Services

Strategic Management Services, LLC (Strategic Management) was founded over 25 years ago by Richard Kusserow, who had served 11 years as DHHS Inspector General. The firm is a pioneer in healthcare compliance and was the first consulting firm to focus on it – before the government had even issued any formal compliance program guidance documents for the industry. The firm has assisted over 2,000 healthcare organizations with regulatory compliance services, such as the development of compliance program infrastructure, evaluation of compliance programs, standard of conduct development and reviews, compliance training programs, hotline setup, risk assessments, claims data analysis, assistance with the CIA requirements, IRO duties, and litigation support. Strategic Management also operates the Compliance Resource Center (CRC), which provides tools for Compliance Officers, including hotline services, policy development, eLearning, sanction screening, and compliance surveys.

About SAI Global

SAI Global helps organizations proactively manage risk to create trust and achieve business excellence, growth, and sustainability. Our integrated risk management solutions are a combination of leading capabilities, services and advisory offerings that operate across the entire risk lifecycle allowing businesses to focus elsewhere. Together, these tools and knowledge enable clients to develop an integrated view of risk. To see our tools in action, request a free demo.

We have global reach with locations across Europe, the Middle East, Africa, the Americas, Asia and the Pacific.

For more information
visit
www.saiglobal.com/risk

SAI GLOBAL