2020 Report Summary

2020 HIPAA COMPLIANCE BENCHMARK SURVEY

Introduction:

The National HIPAA Compliance Benchmark Survey was conducted for the second year by SAI Global, collaborating with Strategic Management Services, LLC. The goal is to continue understanding how organizations structure, develop, implement, and maintain their HIPAA Privacy Programs and respond to increasing challenges in today's environment.

This report summarizes the findings from the 2020 National HIPAA Compliance Benchmark 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; and
- HIPAA program planning, priorities, and resources.

The HIPAA Survey was conducted among 158 respondents located within the United States and representing various provider types. Nearly half of respondents reported being associated with a hospital or health system, with 16% working in behavioral/ mental health, 15% working in a physician/group practice, 13% working for a health plan/insurance provider, 12% working in skilled nursing/long-term care, and 10% working in a clinic/ambulatory surgery center. The remaining respondents were dispersed over various healthcare provider types or vendors (i.e., home health, laboratory, pharmacy, etc.). Survey results further indicated that most respondents were covered entities, with 78% healthcare providers/covered entities, 10% health plans/covered entities, and 11% business associates.

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

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

HIPAA Compliance Survey Highlights :

HIPAA PROGRAM STRUCTURE – RESPONSIBILITY AND OVERSIGHT

Consistent with last year's survey results, many organizations receive positive support from their executive leadership and Board of Directors (Board) for the HIPAA program. Further, most Privacy Officers report to the Board, an Audit/Compliance Committee of the Board, or an Executive-level Compliance Committee. Also, the majority of respondents have at least one full-time person responsible for HIPAA Privacy. This highlights that most organizations take HIPAA Privacy seriously and keep Executive Management and Board Members informed on HIPAA Privacy issues.

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 have their policies and procedures in a central computerized location. In addition, most participants receive HIPAA compliance training during new employee orientation and annually and maintain adequate information on their HIPAA training.

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

HIPAA INVESTIGATIONS, BREACH MANAGEMENT, AND AUDITS.

Responses indicate that organizations have a wide variety of items and issues on their audit work plans, and they audit most large risk areas related to the HIPAA Privacy Rule. Around one-third of respondents stated they had never conducted an effectiveness evaluation of their HIPAA Privacy Program or did not know if one was ever completed. Slightly over half of the respondents answered that they were "very confident" that their organization was meeting HIPAA Privacy, Security, and Breach notification requirements, which was slightly more than last year's survey results. Half of the respondents reported a breach within the previous year. However, most organizations had no encounters with OCR over the past two years.

HIPAA PROGRAM PLANNING, PRIORITIES, AND RESOURCES.

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

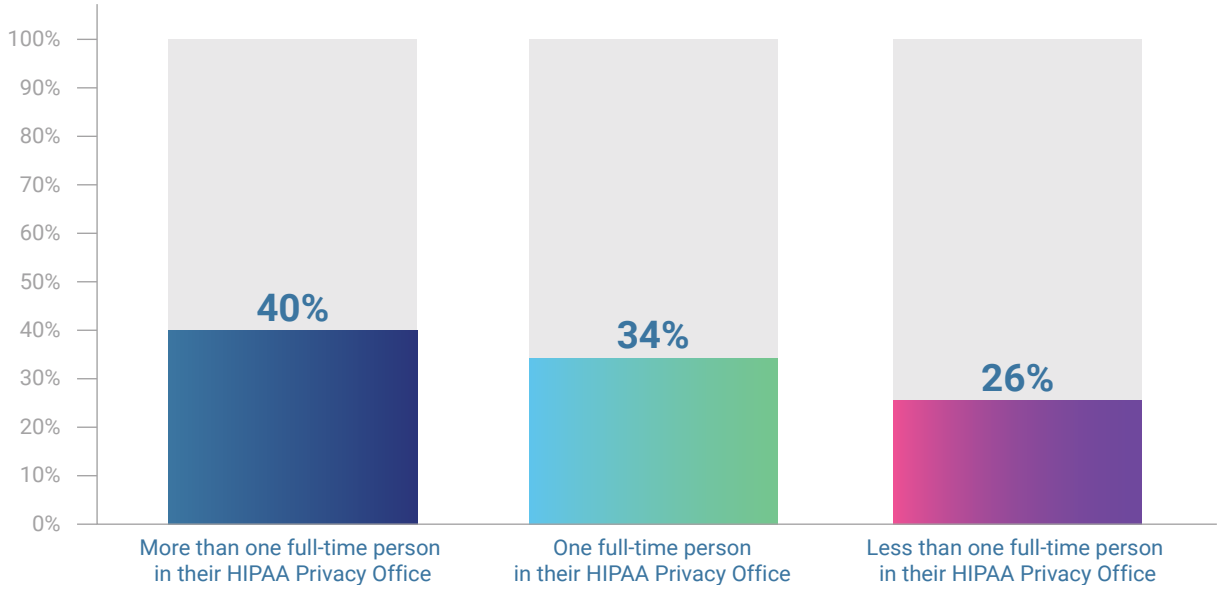
HIPAA Program Structure Responsibility and Oversight

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

WHAT WE FOUND:
40% of survey respondents indicated more than one full-time person in their HIPAA Privacy Office, which is slightly higher than last year's survey results. **34%** of survey respondents stated that there is a full-time person, and **26%** of survey respondents have less than one full-time person.

WHAT THIS SUGGESTS:
That most organizations have at least one full-time person responsible for the HIPAA Program. However, there were still many organizations with less than one person responsible for HIPAA at the organization. Although it may be feasible for smaller organizations that hold a small amount of protected health information (PHI) to have one full-time privacy position or for someone to split duties between Privacy Officer and another function, given the complexity of HIPAA Privacy issues and the regulatory risks, this is not ideal. Often organizations will have their Compliance Officer or Legal Counsel also act as the Privacy Officer. Still, they may not have the bandwidth to deal with HIPAA Privacy and their other job duties fully. Similarly, medium and large organizations often need a HIPAA Privacy team, in addition to a Privacy Officer, to properly deal with all privacy issues.

STAFFING LEVEL FOR THE HIPAA PRIVACY OFFICE

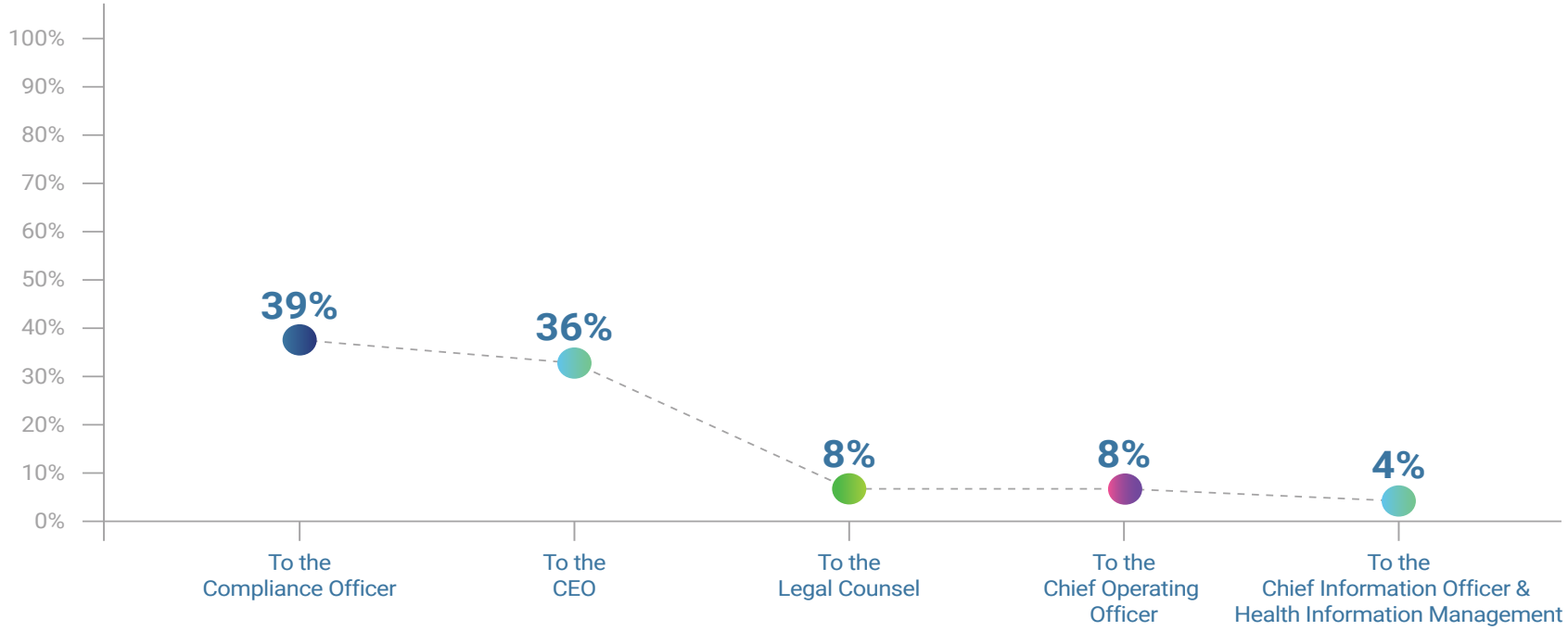


Q: To whom does the Privacy Officer directly report?

WHAT WE FOUND:
Like last year's survey results, about **39%** of respondents stated that the Privacy Officer reports to the Compliance Officer, with **36%** of Privacy Officers reporting directly to the CEO/President of the organization. Around **8%** of respondents reported to Legal Counsel, and **8%** reported to the Chief Operating Officer. A smaller percentage of respondents also indicated that their Privacy Officer reported to the Chief Information Officer and Health Information Management.

WHAT THIS SUGGESTS:
HIPAA Privacy and compliance are largely linked or grouped together for most organizations. It also shows that the Privacy Officer is a high-level officer who reports directly to executive members of the organization's management.

WHO DOES THE PRIVACY OFFICER DIRECTLY REPORT TO?



Q: To what oversight committee does the Privacy Officer provide formal reports?

