The Current State of HIPAA:

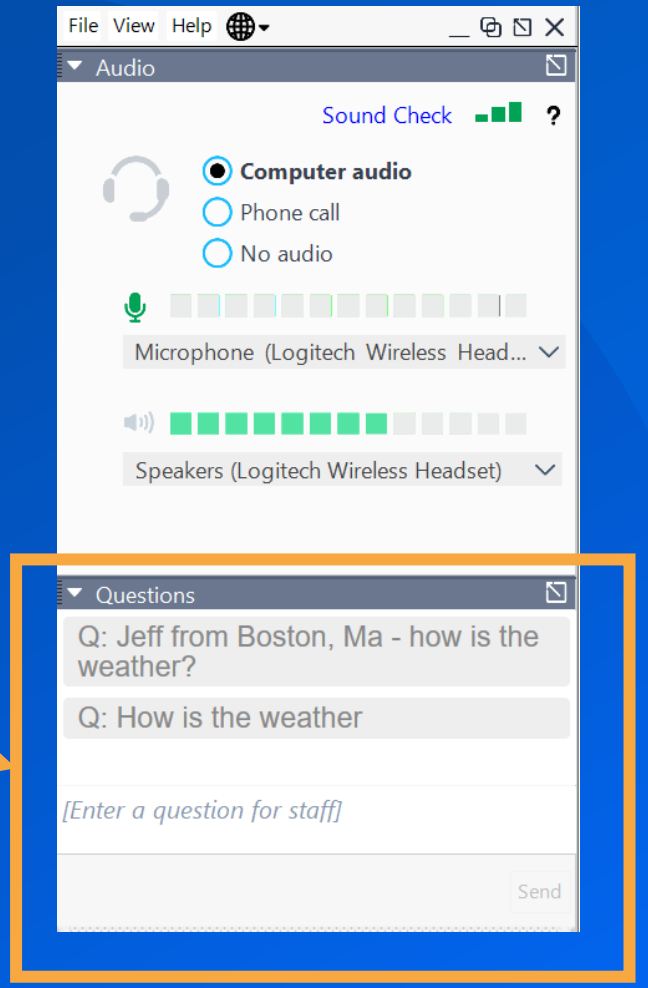
Reviewing Our 2023 HIPAA Compliance Benchmark Survey Results

SAI360

STRATEGIC MANAGEMENT SERVICES

Questions or Feedback?

Please type your questions or comments in the "Questions" tab.



WHO WE ARE

STRATEGIC MANAGEMENT SERVICES

has provided HIPAA and compliance advisory services for over 25 years to more than 2,000 organizations, including development and evaluation of HIPAA compliance programs, policies and procedures, training, breach assessments, state and local regulatory compliance, and security risk assessments, as well as overall compliance services that include claims data analyses, arrangement reviews, assistance with CIAs, acting as IROs and Board Compliance Experts, and litigation support.

CRC COMPLIANCE RESOURCE CENTER

operates hotline services, sanction checking and resolution services, compliance surveys, and a compliance related document development and training program.

SAI360

SAI360 is giving companies a new perspective on risk management. By integrating Governance, Risk, Compliance 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.

TODAY'S PRESENTERS

Robbi-Lynn Watnik
Senior Consultant,
Strategic Management Services

Natalie Lesnick
Consultant,
Strategic Management Services

STRATEGIC MANAGEMENT

SAI360

AGENDA

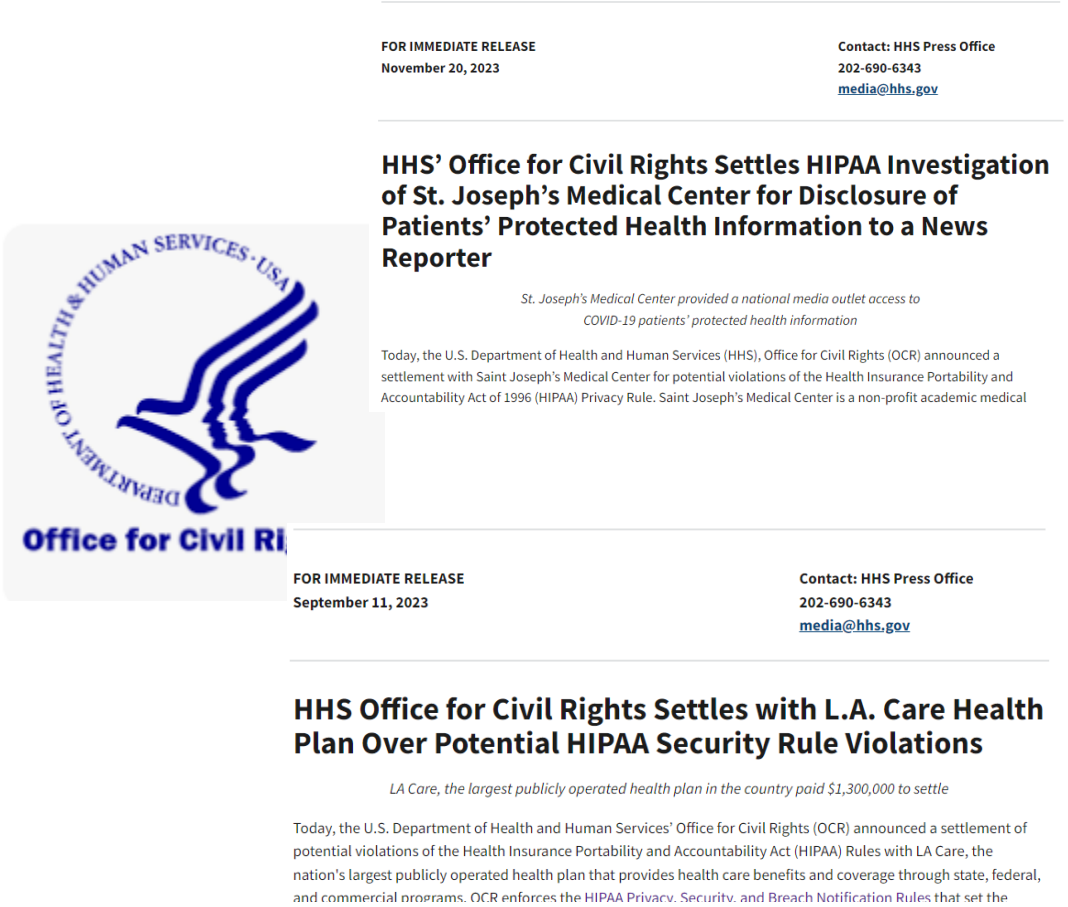
- Survey Introduction
- HIPAA Program Structure, Responsibility, and Oversight
- HIPAA Program Operations, Policies, Trainings, and Business Associates
- HIPAA Investigations, Breach Management, and Audits
- HIPAA Program Assessment and Priorities
- Overall Conclusion
- Q&A Session

STRUCTURE OF SURVEY

- 29 survey questions.
- 178 survey respondents.
- Nearly half of respondents reported being associated with a hospital or health system, while others were associated with behavioral/mental health, physician/group practice, health plan/insurance provider, skilled nursing/long-term care, and clinic/ambulatory surgery center.
- There was a significant increase in respondents associated with physician groups.
- Respondents were dispersed over a variety of health care provider types or vendors (i.e., home health, laboratory, pharmacy, etc.).

