Panel Discussion:
Updates from the 2019 National HIPAA Compliance Benchmark Survey Report

HIPAA SUMMIT – MINI - SUMMIT I

WEDNESDAY, MARCH 4, 2020

11:00 AM – 12:00 PM

Panel Moderators

Catie Heindel, JD, CHC, CHPC, CHPS
Managing Senior Consultant
Strategic Management Services, Alexandria, VA
cheindel@strategicm.com

Lisa Shuman, MPA, CHC, CHPC, CHRC
Senior Consultant
Strategic Management Services, Alexandria, VA
lshuman@strategicm.com

Panel Members

Cathy Bodnar, MS, RN, CHC
Chief Compliance and Privacy Officer, Cook County Health, Chicago, IL
cbodnar@cookcountyhhs.org

Josephine N. Harriott, JD
Deputy Chief Compliance Officer, Health Sciences at Howard University, Washington, DC
josephine.harriott@Howard.edu

Darlene Mitchell, MBA
Vice President of Corporate Compliance, Advantia Health, Arlington, VA
darlene.mitchell@advantiahealth.com

Cook County Health

Provider

- Academic Medical Center with 450-beds
- 79-bed Community Acute Care Hospital
- 120,000 inpatient days
- 140,000 ED visits
- 16-community centered clinics
- 1M outpatient visits
- 1.5M prescriptions
- 45% uninsured

Health Plan

- 1 in 3 Cook County residents enrolled in Medicaid are members of CountyCare
- 300,000 members from nearly every zip code in Cook County
- Network includes more than 70 hospitals and 15,000 specialists
- Contributed more than $1B to CCH since 2014

Correctional Health

- 50,000+ intake screenings at the Cook County Jail and the Juvenile Temporary Detention Center
- 30%+ detainees with behavioral health needs
- 5,000 naloxone kits distributed
- 6M doses of medication annually
- 10,000 detox patients annually

Public Health

- State and nationally certified public health authority for 2.3 million residents in 125 suburbs
- Responsible for the prevention and spread of more than 70 diseases, emergency preparedness and environmental health

Advantia Health

o **Privately-held healthcare company based in Arlington, Virginia**

o **Mission: Transforming healthcare for all women**

o **OB-GYN and Coordinated Specialists Offices**
  - o **4 States (MD, VA, IL, MO) and coming soon to Washington, DC**
  - o **Over 200 Providers**
  - o **60 Locations**
  - o **Serving over 430,000 patients**
  - o **14,000 births in 2019**

o **Pacify: Uber-like telehealth app for new parents**

www.advantiahealth.com   **www.pacify.com**

Howard University Health Sciences

Howard University Health Sciences includes Howard University Hospital, our Faculty Practice Plan, the Louis B. Stokes Health Sciences Library, and our Colleges of Medicine, Dentistry, and Pharmacy, Nursing, and Allied Health, as well as several specialty institutes and centers.

Over the course of its 145-year history of providing the finest primary, secondary and tertiary health care services, Howard University Hospital has become one of the most comprehensive health care facilities in the Washington, D.C. metropolitan area and designated a DC Level 1 Trauma Center.

A private, nonprofit institution, HUH is the nation's only teaching hospital located on the campus of a historically Black university.

http://healthsciences.howard.edu/

Agenda

o Survey Introduction and Background

o Panel Discussion on Survey Findings:
   o HIPAA program structure, responsibility and oversight
   o Program operations
   o Business Associate Agreements (BAA) management
   o Program assessment and priorities
   o Investigations, breaches, and disciplinary action
   o Interactions with enforcement

