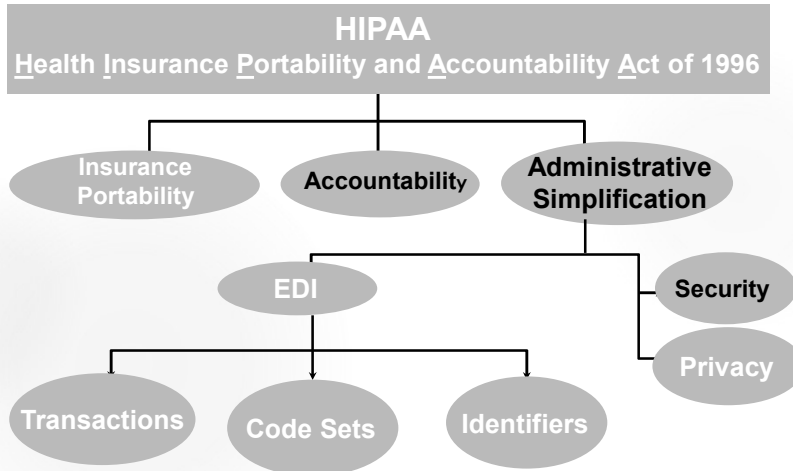


# 2020 HCCA Board & Audit Committee Compliance Conference

HEALTHCARE PRIVACY & SECURITY  
FEBRUARY 25, 2020

1




2



2

**Enforcement**


3

-  Office for Civil Rights (OCR) - Privacy and Security Civil complaints
-  Centers for Medicare and Medicaid Services (CMS) - Transactions and code sets
-  Department of Justice (DOJ) - Privacy Criminal complaints


3

**Security and Privacy**

4



Privacy rule identifies **what** is to be protected and outlines the individual's rights to control access to their PHI



The security rule defines **how** to protect PHI in electronic form

The security rule only applies to PHI maintained or transmitted in electronic form, called ePHI

4

## 6 Questions for Board Members and Senior Leaders

5

1. Healthcare Organizations, Vendors and Contractors--who has the ultimate accountability for the data?
2. HITRUST certification-what is it and what does it mean?
3. Why is there value in having the Privacy Officer participate in regularly scheduled meetings with Board Members and Senior Leaders?
4. What can be learned from OCR investigations and settlements?
5. What are ways to demonstrate the value of privacy and IT security resources?
6. What are some leading IT Security risks?

5

### 1. Healthcare Organizations, Vendors and Contractors—who has the ultimate accountability for the data?

6

- a) A Business Associate ("BA") is accountable to "The HIPAA Rules"
- b) A Business Associate Agreement defines how PHI will be safeguarded and aligned with the healthcare organization's policies and procedures
- c) The obligations of BA sub-contractors
- d) Ultimately, the custodian of the PHI is the healthcare organization and thus, has the ultimate accountability

6

FOR IMMEDIATE RELEASE  
December 4, 2018  
Contact: HHS Press Office  
202-690-6343  
[media@hhs.gov](mailto:media@hhs.gov)

7

## Florida contractor physicians' group shares protected health information with unknown vendor without a business associate agreement

*"OCR's investigation revealed that Advanced Care Hospitalists PL never entered into a business associate agreement with the individual providing medical billing services to ACH, as required by HIPAA and failed to adopt any policy requiring business associate agreements until April 2014."*

7

## Board Questions

8

- ▶ How do we monitor our Business Associates?
- ▶ Do we request documentation as evidence that Business Associates can adequately safeguard our data?
- ▶ What happens when our Business Associate does not safeguard our data and is responsible for a data breach?

8

## 2. What is HITRUST?

9

- ▶ HITRUST – abbreviation for the **Health Information Trust Alliance**
- ▶ HITRUST – refers to the Common Security Framework ("CSF") for assessment of controls and processes
- ▶ Validated Assessor submits assessment to HITRUST Alliance for review and certification
- ▶ Application-based certification (Scope)
- ▶ Up to 1800 control requirements scored on 5 elements:
  - Policy
  - Control
  - Proof of control
  - Measure of performance
  - Improvement on the measure
- ▶ Certification is good for 2 years
  - Re-certification focus is how the program is measured, managed and improved.