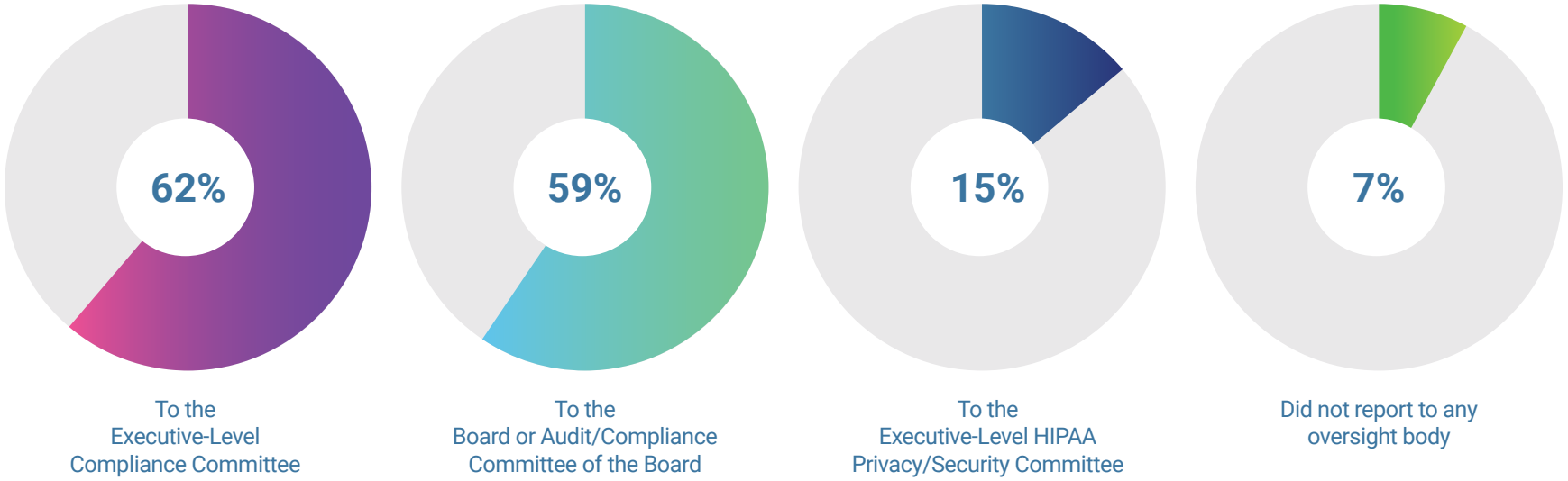
WHAT WE FOUND:

- **62%** of participants indicated that the Privacy Officer provides formal reports to the Executive-Level Compliance Committee.
- **59%** of respondents reported that the Privacy Officer provides formal reports to the Board or Audit/ Compliance Committee of the Board.
- **15%** noted that they provide reports to an Executive-Level HIPAA Privacy/Security Committee.
- **7%** stated that the Privacy Officer did not report to any oversight body.

WHAT THIS SUGGESTS:

A small number of respondents had the Privacy Officer reporting to a specific Executive-Level HIPAA Privacy/Security Committee. Otherwise, most Privacy Officers report to the Board, an Audit/Compliance Committee of the Board, or an Executive-Level Compliance Committee. This suggests that organizations primarily see HIPAA Privacy operations as part of, or related to, compliance. This also indicates that most organizations take HIPAA Privacy seriously and keep Executive Management and Board members informed on HIPAA Privacy issues.

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



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

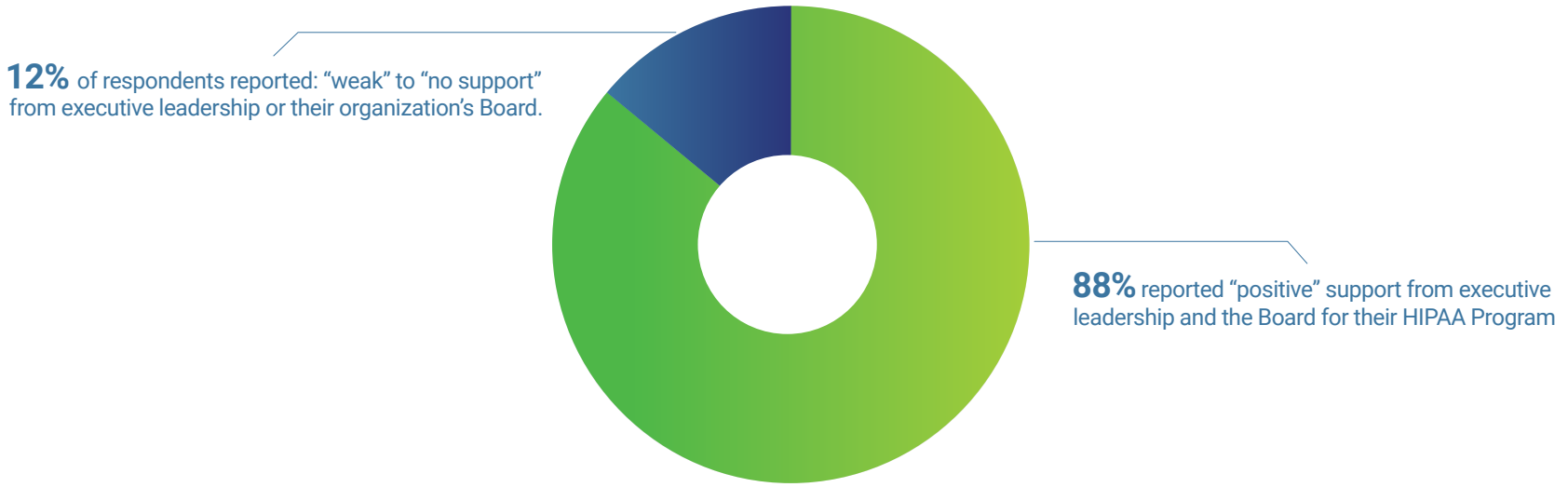
WHAT WE FOUND:

- Approximately **88%** of respondents reported "positive" support from executive leadership and the Board for their HIPAA Program, which is slightly higher than last year's survey results.
- The remaining **12%** of respondents reported: "weak" to "no support" from executive leadership or their organization's Board.

WHAT THIS SUGGESTS:

A significant majority of respondents stated that they receive positive support from executive leadership and Board members for their HIPAA Program. This indicates that most health care organizations and their leadership take HIPAA Privacy very seriously, which is vital because HIPAA Privacy violations can lead to reputational harm and large fines from the Office for Civil Rights (OCR).

STATEMENTS BEST DESCRIBES THE SUPPORT RECEIVED FROM YOUR EXECUTIVE LEADERSHIP AND BOARD OF DIRECTORS?



Talk to us about challenges you are facing, we can help.

HIPAA Program Operations – Policies, Training, and Business Associates

Q: How does your workforce access HIPAA related policies and procedures?

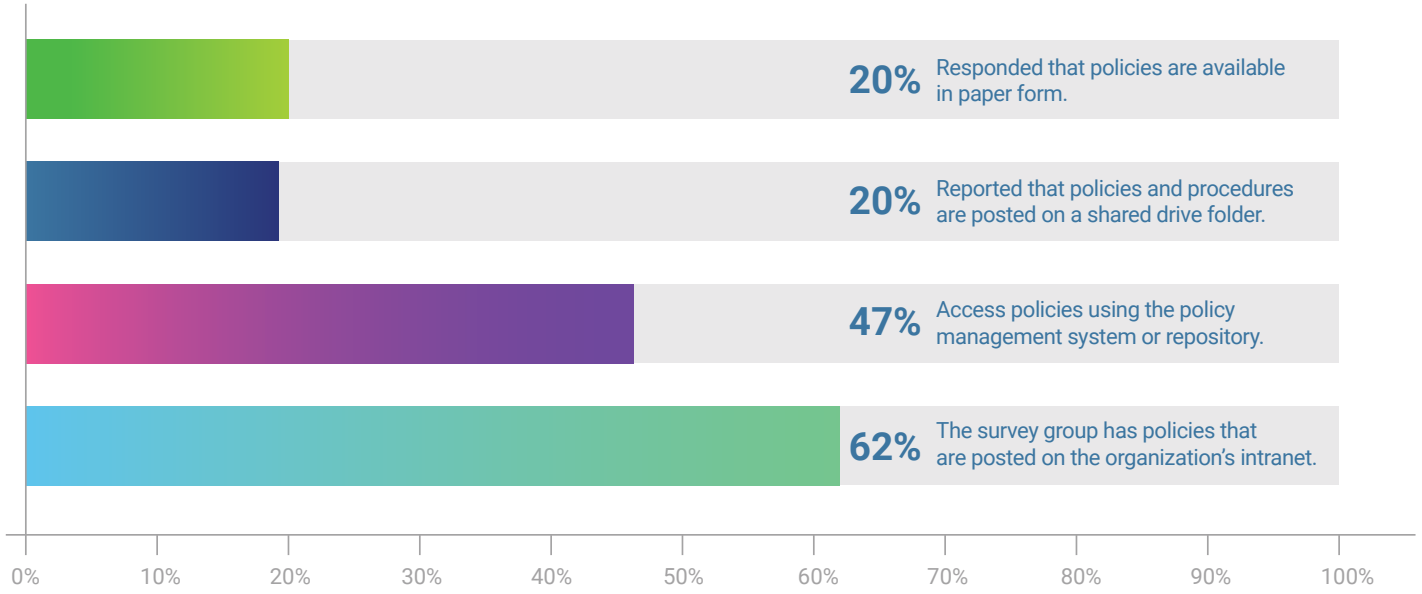
WHAT WE FOUND:

- **62%** of the survey group has policies that are posted on the organization's intranet.
- **47%** of the participants access policies using the policy management system or repository.
- **20%** reported that policies and procedures are posted on a shared drive folder.
- **20%** responded that policies are available in paper form (for example, a binder)

WHAT THIS SUGGESTS:

The majority of respondents provide access to their policies and procedures in a central computerized location. However, 20% of respondents also, or exclusively, have policies in paper form. Maintaining paper form policies can cause version control issues because workforce members may have access to multiple paper versions that get copied or used. It is likely easier for workforce members to access policies from almost any location and at any time if they are in a centralized computerized system.

HOW DOES YOUR WORKFORCE ACCESS HIPAA RELATED POLICIES AND PROCEDURES?