SURVEY GOALS

- The nature and level of commitment that healthcare organizations have made to HIPAA compliance in 2023
- HIPAA training frequency and enforcement
- HIPAA Audit areas
- Enforcement encounters entities have experienced
- Potential HIPAA priorities for organizations



FOR IMMEDIATE RELEASE
November 20, 2023

Contact: HHS Press Office
202-690-6343
media@hhs.gov

HHS' Office for Civil Rights Settles HIPAA Investigation of St. Joseph's Medical Center for Disclosure of Patients' Protected Health Information to a News Reporter

St. Joseph's Medical Center provided a national media outlet access to COVID-19 patients' protected health information

Today, the U.S. Department of Health and Human Services (HHS), Office for Civil Rights (OCR) announced a settlement with Saint Joseph's Medical Center for potential violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule. Saint Joseph's Medical Center is a non-profit academic medical

DEPARTMENT OF HEALTH & HUMAN SERVICES · USA

Office for Civil Ri

FOR IMMEDIATE RELEASE
September 11, 2023

Contact: HHS Press Office
202-690-6343
media@hhs.gov

HHS Office for Civil Rights Settles with L.A. Care Health Plan Over Potential HIPAA Security Rule Violations

LA Care, the largest publicly operated health plan in the country paid $1,300,000 to settle

Today, the U.S. Department of Health and Human Services' Office for Civil Rights (OCR) announced a settlement of potential violations of the Health Insurance Portability and Accountability Act (HIPAA) Rules with LA Care, the nation's largest publicly operated health plan that provides health care benefits and coverage through state, federal, and commercial programs. OCR enforces the HIPAA Privacy, Security, and Breach Notification Rules that set the

STRATEGIC MANAGEMENT

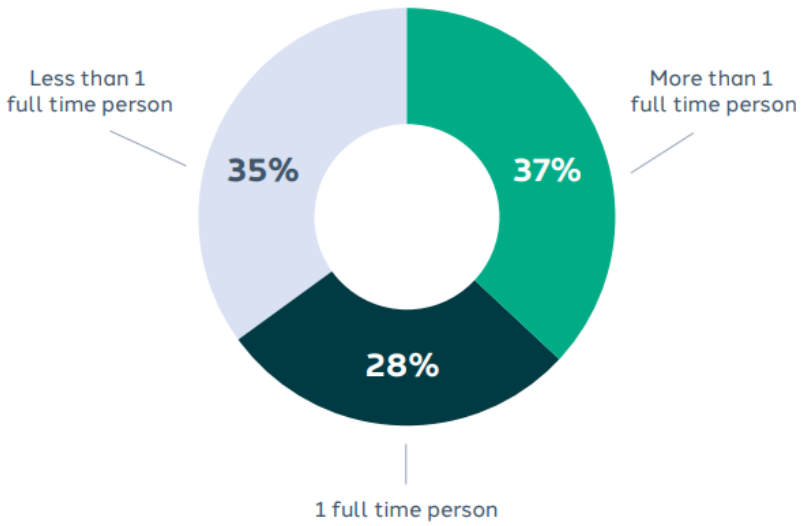
SAI360

STRATEGIC MANAGEMENT

HIPAA Program Structure, Responsibility, and Oversight

SAI360

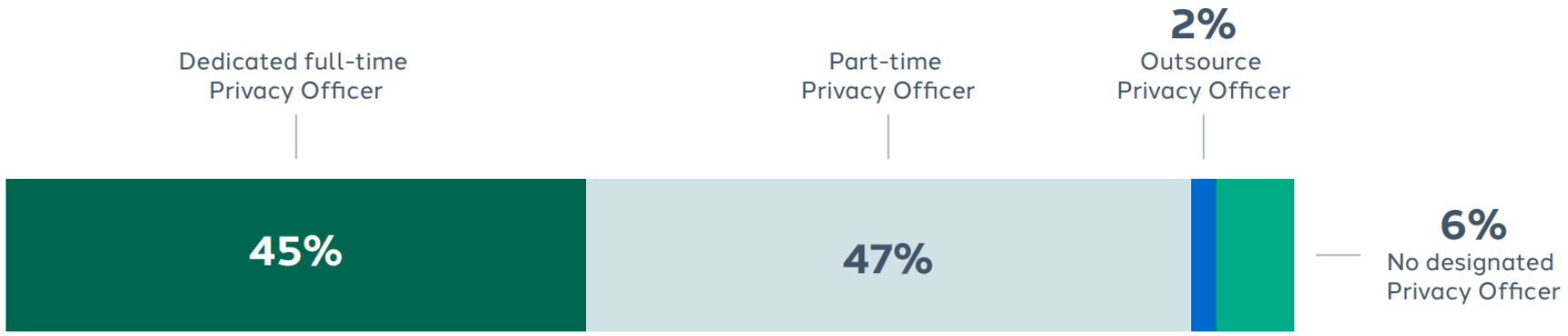
WHAT IS THE STAFFING LEVEL FOR THE HIPAA PRIVACY OFFICE FUNCTION?



DISCUSSION:

- Decreases in percentage of full-time privacy officer function may be attributed to the higher percentage of respondents associated with physician/group practices.
- The HIPAA Privacy Rule requires a covered entity to “designate a privacy office who is responsible” for HIPAA compliance.
- The rule does not specifically require the amount of time that this individual is expected to devote to their role as the HIPAA Privacy Officer.
- Not having a full-time privacy officer is a risk, especially for larger organizations.
- It is advisable to have an individual with the expertise and bandwidth to properly deal with all privacy issues.

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



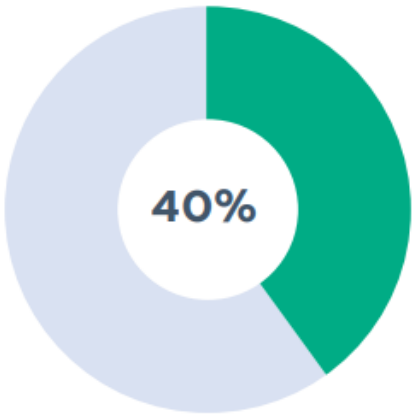
DISCUSSION:

- The higher percentage of respondents indicating Privacy Officers have part-time or secondary duty positions may be due to the higher percentage of physician/group practice respondents.
- Between these two initial questions, we gather that HIPAA privacy is not necessarily front and center to many covered entities.
- Remember: the HIPAA Privacy Rule requires covered entities to designate a privacy officer.
- OCR has stated that the privacy rule is “scalable” so that providers can tailor the program based on their size.
- Providers are advised to be cautious to make sure they meet basic HIPAA Privacy requirements.

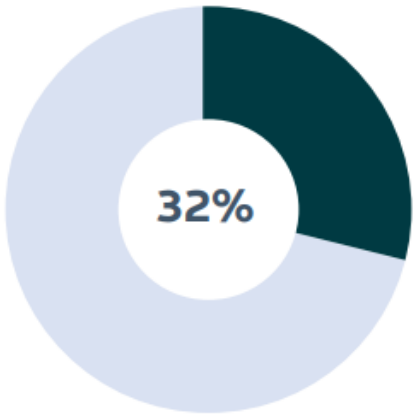
TO WHOM DOES YOUR PRIVACY OFFICER REPORT?

DISCUSSION:

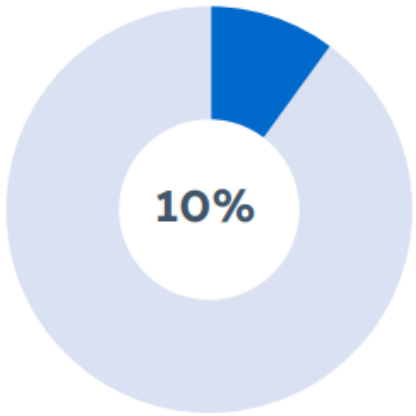
- OCR nor the regulations specify to whom a privacy officer should report.
- It remains advisable that the Privacy Officer have a direct reporting relationship with the highest level within an organization.