o Audience Question & Answer (Q&A) Session

2019 HIPAA Compliance Benchmark Survey

The HIPAA Compliance Survey report, along with the interactive webpage, can be found at the following link:
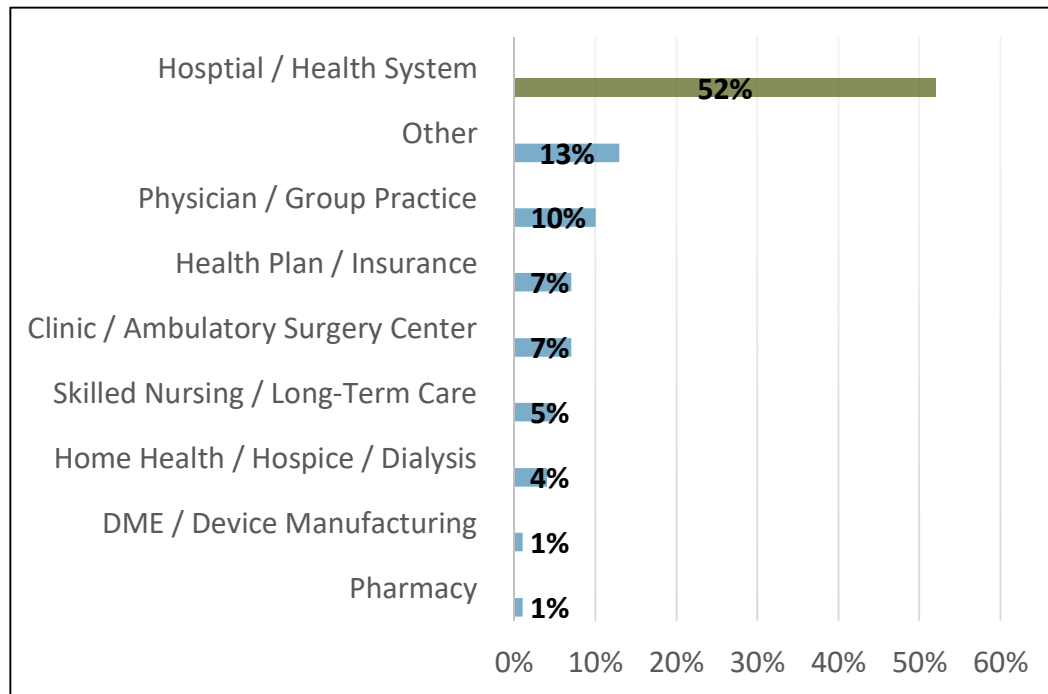
http://view.ceros.com/sai-global/hipaa-survey-2019-1/p/1

Survey Background

Organization types surveyed

2019 HIPAA Compliance Benchmark Survey

Chart: Organization types surveyed

Organization Type	Percentage
Hosptial / Health System	52%
Other	13%
Physician / Group Practice	10%
Health Plan / Insurance	7%
Clinic / Ambulatory Surgery Center	7%
Skilled Nursing / Long-Term Care	5%
Home Health / Hospice / Dialysis	4%
DME / Device Manufacturing	1%
Pharmacy	1%

o 29 survey questions

o 352 survey respondents

o Respondents were dispersed over a variety of health care provider types, health plans, and business associates (i.e., device manufacturer, pharmaceutical company, etc.).

Survey Goals

To better understand….

- The nature and level of commitment that healthcare organizations have made to HIPAA compliance in 2019

- The types of HIPAA related risk areas facing health care entities

- How entities are handling potential and actual breach incidents

- The types of enforcement action entities have experienced on a federal, state and local level

- HIPAA priorities for organizations

Positive Impressions

2019 HIPAA Compliance Benchmark Survey

o Organizations appear prepared for a HIPAA investigation and understand the importance of implementing a response plan, policies and procedures, and software tools to properly demonstrate their HIPAA compliance efforts to OCR.

o Executive leadership and the Board are largely supportive of HIPAA Programs, indicating that HIPAA Programs are doing a good job educating their Board and leadership regarding the regulatory and enforcement environment and relevant HIPAA risk areas for their organization.

o Virtually all organizations maintain some degree of HIPAA policies and procedures and training records, particularly documentation of who was trained, when it took place and what was included in the training.

o Organizations have a good understanding of the breach notification rule requirements, as many noted that they use a breach risk assessment tool, with stating that they use their tool to assess all privacy and security related incidents.