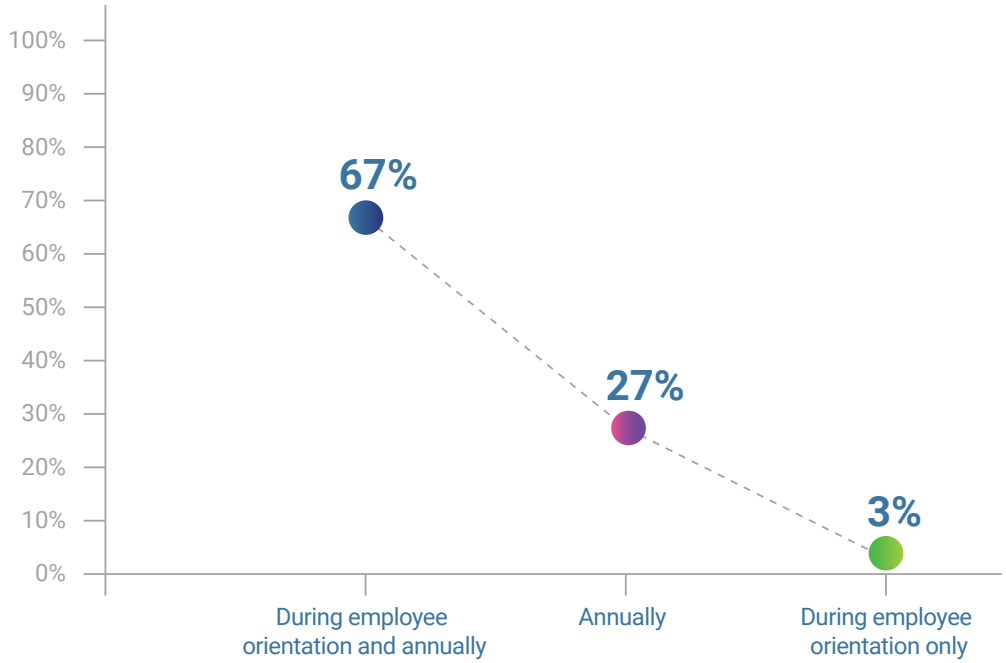


Q: How often do you conduct HIPAA compliance training with your employees?

WHAT WE FOUND:
We found that **67%** of participants receive HIPAA compliance training during new employee orientation and annually. In comparison, **26%** responded that they receive HIPAA compliance training annually. Only about **3%** answered that they receive HIPAA compliance training during new employee orientation only.

WHAT THIS SUGGESTS:
Like last year's survey results, most survey respondents reported that they conduct HIPAA training annually and during employee orientation. It is best practice for organizations to provide workforce members with HIPAA training both at the time of hire and then at least annually. Two-thirds of respondents follow best practices for HIPAA Privacy training. A quarter of respondents only provide HIPAA training annually. Although this is better than giving no training or infrequent training, it is essential to train new staff on HIPAA Privacy and Security, especially if they are new to healthcare and may not have worked with PHI before. Also, suppose someone is hired months before the annual training. In that case, they may have access to PHI long before they are trained on proper procedures and safeguards, leading to many potential HIPAA violations.

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

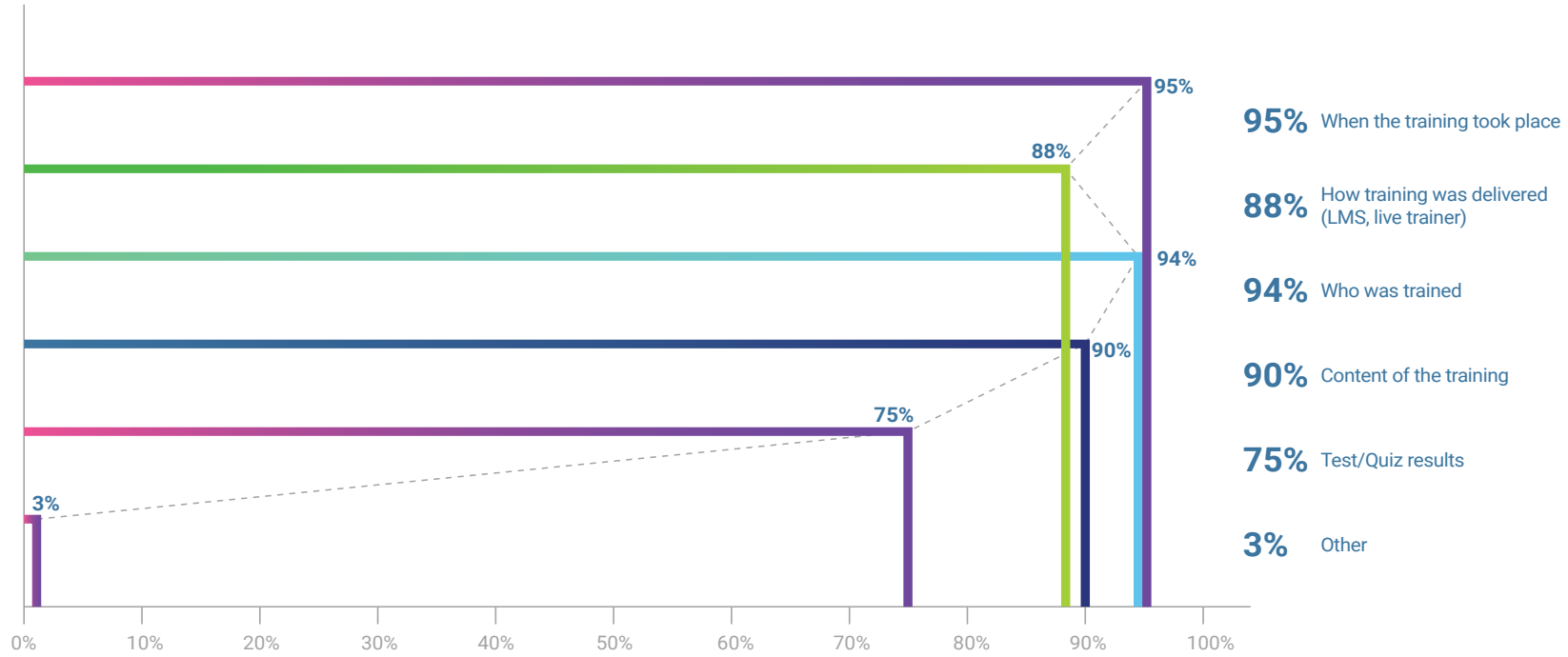


Q: What type of information does your organization maintain for HIPAA Training?

WHAT WE FOUND:
Like last year's survey results, we found that most respondents maintain HIPAA training information on when the training took place, how the training was delivered, who was trained, the training content, and test/quiz results.

WHAT THIS SUGGESTS:
Most respondents keep adequate documentation on HIPAA training, which is important for auditing and record retention purposes. The most important items to track include who has taken the training and when they completed the training. These are most important because that is often what outside auditors and OCR look at to ensure an organization has conducted HIPAA training.

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

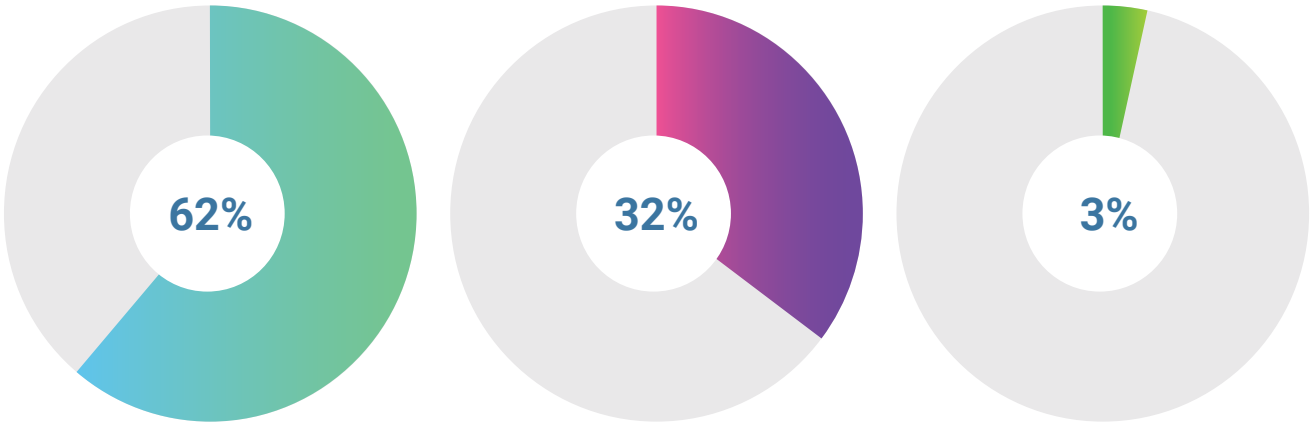


Q: Is HIPAA training mandatory for all employees and business associates (i.e., is disciplinary action taken if the training is not completed)?

WHAT WE FOUND:
62% of respondents stated that HIPAA training is mandatory for all employees, but not business associates. **32%** indicated that HIPAA training is mandatory for all employees and business associates. A minimal number, less than **3%** of participants indicated that HIPAA training is only mandatory for select employees within the organization or that HIPAA training is encouraged, but not required.

WHAT THIS SUGGESTS:
Only one-third of respondents provide HIPAA training to both their employees and business associates. While just under two-thirds of the respondents make HIPAA training mandatory for their employees, they do not require HIPAA training for their business associates. It can be resource-intensive, time-consuming, and logistically challenging to provide HIPAA training for all business associates, especially large organizations with dozens, or even hundreds of business associates. However, organizations should still ensure that business associates receive HIPAA training, which can be achieved by requiring training via mandatory provisions in a Business Associate Agreement (BAA). A small percentage of respondents stated they did not require HIPAA training for employees or all employees, making the organization non-compliant with the HIPAA regulations.

IS HIPAA TRAINING MANDATORY FOR ALL EMPLOYEES AND BUSINESS ASSOCIATES?



Q: Who is responsible for making the final determination of whether a Business Associate Agreement (BAA) is needed with a third-party vendor?