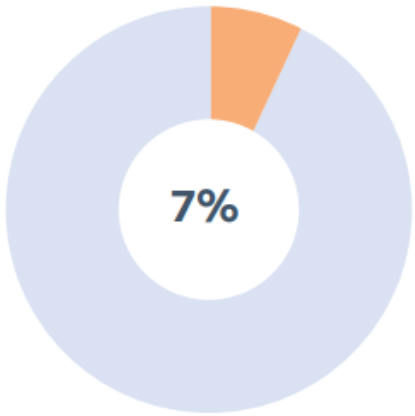
Reports to CEO/President



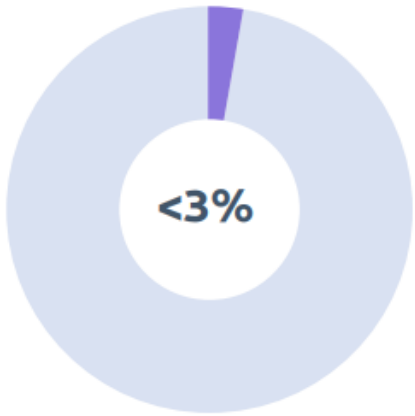
Reports to Compliance Officer



Reports to Legal Counsel



Reports to Chief Operating Officer



Reports to Chief Information Officer/ Health Information Management

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

61%
Board or Board Compliance Committee

44%
Executive-Level Compliance Committee

16%
Executive-level HIPAA Privacy/Security Committee.

12%
Organization does not have an oversight body for HIPAA operations.

DISCUSSION:

- These results are almost opposite to the results from the 2020 survey in which most respondents stated that the Privacy Officer reported to the Executive-Level Compliance Committee.
- This year most respondents stated they reported directly to the Board of Directors.
- Respondents were invited to check more than one choice so respondents may have multiple reporting obligations.
- With only a little more than 12% of respondents indicating their organization did not have an oversight body for HIPAA operations, organizations and their leaders may be taking much more interest in HIPAA privacy.

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

DISCUSSION:

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

STRATEGIC MANAGEMENT

HIPAA Program Operations – Policies and Procedures

SAI360

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

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

15.5% have 16-20.

15% have 1-5.

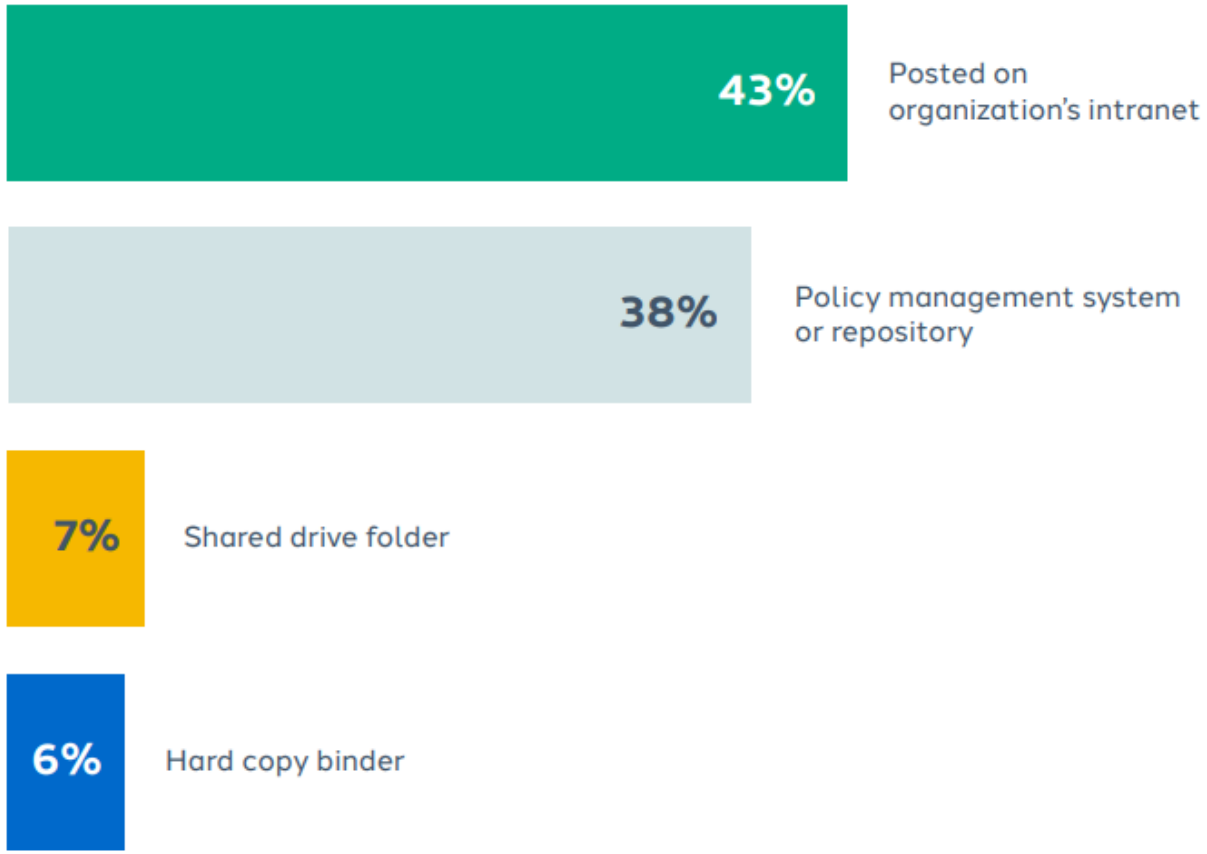
DISCUSSION:

- Based on HIPAA regulatory requirements, a covered entity is advised to have at least 15 single-topic policies.
- Over 50% reported having at least 16 or more policies.
- Anything lower indicate that the organization is not fully addressing the Privacy Rule requirements.

STRATEGIC MANAGEMENT

SAI360

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



DISCUSSION:

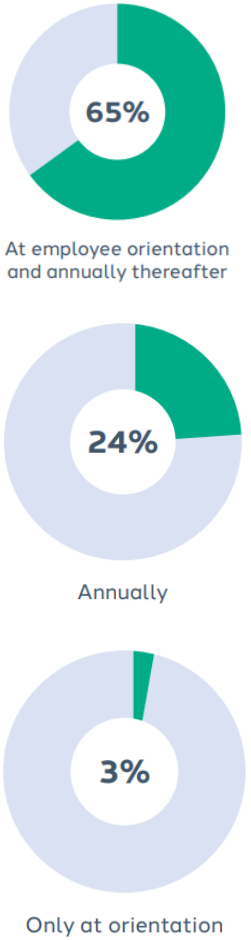
- A majority of respondents rely on electronic means for employees to access HIPAA-related policies and procedures.
- The percentage of respondents who continue to make policies available in paper format is a significant reduction from our previous survey.

STRATEGIC MANAGEMENT

HIPAA Program Operations - Training

SAI360

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



DISCUSSION:

- While slightly lower, these responses are not significantly different from the 2020 survey.
- There is continued evidence that organizations recognize that education is key.
- It is a best practice to provide training to workforce members when hired and at least annually.
- There is also no specific regulatory requirement for annual training, only workforce members must be trained “as necessary and appropriate for the members of the workforce to carry out their functions within the covered entity.”

STRATEGIC MANAGEMENT

SAI360

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

DISCUSSION:

- It appears that most respondents keep adequate documentation on HIPAA training.
- Who has taken the training and when they completed the training are important items to track.

- Best practice: consider maintaining records of test and quiz results to evidence workforce understanding of the privacy rule and the organization's policies therein.