Identified Areas for Improvement

2019 HIPAA Compliance Benchmark Survey

o Some HIPAA programs appear understaffed, as many indicated that they either have only one full-time, one part-time employee or less than one part-time employee in their HIPAA Privacy Office.

o Oversight for the HIPAA Privacy program operations is somewhat scattered and occurs at multiple levels throughout the organizations surveyed.

o While a majority of respondents indicated that the organization had conducted a thorough assessment of the risks and vulnerabilities ePHI, we would expect to see all organizations focusing on this requirement given recent OCR emphasis.

o A very minimal amount of participants reported having an interaction with state/local laws or enforcement entities, which is surprising given recent developments in the emerging trend of non-federal authorities enforcing against privacy or security violators based on state law requirements.

o Almost a majority of respondents indicated that either an effectiveness evaluation of their HIPAA Privacy Program had <u>never</u> been conducted or that they did not know if one was ever completed.

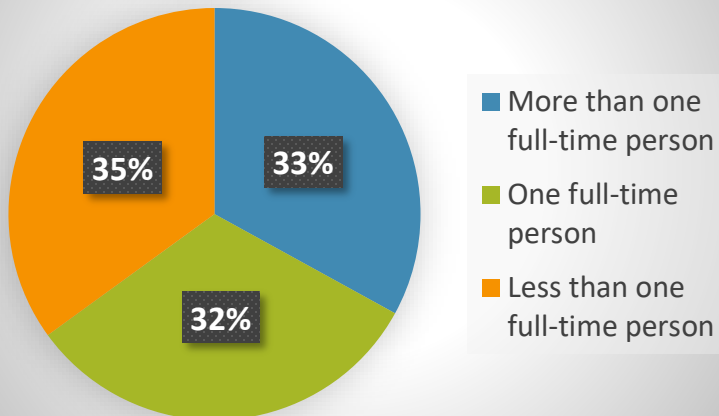# Survey Results - Program Structure, Responsibility and Oversight

To whom does your privacy officer report?

- **37%** PO reports to Compliance Office
- **40%** PO reports to CEO/President
- **16%** PO reports to Counsel

Who is accountable for oversight of HIPAA operations?

- **37%** Oversight was delegated to an executive level committee
- **34%** Reported that HIPAA program oversight was at the Board level
- **27%** Participants had accountability to a senior executive
- **8%** No oversight

Program Staffing

- 33% More than one full-time person
- 32% One full-time person
- 35% Less than one full-time person

What kind of support do you receive from your Executive Leadership and Board?

o **80%** receive "positive" support from executive leadership and the Board. The remaining **20%** of respondents reported "weak" to "no support" from executive leadership or their organization's Board.

Panel Questions

HIPAA Program Structure, Responsibility and Oversight

1. What is the staffing level and oversight structure for your organization? Do you find sufficient to meet the needs of your Program (i.e., given volume of issues received/handled)? How do you manage the dual roles of Privacy Officer AND the Compliance Officer?

2. How do you typically report matters to leadership and the Board to make them aware of HIPAA incidents and any gaps or achievements with your HIPAA Program? What type of feedback do you receive?

Survey Results - Program Operations

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?

o Virtually all respondents indicated that they maintain HIPAA compliance training records.

Panel Questions

Program Operations

1. What type of HIPAA training is provided to all staff at your organization? Do you have certain staff/divisions - including HIPAA/Compliance staff - who receive additional/focused privacy training?

2. How do you track and communicate regulatory changes/updates to Compliance staff and stakeholders?

Survey Results - Business Associate Agreements (BAA) Management

Who maintains your BAAs? Who determines if a BAA is needed?

- 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.