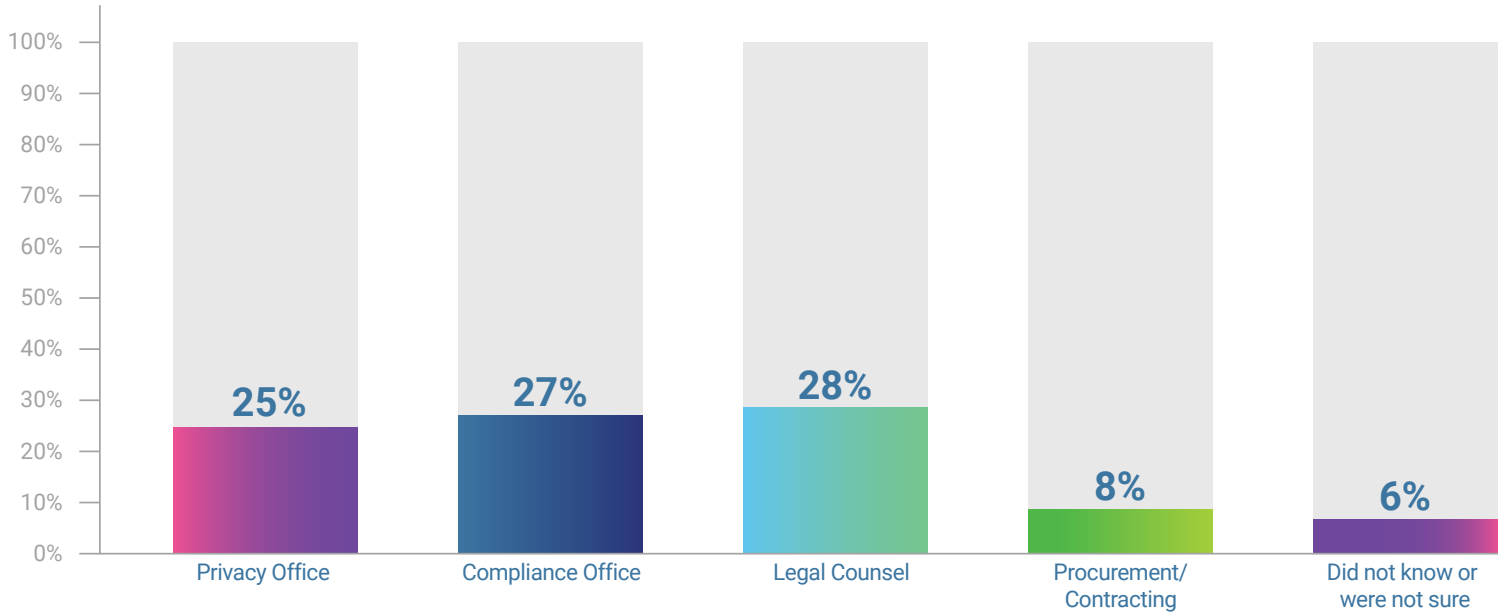
WHAT WE FOUND:

- **25%** indicated that the Privacy Office was responsible for making the final decision regarding BAA's.
- **27%** responded that the Compliance Office was responsible for making the final decision regarding BAA's.
- **28%** noted that Legal Counsel was responsible for making the final decision regarding BAA's.
- Only **8%** of respondents indicated that procurement/ contracting was accountable for making the final decision regarding BAA's, and **6%** did not know or were not sure.

WHAT THIS SUGGESTS:

Responses were split evenly regarding who between the Privacy Office, the Compliance Office, or the Legal Counsel is responsible for making final decisions on whether a BAA is needed. A small group of about 8% of respondent organizations has their procurement/contracting department decide on BAAs. Although this is not uncommon, the procurement team needs to have a thorough understanding of the HIPAA requirements to ensure that BAAs are in place with the appropriate vendors.

WHO DETERMINES THE NEED FOR A BAA WITH A THIRD-PARTY VENDOR?

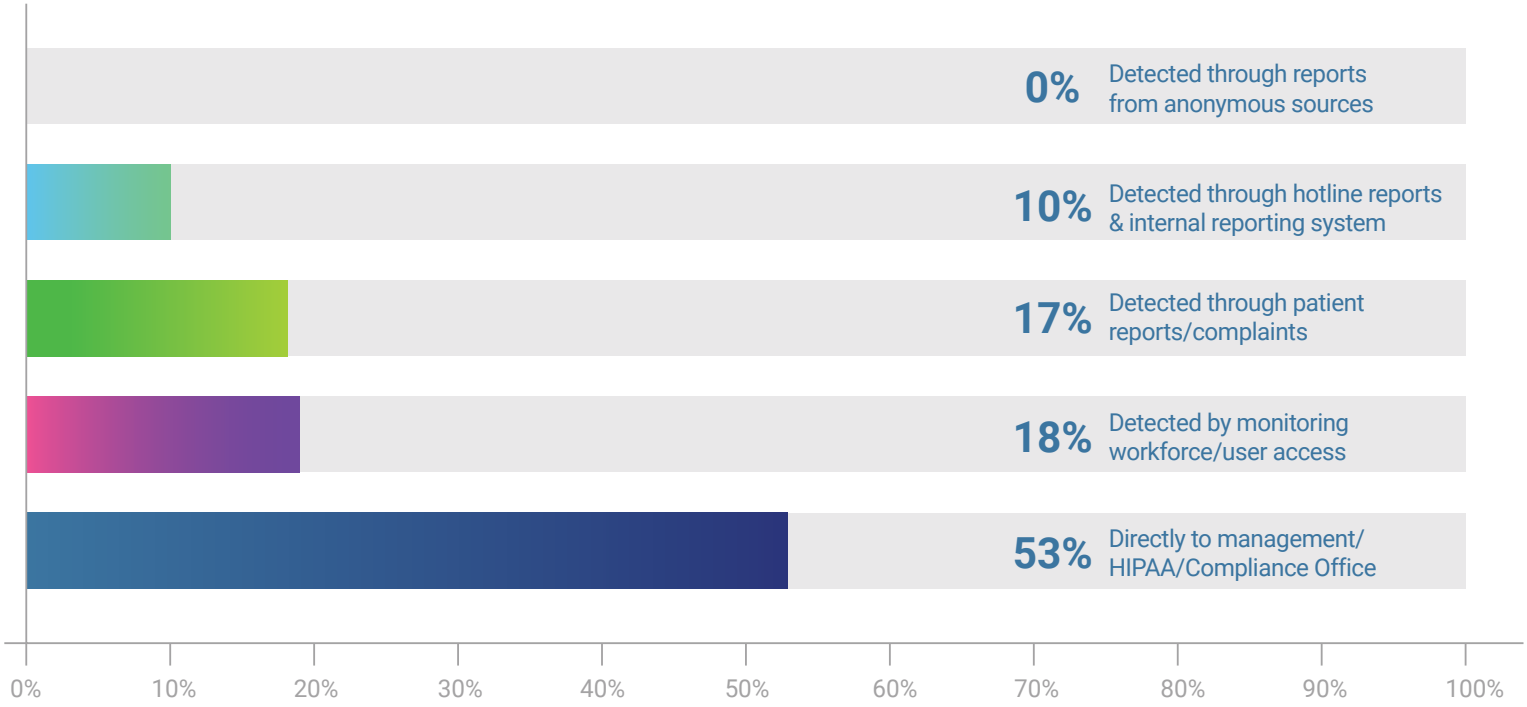


Q: How are most HIPAA Privacy incidents detected at your organization?

WHAT WE FOUND:
53% of respondents indicated that employees report directly to management/HIPAA/Compliance Office. Around **18%** responded that privacy incidents are detected by monitoring workforce/user access, and **17%** responded that privacy incidents are detected through reports from patients/health plan members and complaints. A small percentage of participants also indicated that privacy incidents are detected through hotline reports and internal reporting system reports. Notably, no respondents indicated that privacy incidents were detected through reports from anonymous sources or outside government agencies.

WHAT THIS SUGGESTS:
The results indicate a positive trend that many organizations have an embedded culture of compliance and that workforce members feel comfortable reporting issues internally. Detecting HIPAA Privacy incidents through monitoring workforce/user access is another proactive way to identify potential offenses. However, having HIPAA incidents reported solely through patient/health plan member reports and complaints is not ideal. This could be an indication that proper controls and monitoring are not in place, and it might result in significant delays for organizational responses, disclosure of breaches, and issue mitigation.

HOW ARE MOST HIPAA PRIVACY INCIDENTS DETECTED AT YOUR ORGANIZATION?



Talk to us about challenges you are facing, we can help.

HIPPA Investigations, Breach Management, and Audits

2020 HIPAA Compliance Benchmark Survey

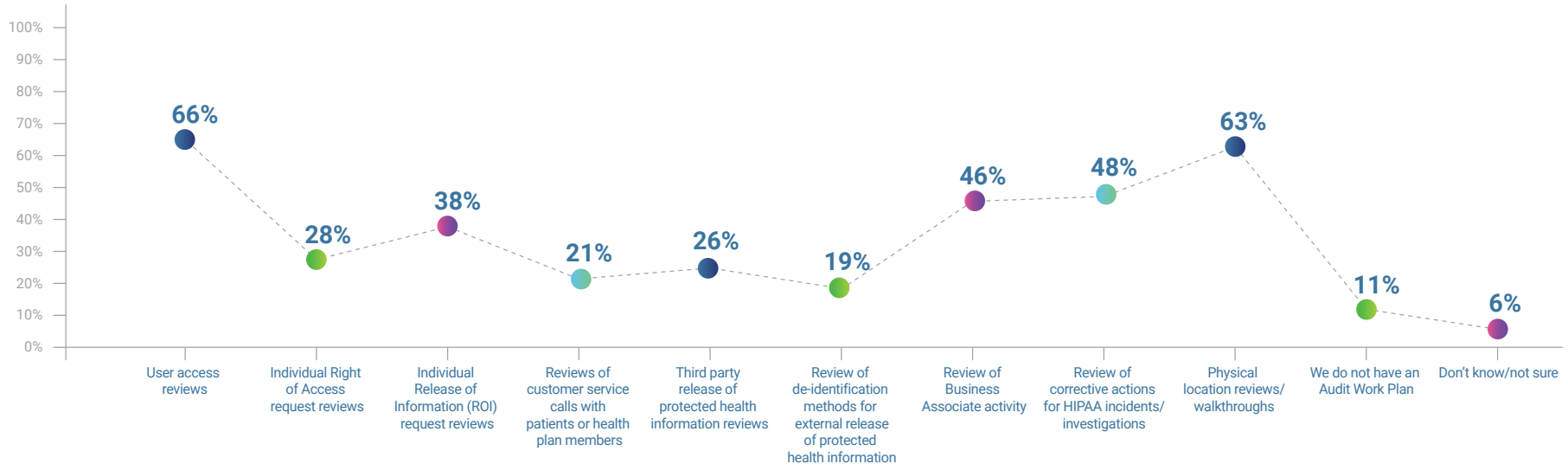
HIPPA Investigations, Breach Management, and Audits

Q: Which of the following items are currently on your HIPAA/Compliance Audit Work Plan?