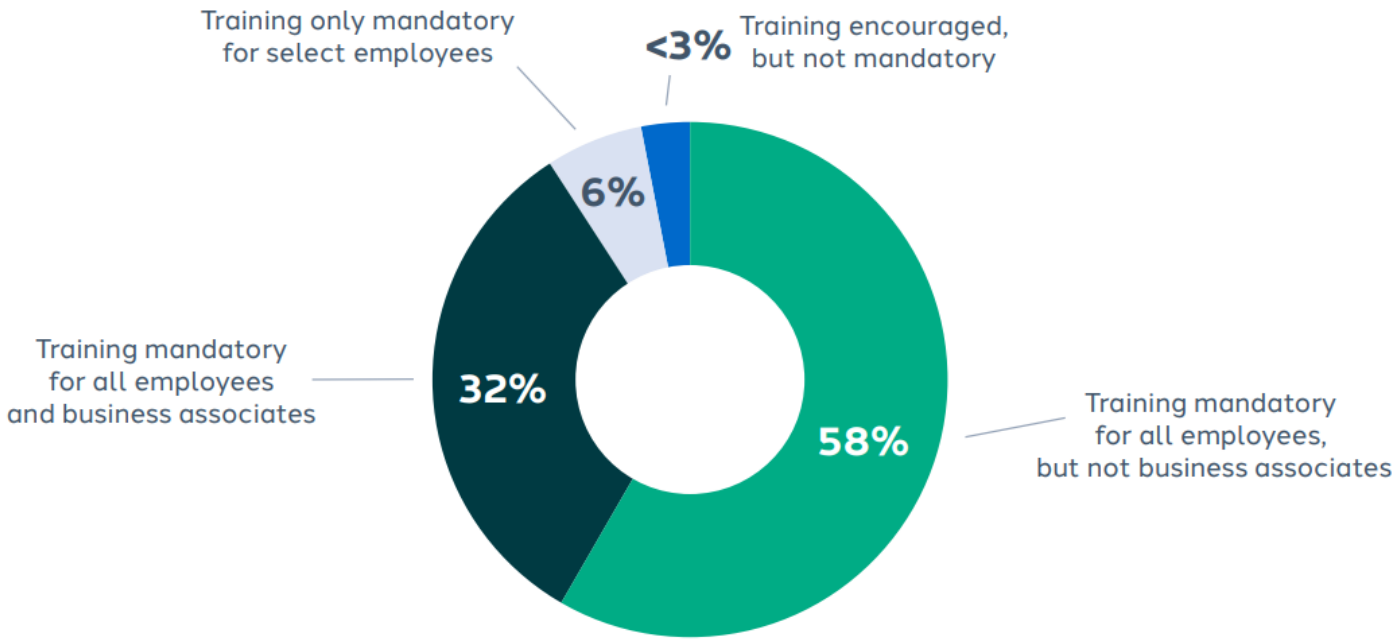
STRATEGIC MANAGEMENT

SAI360

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

DISCUSSION:

- Only one-third of respondents reported they require training for employees and business associates.
- Almost 10% of respondents indicated that training is not required of all employees. This is contrary to the HIPAA Privacy Rule and best practices.



STRATEGIC MANAGEMENT

HIPAA Program Operations – Working with BAs

SAI360

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

75%

An overwhelming majority of respondents indicated they maintain such an inventory

DISCUSSION:

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

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

DISCUSSION:

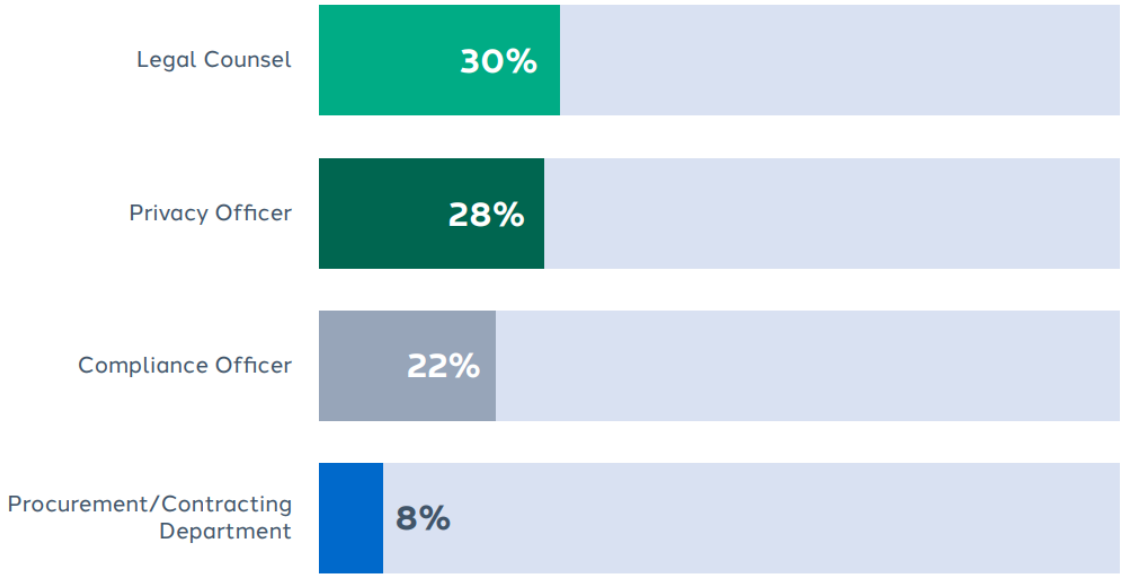
- Having an agreement in place with identified BAs is important to protect against unauthorized disclosures of PHI.
- It is also a regulatory requirement and can lead to hefty fines.
- Covered entities are advised to have a checklist in place to identify which vendors meet the definition of a BA and execute an agreement containing at a minimum, the elements in the regulation.

An overwhelming majority of respondents answered yes to this question

STRATEGIC MANAGEMENT

SAI360

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



DISCUSSION:

- There are risks if vendors are not identified as business associates and agreements are not executed accordingly.
- A checklist to identify which vendors are BAs is helpful.
- It is a best practice that if the Privacy Officer is not a decision maker, they serve as consultants to the decision maker to identify potential Business Associates.
- In many cases, this will be a straightforward determination, but in other cases, the privacy officer's expertise and knowledge will be invaluable.
- If a procurement/contracting department is making the determination, someone in the department should understand HIPAA.

STRATEGIC MANAGEMENT

Investigations, Breaches, Disciplinary Actions

SAI360

HOW ARE MOST HIPAA PRIVACY INCIDENTS DETECTED?

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

DISCUSSION:

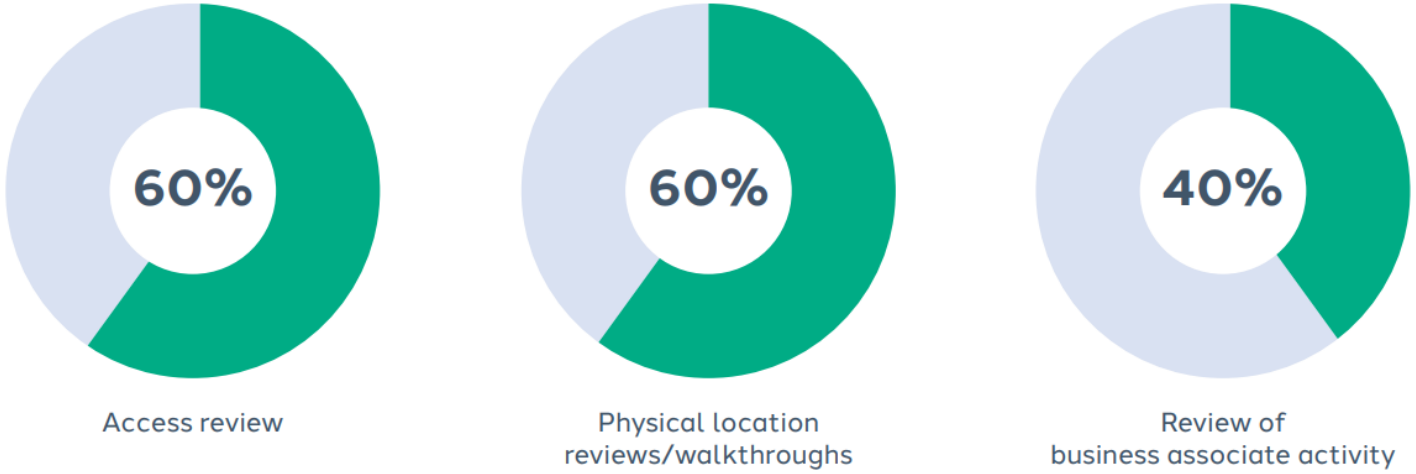
- While slightly lower than the 2020 survey, almost half of respondents indicated their organization learned of a privacy incident through an employee report is a positive.
- Almost 50% decrease in reports/complaints from patients.

STRATEGIC MANAGEMENT

Program Assessment and Priorities

SAI360

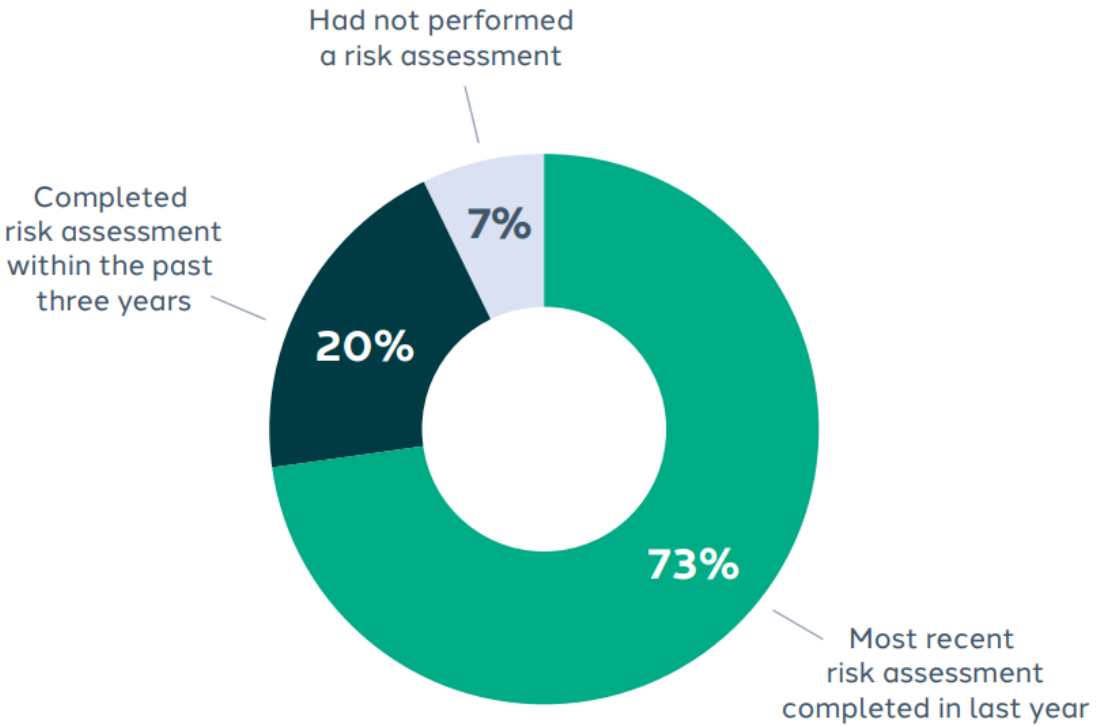
WHICH OF THE FOLLOWING ITEMS ARE CURRENTLY ON YOUR HIPAA/COMPLIANCE AUDIT WORK PLAN?



DISCUSSION:

- The responses continue to indicate that organizations have a wide variety of items and issues in their audit work plans.
- Best practices promote the use of audit work plans, but smaller organizations may not have the resources to complete a formal audit.
- Organizations should consider a more streamlined approach to auditing.

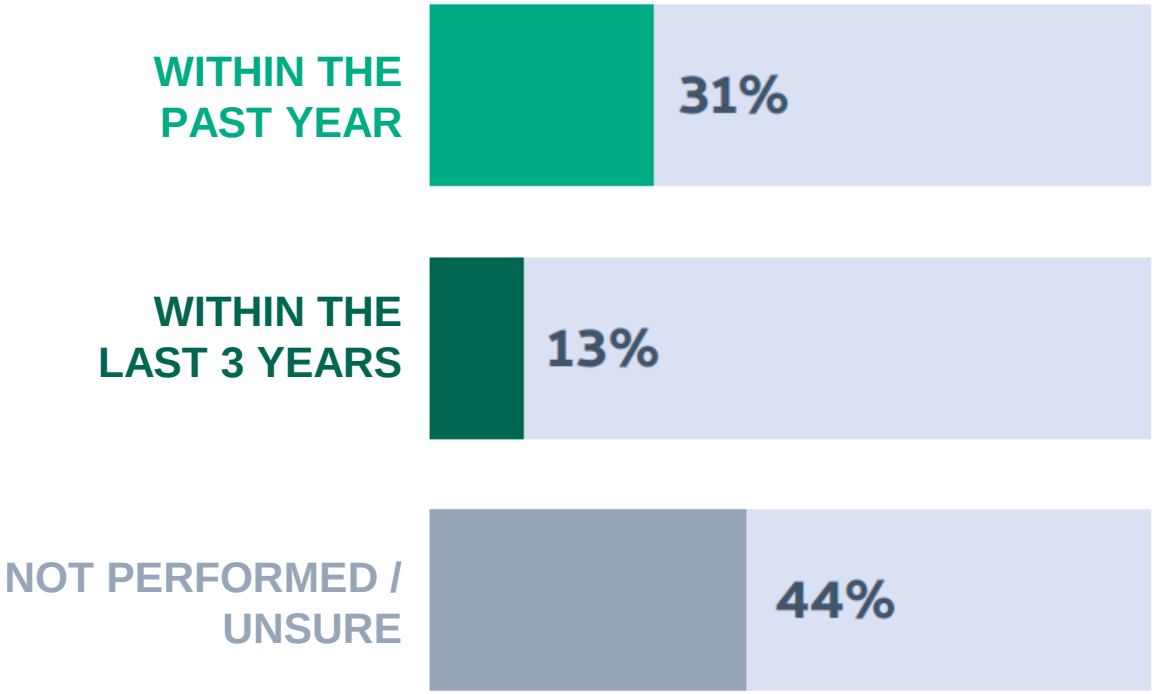
HIPAA REQUIRES PERFORMING A SECURITY RISK ANALYSIS TO IDENTIFY VULNERABILITIES THAT COULD RESULT IN A BREACH OF PHI.



DISCUSSION:

- Risk assessments are required.
- The rule does not specify the frequency of conducting the assessment.
- OCR guidance states that the “risk analysis process should be ongoing” and that covered entities may perform the assessment annually, bi-annually or every three years.
- If there is an incident, OCR investigators will most likely request data on the entity’s most recent risk assessment.

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



DISCUSSION:

- Conducting an effectiveness evaluation within the past year follows a best practice for measuring compliance with the HIPAA Privacy Rule.
- The rule does not require covered entities to conduct independent reviews, but it is an important tool.
- An independent evaluation of the program may help organizations with small privacy and compliance workforces.
- Outside independent reviews are also helpful tools if an organization is going through a transition that may impact HIPAA privacy.