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.
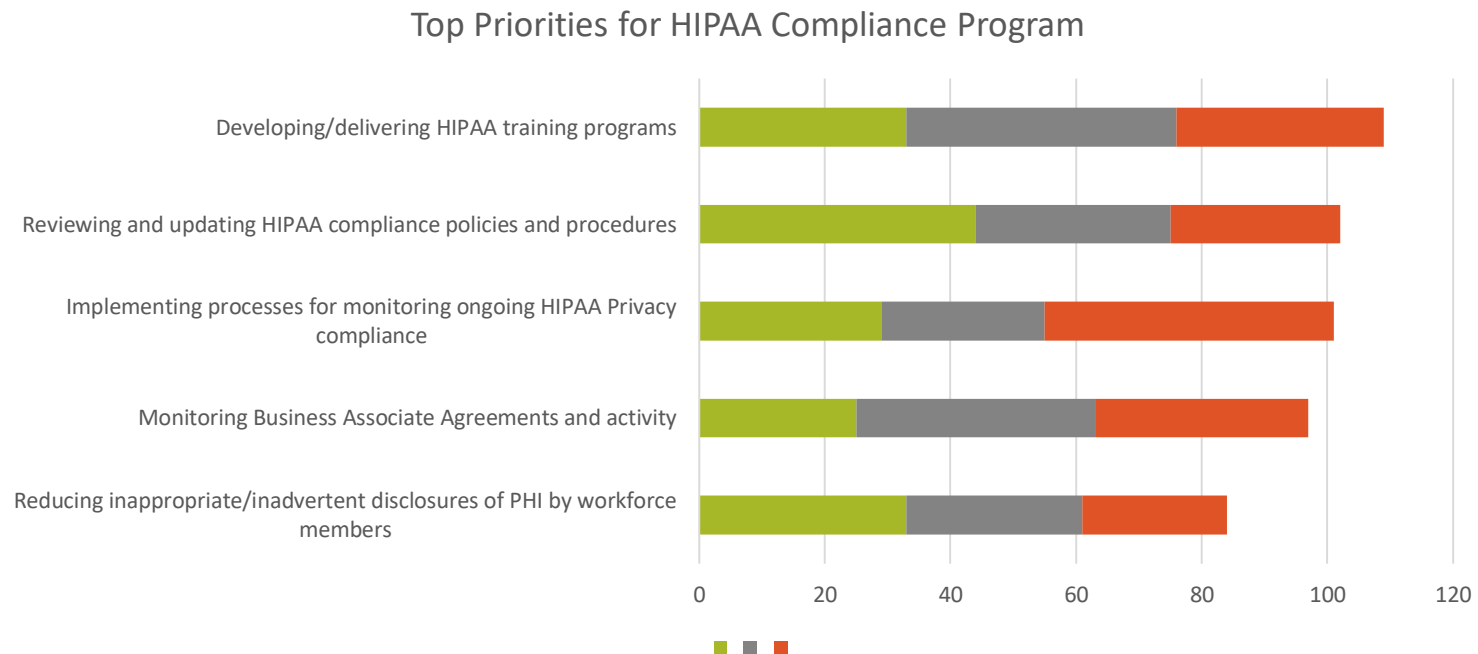
Panel Questions

Business Associate Management

1. How do you maintain, track and monitor Business Associate Agreements (BAAs)? What is the most valuable lesson you've learned for monitoring BAAs?

Survey Results - Program Assessment and Priorities

What are the top three priorities that you will address,

as part of your HIPAA compliance program operations, in the next year?

Top Priorities for HIPAA Compliance Program

Panel Questions

Program Assessment and Priorities

1. What are your priorities in 2020 for your HIPAA Program?
2. What is the most challenging aspect of your HIPAA Program?

Survey Results - Disciplinary Action & Enforcement

Are disciplinary procedures for incidents applied consistently throughout your organization?

- **52%** commented that disciplinary procedures following a HIPAA violation are <u>always</u> applied consistently

- **34%** said that disciplinary actions are only <u>sometimes</u> applied consistently

- **3%** reported that disciplinary action related to HIPAA issues are <u>never</u> applied uniformly

48%

REPORTED A HIPAA BREACH TO OCR IN THE LAST 12 MONTHS

- **46%** had no encounters with OCR over the last five years

- **32%** had an encounter with OCR following a breach

- **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

Panel Questions

Investigations, Breaches, and Disciplinary Action

1. How do you ensure that your organization applies disciplinary procedures for HIPAA incidents consistently throughout the organization?

Interactions with Enforcement

1. What helpful feedback from OCR or other government agencies relating to HIPAA/Privacy have you received or learned of through cases involving other entities?

Wrap Up & Conclusion

Based on your own experiences or those you have learned of from colleagues at other facilities, what are some lessons learned or advice you would give to others regarding interacting with law enforcement, interacting with patients who raise privacy concerns, and / or reporting breaches to management and the board?

Any Questions?