WHAT WE FOUND:
There was a wide range of participants' responses regarding items found on their HIPAA/Compliance Audit Work Plans. Over **60%** of respondents reported physical location reviews/ walkthroughs were included in their audit work plan. Additionally, over **60%** of respondents reported conducting user access reviews of electronic health records (EHRs) and other PHI applications. However, almost **12%** of respondents stated they do not have an audit work plan.

WHAT THIS SUGGESTS:
Answers indicate that organizations have a wide variety of items and issues on their audit work plans, and audit most high-risk areas related to the HIPAA Privacy Rule. Best practices suggest that organizations should have an audit work plan. Small organizations that may not have many resources to commit to a formal audit process should still identify a handful of risk areas and conduct audits in those areas over twelve months.

ITEMS CURRENTLY ON HIPAA/COMPLIANCE AUDIT WORK PLAN

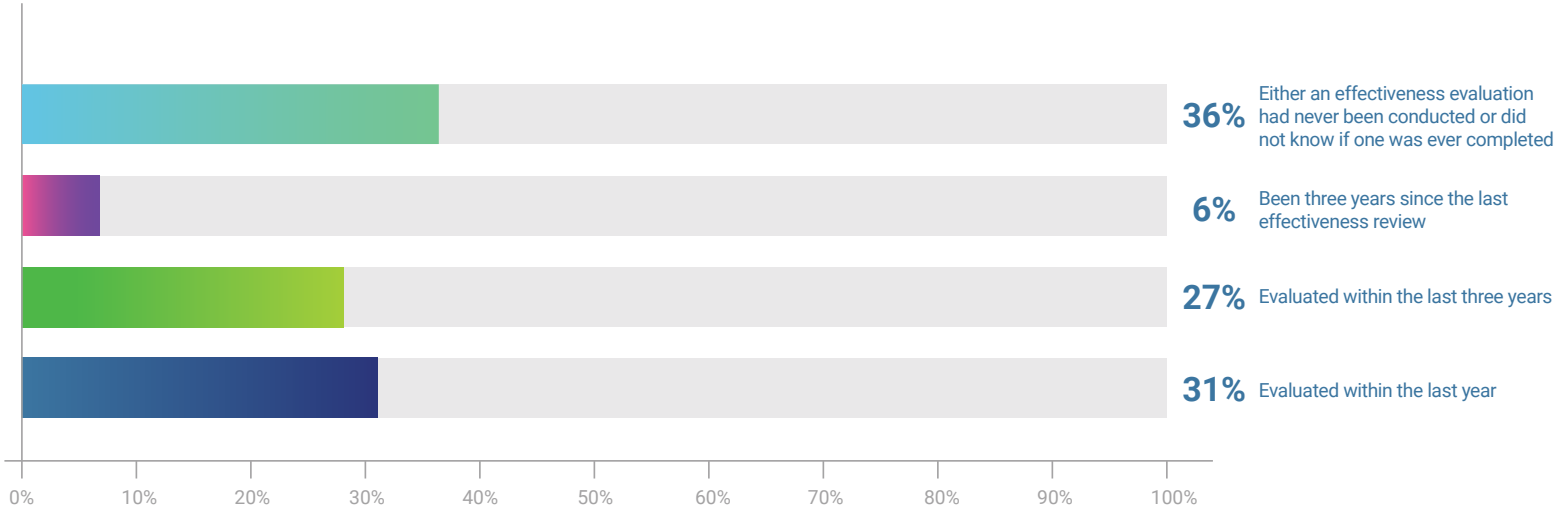


Q: When was the last time, the effectiveness of your HIPAA Privacy Program was independently evaluated?

WHAT WE FOUND:
31% of respondents commented that an independent party evaluated the effectiveness of their organization's HIPAA Privacy Program within the last year. This is a slightly higher response than last year's survey results, which indicated that **23%** had an evaluation within the previous year. **27%** of respondents stated that the evaluation occurred within the last three years. **6%** indicated that it had been at previous three years since their last effectiveness review. The other 36% of respondents stated that either an effectiveness evaluation of their HIPAA Privacy Program had never been conducted or they did not know if one was ever completed.

WHAT THIS SUGGESTS:
The one-third of respondents who conducted an independent review within the last year follows a best practice for measuring compliance with the HIPAA Privacy Rule. Another quarter of respondents had an independent review within the previous three years, which is still an adequate period to conduct its internal monitoring and program reviews. However, the remainder of respondents stated their organization had not had an independent review of their HIPAA Privacy Program or the respondent was unsure if an independent review had been done. Although the HIPAA Privacy Rule does not require covered entities to conduct independent reviews, it is an important tool for detecting compliance failures with other HIPAA Privacy Rule requirements. Outside independent reviews can also be helpful tools if an organization is going through a transition that impacts HIPAA Privacy, such as adopting a new EHR, expanding into different states, or merging with another covered entity.

EFFECTIVENESS OF HIPAA PRIVACY PROGRAM INDEPENDENTLY EVALUATED

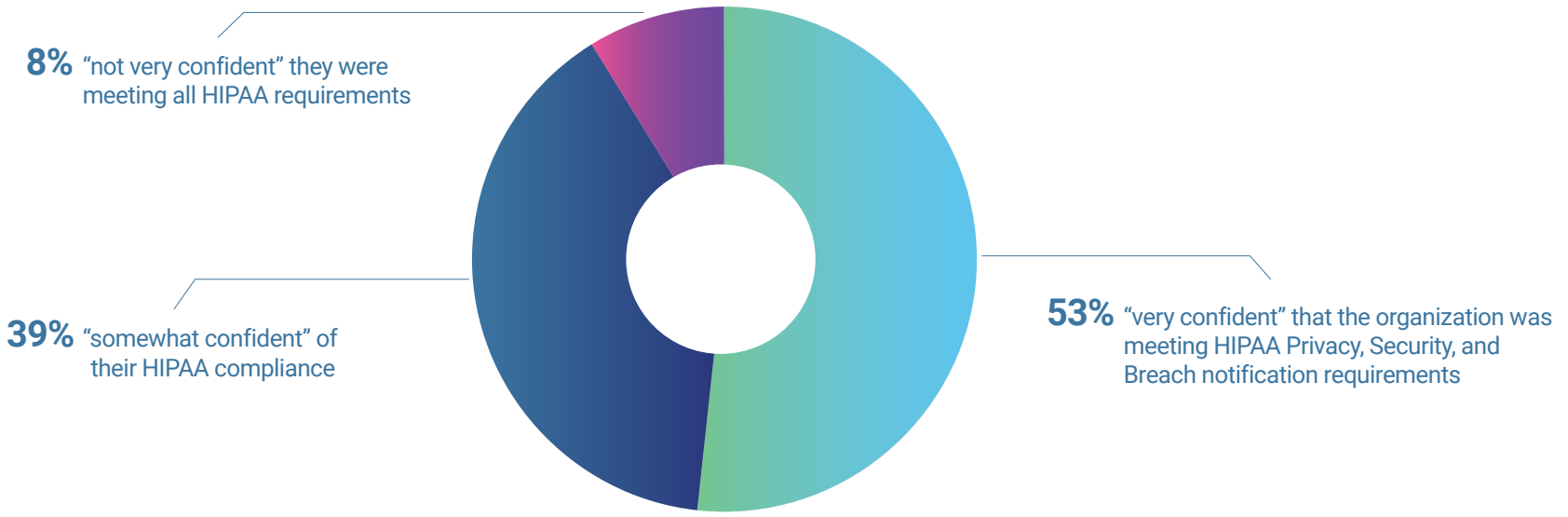


Q: How confident are you that your organization is meeting the HIPAA Privacy, Security, and Breach Notification Rule Requirements?

WHAT WE FOUND:
Approximately **53%** of respondents answered that they were "very confident" that their organization was meeting HIPAA Privacy, Security, and Breach notification requirements. **39%** of respondents indicated they were "somewhat confident" of their HIPAA compliance, with **8%** noting that they were "not very confident" they were meeting all HIPAA requirements.

WHAT THIS SUGGESTS:
Last year's survey results indicated that 39% of respondents were "very confident" that their organization was meeting the HIPAA Privacy, Security, and Breach notification requirements. In comparison, this year's survey results indicate that more respondents are "very confident" that their organization meets the HIPAA regulations' needs, suggesting they likely have enough resources, safeguards, and leadership support when it comes to HIPAA privacy and security concerns. To help increase their confidence in meeting the HIPAA privacy requirements, organizations can identify what gaps they have in their program through an internal risk assessment or audit and discuss these areas of risk with other HIPAA Privacy/Compliance Committee members and other members of executive management.

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



Q: When was the last time your organization had a HIPAA Breach that has been reported to the Office for Civil Rights?