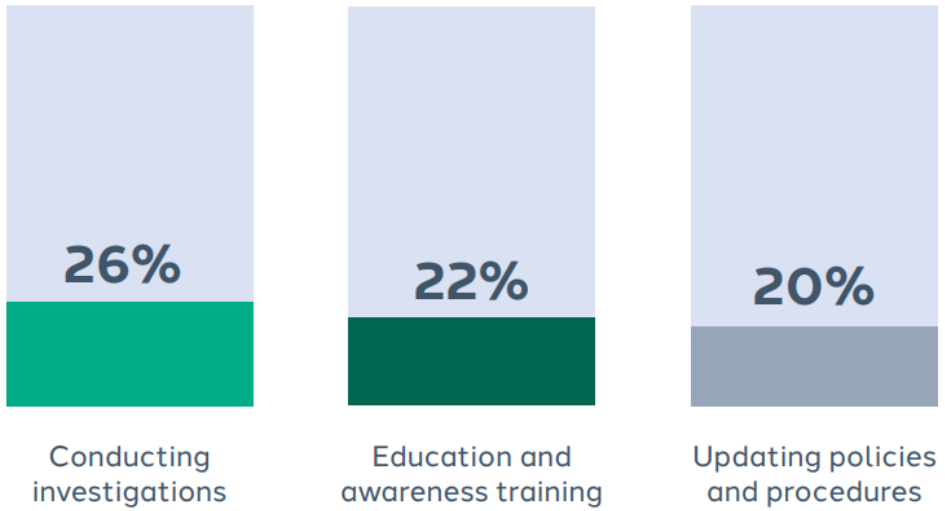
PLEASE SELECT THE TOP THREE PRIORITIES TO BE ADDRESSED BY YOUR HIPAA COMPLIANCE PROGRAM IN THE NEXT 12 MONTHS

DISCUSSION:

- The priorities and associated percentages are similar to the 2019 and 2020 surveys.
- Not addressing the top three priorities identified can pose risks to the organization's reputation and financial risks.
- Half of the respondents noted that reducing inappropriate disclosures was a priority. This may indicate a need for increased training and education about HIPAA Privacy Rules, increased monitoring of EHR access, and a need for greater controls over access to the EHR.

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

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



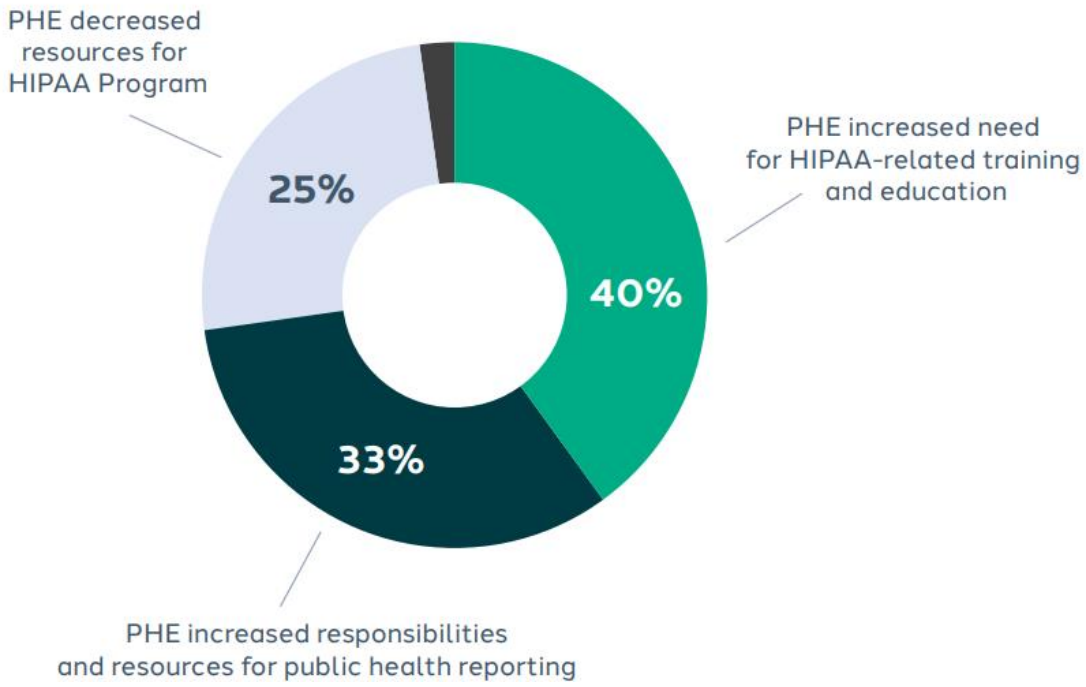
DISCUSSION:

- In the 2020 survey, updating policies and procedures took the most planning and resources.
- The difference this year indicates that organizations are finding standardized processes and timelines for updating policies and procedures.
- There was a 10% increase in respondents indicating that conducting investigations took the most planning and resources.
- There was also a 5% increase in respondents who stated that education and awareness took the most planning.

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

DISCUSSION:

- The increased need for training and education indicates that healthcare entities understood the need to continue safeguarding privacy during COVID-19.
- The costs of treatment and reduced workforce may have necessitated some covered entities to shift resources from HIPAA Privacy to other areas.
- OCR's enforcement discretion of certain HIPAA-related violations expired in May 2023.
- Organizations are advised to return to pre-COVID-19 HIPAA privacy program priorities to avoid fines moving forward.



STRATEGIC MANAGEMENT

SAI360

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

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

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

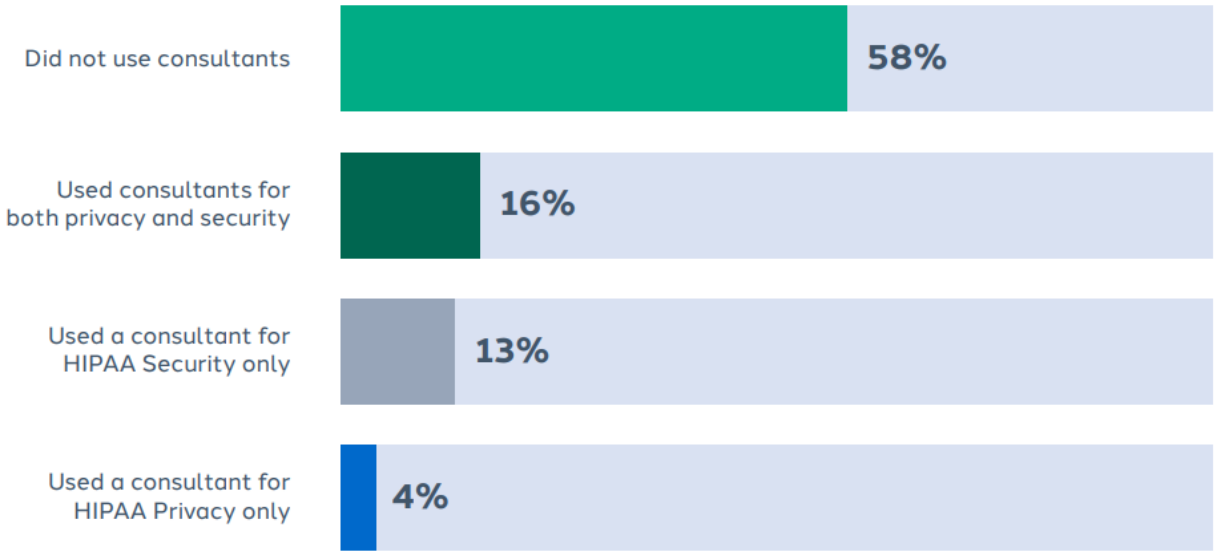
DISCUSSION:

- As with the prior survey, only a small number of organizations reported that they did not use any type of software for their Privacy Program operations.
- Software programs can help track investigations, train staff, and keep track of policies to ensure currency of the policy and facilitate access to the policies.
- BUT not all organizations have the resources for elaborate expensive tools.
- Even using spreadsheets to track audits, policies, breaches, and training will provide the critical documentation to evidence an effective HIPAA compliance program.