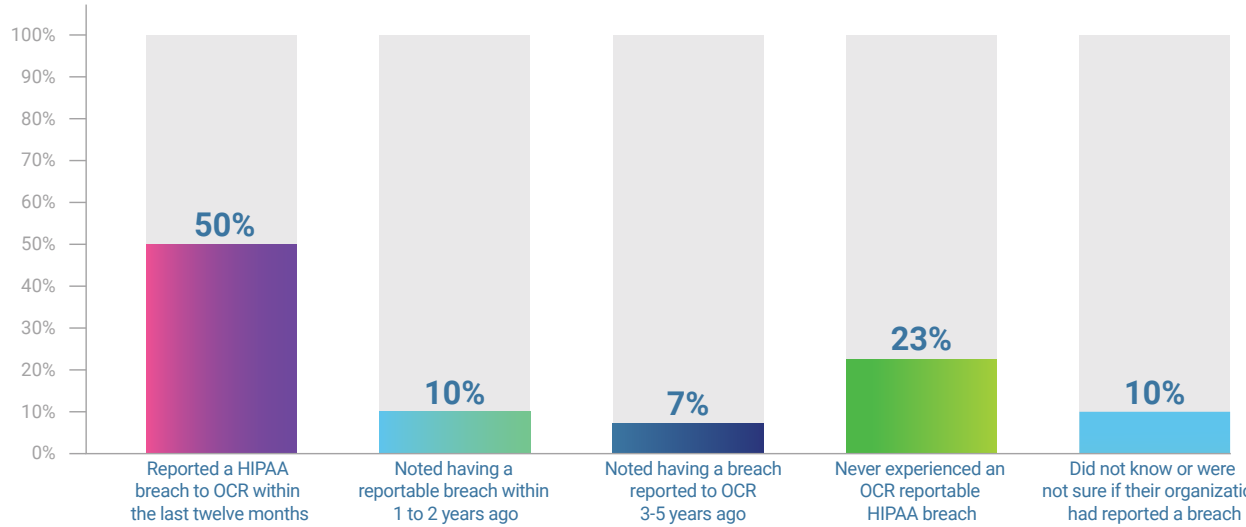
WHAT WE FOUND:

- **50%** of respondents reported a HIPAA breach to OCR within the last twelve months.
- **10%** noted having a reportable breach within one to two years ago.
- **7%** noted having a breach reported to OCR three to five years ago.
- **23%** 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:

Half of the respondents reported a breach within the last year, which is likely due to the consistent and increasing sophisticated work of cyber criminals through phishing attacks and ransomware. During the COVID-19 public health emergency (PHE), there has been an uptick in cyber-attacks on health care organizations using COVID-19 related phishing attacks. Organizations should review the causes of their reportable breaches to identify any gaps and possible additional safeguards that can be put in place to prevent future violations. Over one-third of respondents stated their organizations have either never had a reportable breach or did not know if their organization had a reportable breach. These organizations should review how they detect and report breaches to ensure that their processes are effectively identifying potential breaches. It is important to remember that even breaches that impact less than 500 individuals must be reported to OCR at the end of a calendar year.

HIPAA BREACH REPORTED TO THE OFFICE FOR CIVIL RIGHTS

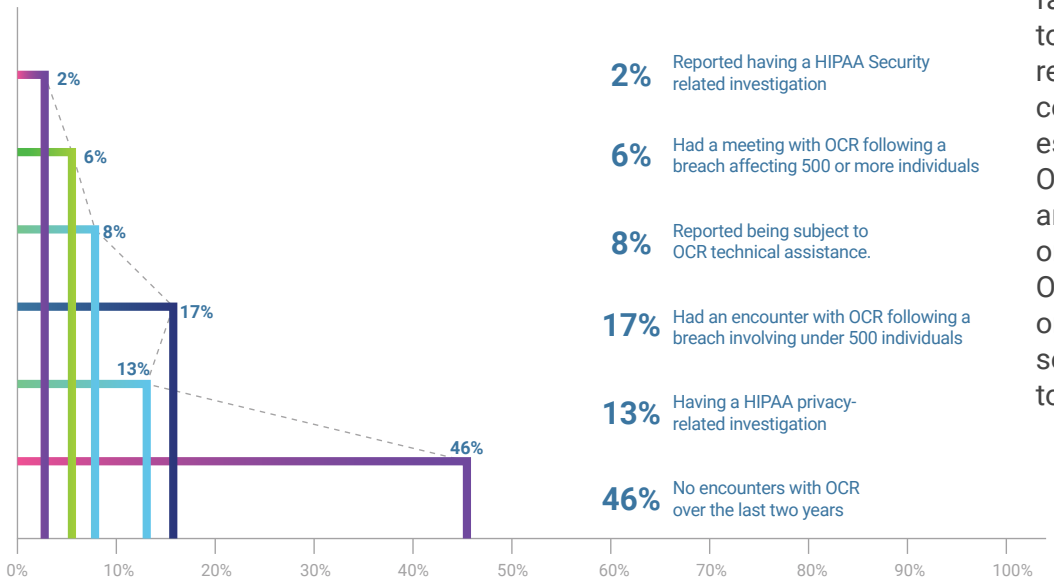


Q: What type of encounters has your organization had with OCR in the last two years?

WHAT WE FOUND:

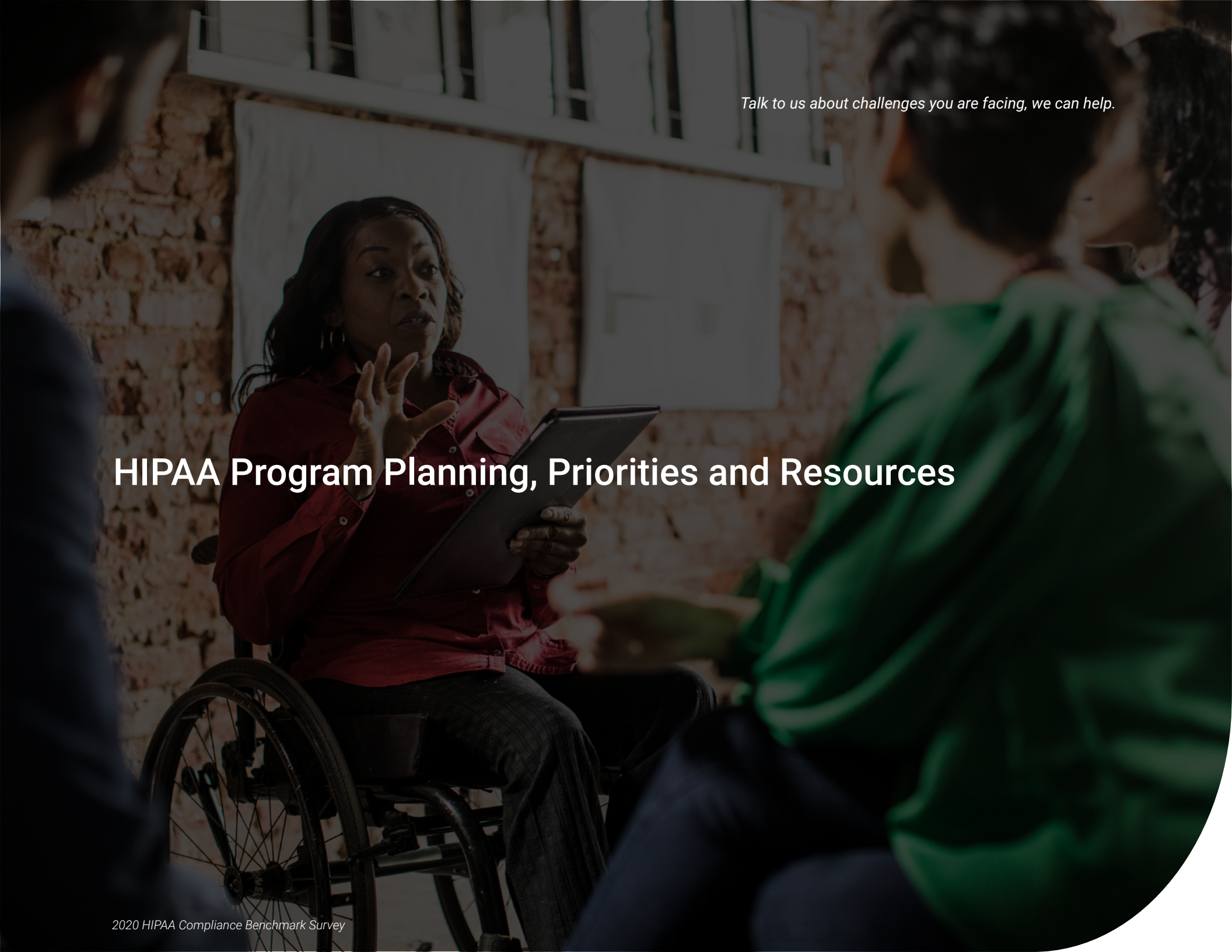
- **46%** of interviewees reported having no encounters with OCR over the last five years.
- **13%** reported having a HIPAA privacy-related investigation, settlement, or corrective action plan.
- **12%** stated that their organization had an encounter with OCR following a breach involving under 500 individuals.
- **8%** reported being subject to OCR technical assistance.
- **6%** said that their organization had a meeting with OCR following a breach affecting 500 or more individuals.
- **2%** reported having a HIPAA Security related investigation, settlement, or corrective action plan.

ENCOUNTERS WITH OCR IN THE LAST TWO YEARS



WHAT THIS SUGGESTS:

Most organizations have had no encounters with OCR over the past two years. For those organizations that did have encounters with OCR, the encounters primarily led to an investigation or technical assistance, but no settlement or corrective action. Only about 15 percent of respondents had encounters that led to disciplinary action or a settlement. This suggests that even if an organization suffers a breach or violates the HIPAA Privacy Rule, the issue can be resolved without significant fines or a corrective action plan if the organization is proactive in its reporting and corrective actions and works with OCR. However, a review of OCR enforcement history shows that certain HIPAA violations are more likely to result in a corrective action plan and a settlement, including failure to fulfill an individual's request for access to their PHI, failure of the organization to conduct regular risk assessments, and failure to implement certain technical safeguards such as encryption, especially after a breach. Since September 2019, OCR has been mainly focused on the right of access, announcing an enforcement initiative focused on the right. Since the beginning of the initiative, OCR has entered corrective action plans with nine organizations. Since June 2020, OCR has settled seven right of access cases, highlighting that it is a top enforcement priority.



Talk to us about challenges you are facing, we can help.

HIPAA Program Planning, Priorities and Resources

Q: Please select the top 3 priorities to be addressed by your HIPAA Compliance Program in the next 12 months

WHAT WE FOUND:
We found that the highest percentage of participants selected the following as one of their top three priorities:

- Incident response and reporting (e.g., conducting investigations and corrective actions).
- Reducing inappropriate/inadvertent disclosures of PHI by workforce.
- Monitoring Business Associate Agreement and activity.
- Breach Notification Management (e.g., conducting breach risk assessments and notifying individuals, OCR, State Agencies, etc. within required timeframes).
- Monitoring inappropriate access to PHI/snooping by workforce.