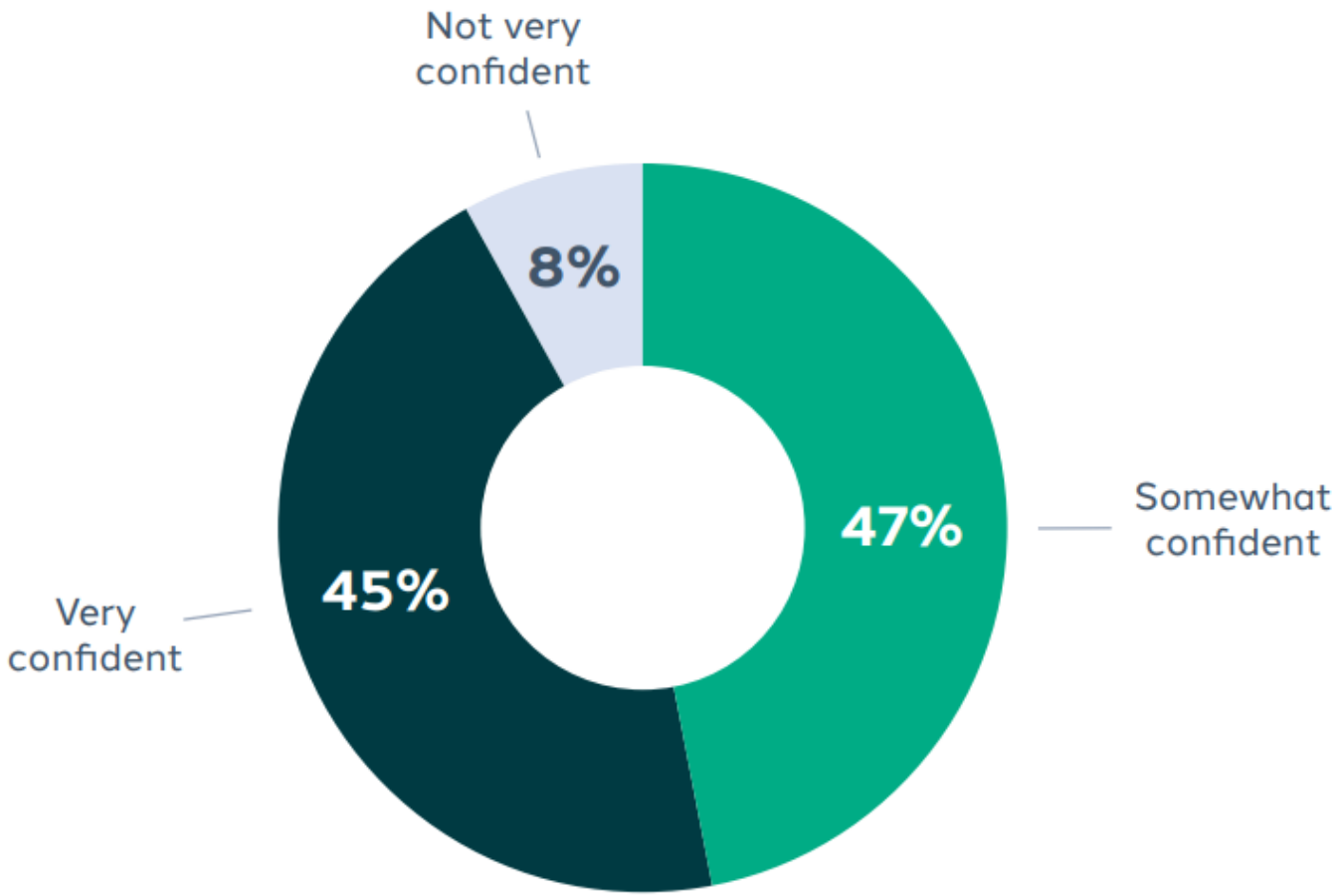
DOES YOUR ORGANIZATION USE ON-CALL CONSULTANT/VENDOR SERVICES TO ASSIST WITH HIPAA PRIVACY AND SECURITY FUNCTION

DISCUSSION:

- The responses to this year's survey are consistent with the 2020 survey results.
- The HIPAA Privacy and Security Rules do not require covered entities or business associates to use external vendors.
- 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.



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



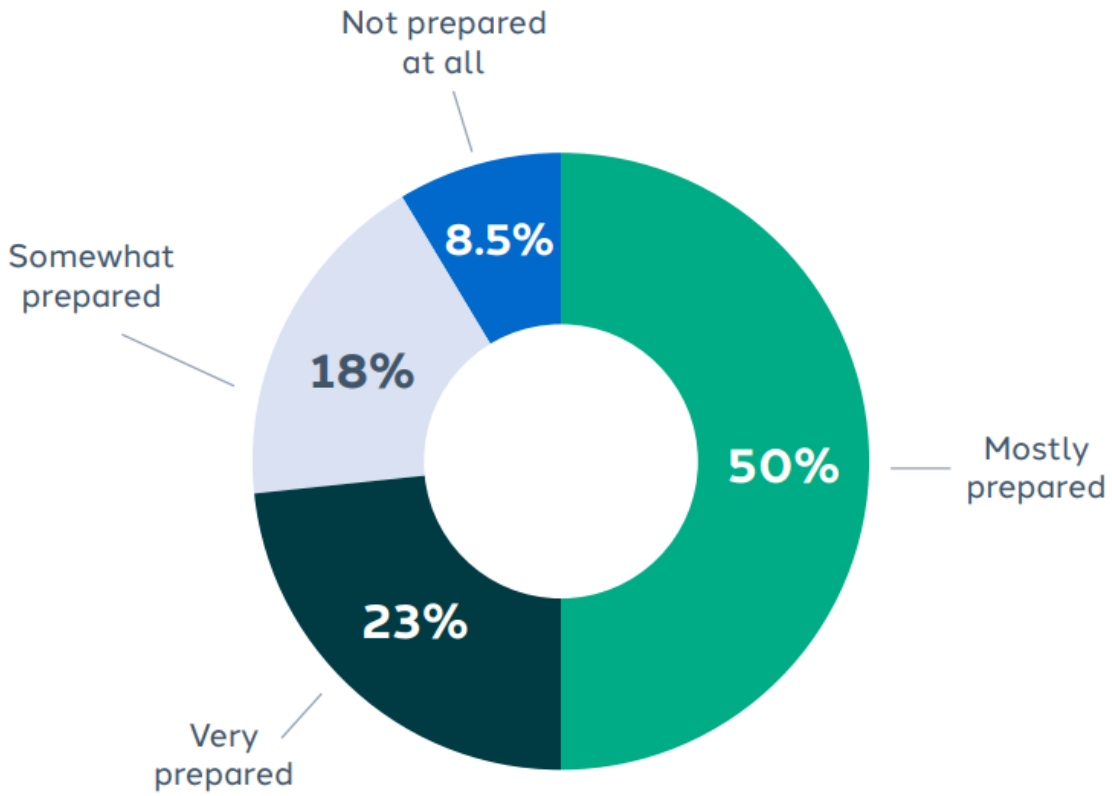
DISCUSSION:

- The percentage of respondents who are only “somewhat confident” was higher than those who were “very confident,” compared to prior surveys.
- Both responses show an increase in those who are “very confident” over those who are “somewhat confident.”

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

DISCUSSION:

- The combined percentage of respondents who indicated they were “mostly” or “somewhat prepared” is a slight increase from the 2020 survey.
- The percentage of those stating that they were “very prepared” was 5% lower.
- The percentage stating they were “not prepared at all” was slightly higher.



STRATEGIC MANAGEMENT

SAI360

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

47%

HIPAA breach reported to OCR within the past 12 months

12%

Breach reported 1 to 2 years ago

13%

Breach reported 3 to 5 years ago

16%

Never reported A breach to OCR

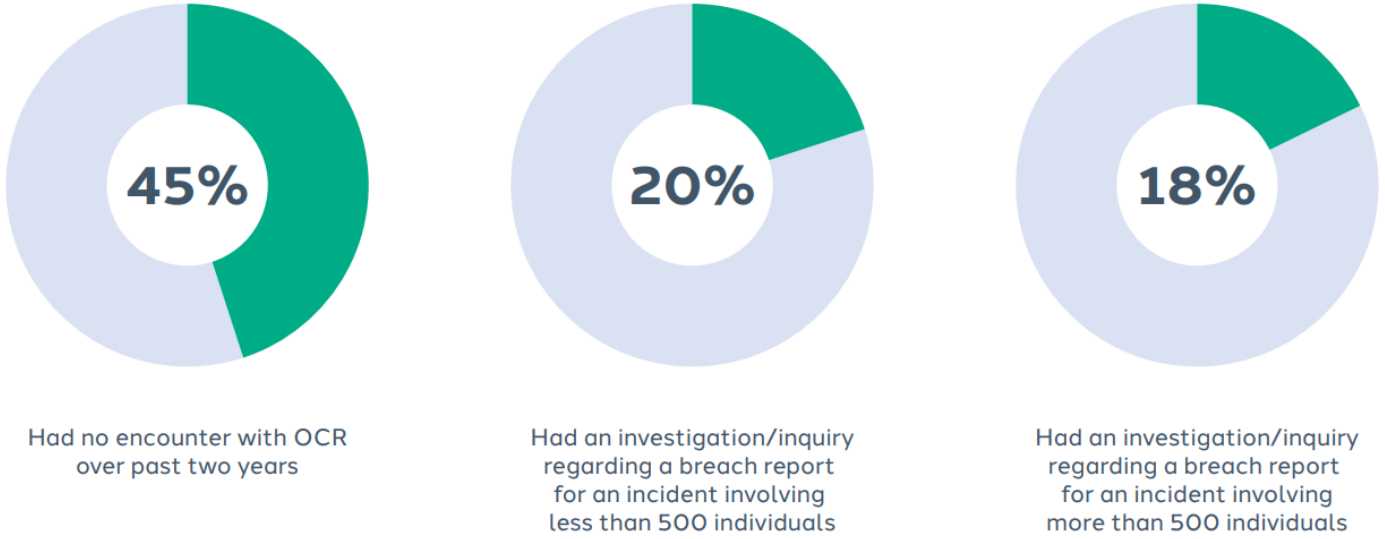
DISCUSSION:

- In total, about 80% of respondents indicated that they experienced an OCR reportable HIPAA breach within the past five years.
- Almost 50% stated they reported a HIPAA breach within the last 12 months.
- It is nearly impossible to prevent all breaches.
- Training of the workforce/early detection of potential incidents with an immediate investigation followed by remediation as needed are key.
- Organizations should implement industry-accepted best practices to decrease the possibility of a data breach involving electronic PHI.

STRATEGIC MANAGEMENT

SAI360

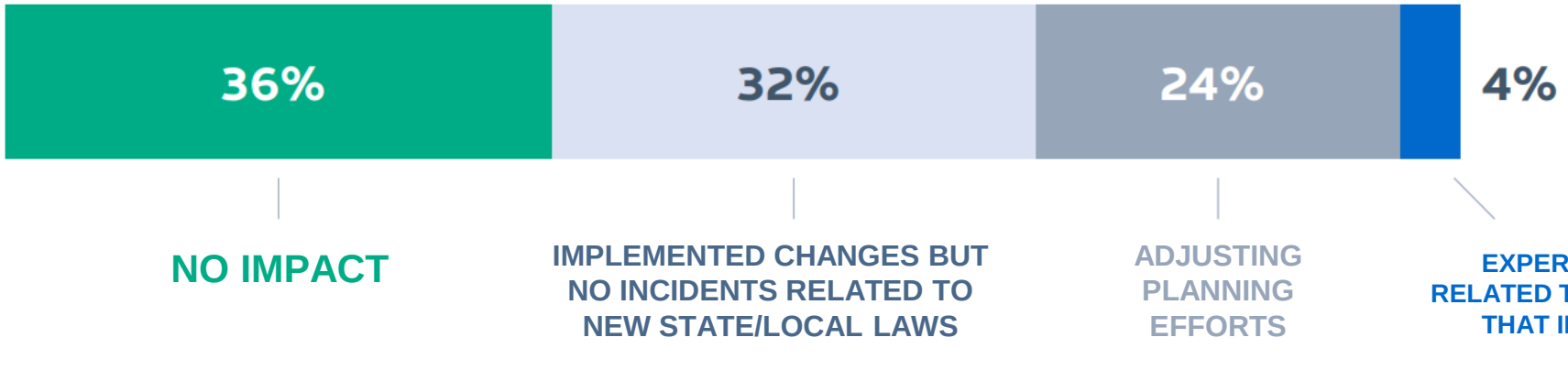
WHAT TYPE OF ENCOUNTERS HAS YOUR ORGANIZATION HAD WITH OCR IN THE LAST 2 YEARS?



DISCUSSION:

- Almost half of the respondents reported having no encounter with OCR in the past two years.
- Responses to this question correlate with the responses to a previous question that addressed how privacy incidents are detected.
- Almost 44% of respondents to that question indicated that employees report issues directly to leadership.

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



DISCUSSION:

- Results from this question suggest that most organizations continue to not feel the impact of state actions and mandates related to patient privacy matters.
- More than 50% are adjusting their planning efforts or implementing changes to their Privacy Program, ostensibly to prepare for new state or local patient privacy laws.
- Even though states are enacting privacy laws, many are exempting those organizations that are subject to HIPAA privacy and security requirements.
- Covered entities should be mindful of state breach reporting requirements since these may be more stringent and may require different reporting processing when a breach occurs.

STRATEGIC MANAGEMENT

SAI360

OVERALL CONCLUSIONS

- There was a marked increase in the percentage of respondents representing physician provider offices, which may indicate an increasing recognition of the important of safeguarding patient privacy and value of a HIPAA Privacy Program regardless of provider type and size.
- Most Privacy Officers are reporting to the CEO or Compliance Officer and are providing formal reports to the Board of Directors and the Executive-Level Compliance Committee.
- Most organizations appear to have implemented operations to address HIPAA requirements.
- More than three-quarters of respondents stated that the COVID-19 public health emergency had increased HIPAA-related training and education, research inquiries, policies, breach activity, responsibilities, and public health reporting.

STRATEGIC MANAGEMENT

QUESTIONS?

SAI360

Thank you!

Robbi-Lynn Watnik

Senior Consultant, Strategic Management Services

rwatnik@strategicm.com

Natalie Lesnick

Consultant, Strategic Management Services

nlesnick@strategicm.com

STRATEGIC MANAGEMENT

Compliance.com

SAI360

sai360.com