WHAT THIS SUGGESTS:
All the listed items are understandably ranked as top priorities since issues such as inappropriate disclosure or business associate agreement problems can lead to violations of the HIPAA Privacy Rule. Compared to last year's survey results, breach notification management and incident response and reporting were listed as top priorities in this year's survey rather than reviewing and updating HIPAA compliance policies and procedures and developing/delivering HIPAA training. Investigations can often be time and resource-intensive, so it is essential to have investigation procedures and run through them when there is no incident. Delayed remediation of incidents can also lead to larger fines for an organization since most HIPAA violations are based on a per-incident basis (i.e., each person affected each day).

TOP 3 PRIORITIES TO BE ADDRESSED BY YOUR HIPAA COMPLIANCE PROGRAM

First Priority:

1. Incident Response and Reporting
2. Reducing Inappropriate/ Inadvertent Disclosures of PHI by Workforce
3. Monitoring Business Associate Agreement and Activity

Second Priority:

1. Incident Response and Reporting
2. Breach Notification Management
3. Reducing Inappropriate/ Inadvertent Disclosures of PHI by Workforce

Third Priority:

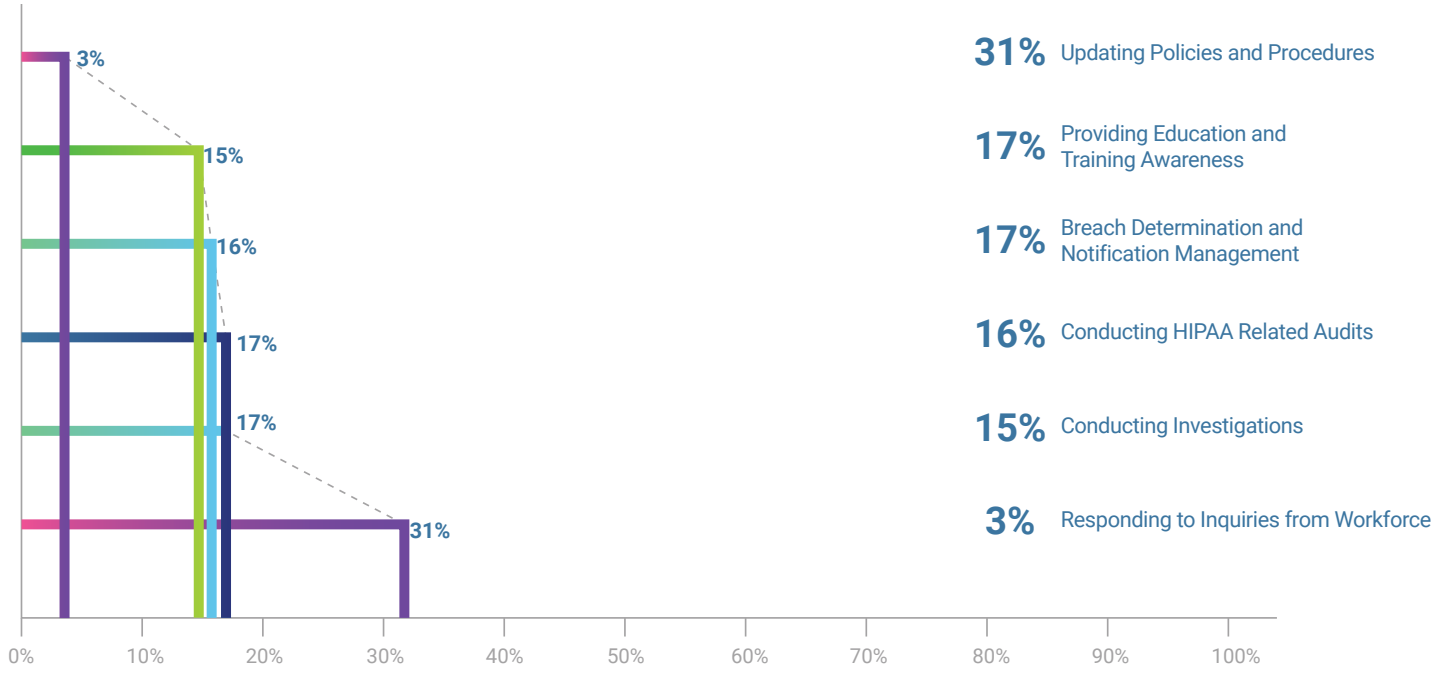
1. Reducing Inappropriate/ Inadvertent Disclosures of PHI by Workforce
2. Monitoring inappropriate access to PHI/Snooping
3. Monitoring Business Associate Agreement

Q: Which of the following HIPAA responsibilities takes the most planning and resources for your organization?

WHAT WE FOUND:
The highest percentage of participants: **31%** responded that updating policies and procedures takes the most planning and resources. Around **15% - 17%** of participants stated the following responsibilities take the most planning and resources: Providing education and training awareness; Conducting investigations; Breach determination and notification management and Conducting HIPAA related audits. Only **3%** of respondents indicated that responding to inquiries from the workforce takes the most planning and resources.

WHAT THIS SUGGESTS:
The creation of policies and procedures can certainly be a time and resource-intensive process in the beginning, but if organizations use a standardized process and timeline for updating policies and procedures, it should take significantly less time in future years. Policy updates can be time-consuming and complicated more because of the frequent changes in technology and internal processes related to patient care or business decisions, rather than changes in the relevant laws or regulations. All the other respondents were split evenly between spending time and resources on training, investigations, breach notification, and audits, which are all time consuming and resource-intensive tasks when done correctly.

WHICH HIPAA RESPONSIBILITIES TAKES THE MOST PLANNING AND RESOURCES



Q: What type of impact has the COVID-19 public health emergency had on your HIPAA Program?

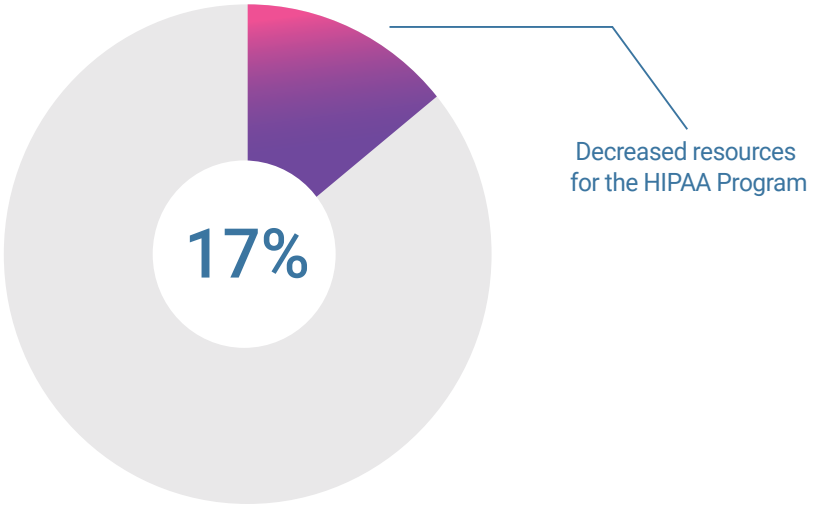
WHAT WE FOUND:

- **36%** of respondents stated that COVID-19 had not impacted their HIPAA Program.
- **23%** of respondents noted that COVID-19 increased HIPAA related training and education, and that 23% of respondents had an increase in HIPAA related research inquiries.
- **17%** of respondents indicated that COVID-19 decreased resources for the HIPAA Program, and 17% indicated that COVID-19 led to the development of additional HIPAA policies.
- **15%** responded that there was an increase in breach activity.
- **12%** noted increased responsibilities and resources needed for public health reporting.
- **5%** stated that COVID-19 increased resources for the HIPAA Program.

WHAT THIS SUGGESTS:

Despite the increase in HIPAA related responsibilities, only a small percentage of respondents reported an increase in resources for the HIPAA Program, where a slightly higher percentage reported a decrease in resources. Although unsurprisingly, resources may have gone to clinical needs, and OCR has eased some regulatory restrictions during the PHE, organizations must continue to follow the HIPAA Privacy rule and incorporate HIPAA into topics developed since COVID-19, such as telemedicine.

TYPE OF IMPACT HAS THE COVID-19 PUBLIC HEALTH EMERGENCY HAD ON YOUR HIPAA PROGRAM?

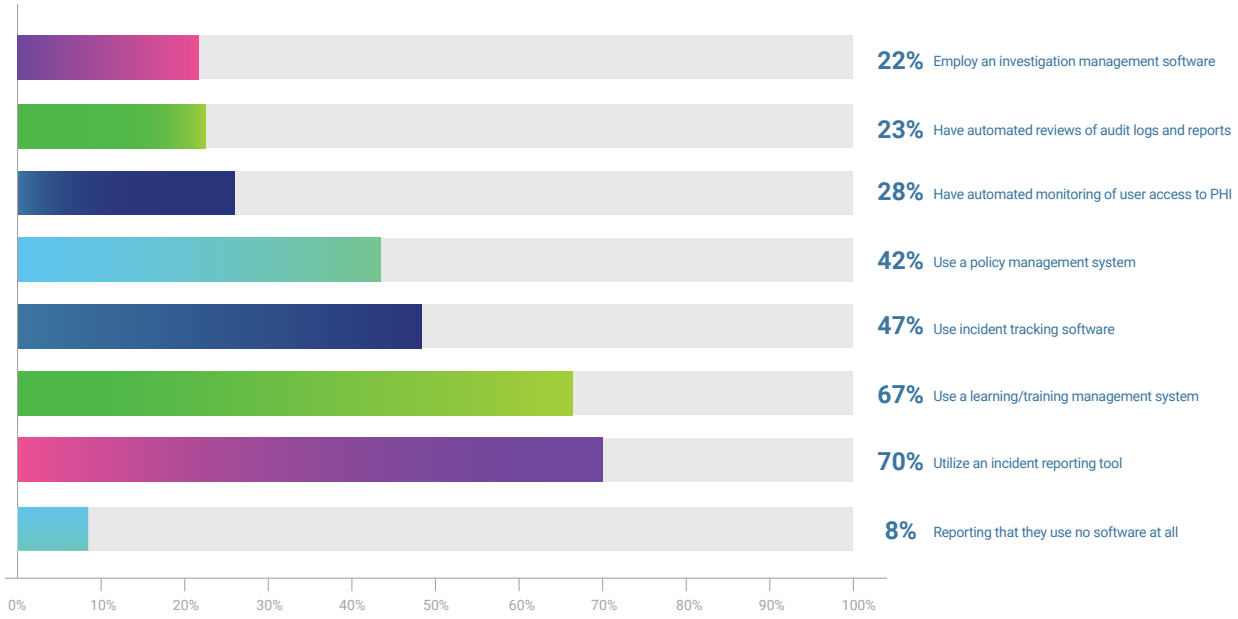


Q: What type of software or hardware tools do you use to carry out the Privacy Program operations at your organization?

WHAT WE FOUND:
Most participants indicated that they use some type of software tool to carry out Privacy Program operations at their organization, with only **8%** reporting that they use no software at all. Of the respondents who use software, **70%** utilize an incident reporting tool, **67%** use a learning/training management system, **47%** use incident tracking software, and **42%** use a policy management system. Additionally, **28%** have automated monitoring of user access to PHI, **23%** have automated reviews of audit logs and reports from the EHR system, and **22%** employ an investigation management software.

WHAT THIS SUGGESTS:
Although a small number of organizations responded that they do not use software for their Privacy Program operations, most respondents use software for one or multiple functions of their program. Many software programs are helpful for tracking investigations, training, and policies. They can make for easy producing documentation if OCR or an outside auditor wants to see how an organization is complying with the HIPAA Privacy Rule. Even smaller organizations that may not have the budget or resources to buy a software for tracking should use something like a spreadsheet to track audits, policy development and changes, breaches, and training because documentation is critical to showing the organization has an effective HIPAA program.

SOFTWARE OR HARDWARE TOOLS DO YOU USE TO CARRY OUT THE PRIVACY PROGRAM OPERATIONS

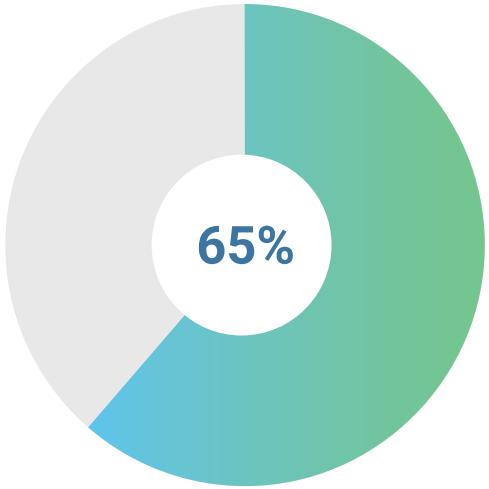


Q: Does your organization use on-call consultant/vendor services to assist with HIPAA Privacy and Security functions (e.g., training, investigation breaches, assisting with evaluations, policies and procedures, risk analysis, etc)?

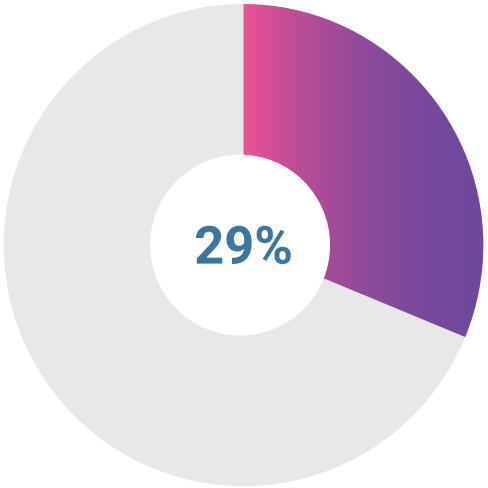
WHAT WE FOUND:
Nearly **65%** of our surveyed group stated that they do not use on-call consultant/vendor services compared to approximately **29%** of respondents who employ contractors to assist with HIPAA Program functions.

WHAT THIS SUGGESTS:
The fact that the majority of organizations do not use on-call consultants or vendors for their HIPAA Privacy Programs could positively suggest that most organizations have the budget, personnel, and expertise in-house to have a well-functioning HIPAA Privacy Program. Even for organizations that can perform many HIPAA Privacy functions in-house, having an on-call consultant can help to respond to independent audits or conduct research on more complicated regulatory questions, such as those surrounding de-identification of PHI or use of PHI in research studies.

USE OF ON-CALL CONSULTANT/VENDOR SERVICES TO ASSIST WITH HIPAA PRIVACY AND SECURITY FUNCTIONS



Do not use on-call consultant/vendor services



Employ contractors to assist with HIPAA Program functions

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

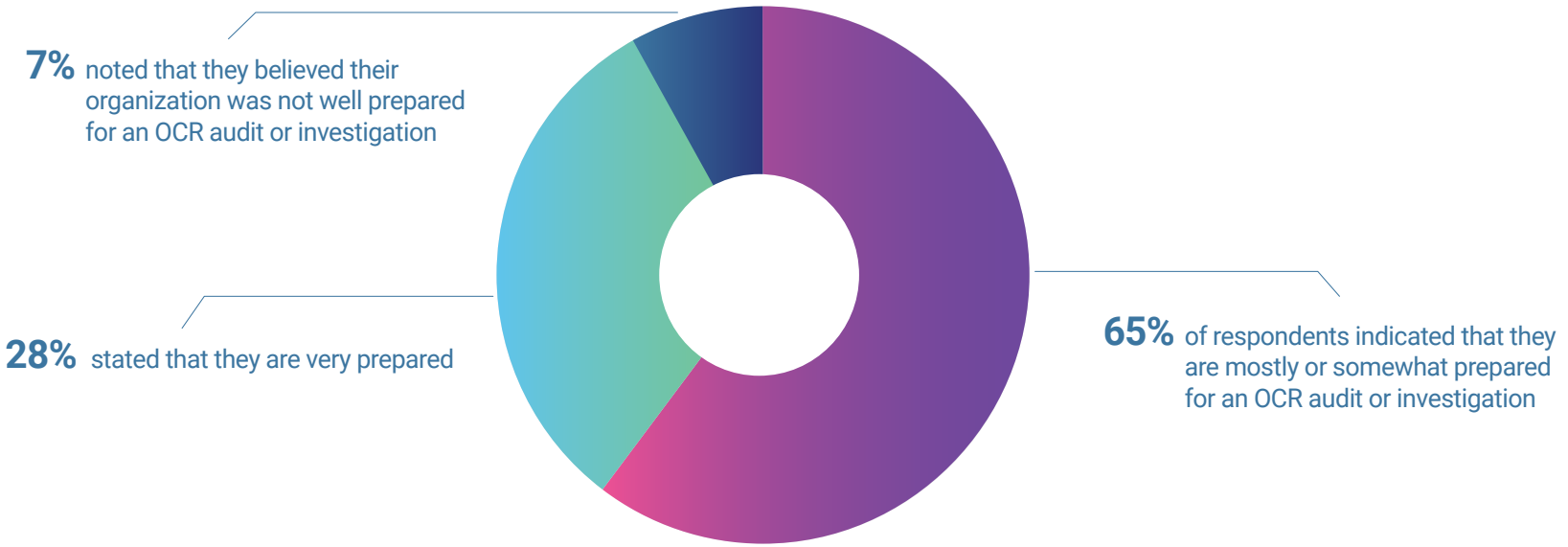
WHAT WE FOUND:

- Approximately **65%** of respondents indicated that they are mostly or somewhat prepared for an OCR audit or investigation.
- **28%** stated that they are very prepared.
- **7%** 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 prepared for an OCR audit or investigation. All organizations must assess their preparedness for an audit or investigation regularly. Because OCR takes the stance that if it is not documented, it did not happen, organizations should ensure they have documentation related to key HIPAA Privacy and Security requirements, such as training, policies and procedures, risk assessments, business associate agreements, the fulfillment of requests for access to PHI, and breach reporting.

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



Conclusion

Overall, this year's survey responses are generally consistent with last year's HIPAA Compliance survey results. It appears that many organizations have HIPAA Privacy Programs that are supported by organizational leadership, with most Privacy Officers reporting to the Compliance Officer or CEO and providing formal reports to the Executive Level Compliance Committee, Board of Directors, or the Audit Compliance Committee of the Board. Engagement by an organization's leadership is an essential component of creating a strong culture of compliance. As the HIPAA regulations and guidance continue to evolve during the COVID-19 pandemic, Privacy Programs must continue to keep its staff, executive leadership, and board-level management informed on the changing regulatory landscape and any emerging HIPAA related risk areas.

The majority of organizations 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. Besides, most organizations appear to maintain adequate documentation of their HIPAA training efforts. It is highly encouraged that organizations maintain policies and procedures in a centralized location that is accessible to all workforce members.

Positively, we also found that organizations are auditing a wide variety of items and issues, including most high-risk areas associated with the HIPAA requirements. However, around one-third of respondents stated that either an effectiveness evaluation of their HIPAA Privacy Program had never been conducted or 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 indicated 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 or research more complicated HIPAA related questions.

Lastly, approximately one-third of respondents stated that the COVID-19 public health emergency had not impacted their HIPAA Program. However, other participants responded that COVID-19 had increased HIPAA related training and education, research inquiries, policies, breach activity, responsibilities, and public health reporting. Organizations must continue to follow the HIPAA Privacy rule and incorporate HIPAA into topics developed since COVID-19, such as telemedicine.

ABOUT SAI GLOBAL

SAI Global helps risk and compliance professionals proactively manage risk to create trust and achieve business excellence, growth and sustainability for their organizations.

SAI360, our world-leading Risk platform, is the most complete integrated approach to risk management on the market including compliance management, enterprise & operational risk management, EHS & operational excellence, ethics & compliance learning and digital risk & business continuity use cases. Combining market-leading software capabilities, learning content and controls, SAI360 provides a line of sight to navigate risk and compliance management by addressing it from every perspective.

SAI Global is headquartered in Chicago, U.S., and operates across Europe, the Middle East, Africa, the Americas, Asia and the Pacific
Discover more at **www.saiglobal.com/risk** or follow us on **LinkedIn**. To see SAI360 in action, **request a demo.**