9

## Board Questions

10

How does our organization measure the following:

- ▶ The environment is secured;
- ▶ Vigilant assessment of what might occur in the evolving security landscape;
- ▶ Implementation of appropriate measures to detect and react to existing and emerging threats;
- ▶ Resilience in the ability to recover operations when a security incident does occur.

10

### 3. Why is there value in having the Privacy Officer participate in regularly scheduled meetings with Board Members and Senior Leaders?

11

- a) Privacy Breaches can impact hospital operations, regulatory non-compliance, reputation in the community and the fiduciary responsibility of Board Members and Senior Leaders
- b) Information can be provided regarding regulatory investigations, breach notification incidents and how these matters are being addressed
- c) Information can be provided regarding how the organization is addressing changing technical standards, changing regulatory requirements, emerging technologies, and the ever changing workforce

11

FOR IMMEDIATE RELEASE  
 May 6, 2019  
 Contact: HHS Press Office  
 202-690-6343  
[media@hhs.gov](mailto:media@hhs.gov)

12

## Tennessee diagnostic medical imaging services company pays \$3,000,000 to settle breach exposing over 300,000 patients' protected health information

*"Covered entities must respond to suspected and known security incidents with the seriousness they are due, especially after being notified by two law enforcement agencies of a problem," said OCR Director Roger Severino. "Neglecting to have a comprehensive, enterprise-wide risk analysis, as illustrated by this case, is a recipe for failure."*

12

13

## Board Question

- ▶ How does the Board obtain information regarding privacy regulatory matters that could impact the organization?

13

14

## 4. What can be learned from OCR investigations and settlements?

- ▶ Since April 2003:
  - ▶ 225,378 HIPAA complaints received
  - ▶ 993 compliance reviews
  - ▶ 99% of cases resolved (222,175).
    - ▶ 27,604 changes, corrective actions, and technical assistance
    - ▶ 40,882 – OCR provided technical assistance
    - ▶ 12,094 - no violation
    - ▶ 141,595 – Not an eligible case for enforcement
  - ▶ Approximately \$111 million in settlements (73 cases)

14

## Issue Types 2015-2018

15

Year	Issue 1	Issue 2	Issue 3	Issue 4	Issue 5
2018	Impermissible Uses & Disclosures	Safeguards	Administrative Safeguards	Access	Technical Safeguards
2017	Impermissible Uses & Disclosures	Safeguards	Administrative Safeguards	Access	Technical Safeguards
2016	Access	Impermissible Uses & Disclosures	Safeguards	Administrative Safeguards	Technical Safeguards
2015	Impermissible Uses & Disclosures	Safeguards	Administrative Safeguards	Access	Technical Safeguards

15

## Board Questions

16

- ▶ What are we doing to make sure we do not have these issues?
  - ▶ Privacy and Security program structure
  - ▶ Look at the biggest risk for breach
  - ▶ Always ask if a Security Risk Assessment has been done.

16



## 5. What are ways to assess the value of privacy and IT security resources? 17

- a) Review data regarding:
  - i. Privacy and IT Security education
  - ii. Number of Privacy investigations
  - iii. Number and types of breach notification incidents
- b) Examine OCR Resolution Agreements which reveal previous regulatory fines and penalties associated with data breach events
- c) Explore the organizational costs associated with obtaining additional resources to manage a major data breach incident

17

18

## Board Notification -

- ▶ When does Board notification occur?
  - ▶ Breaches of 500 individuals or more
  - ▶ Internet posting required
  - ▶ DOJ involvement
  - ▶ OCR investigation v. letter
  - ▶ Lawsuit potential

18

## 6. Leading IT Security Risks 19

### Phishing:

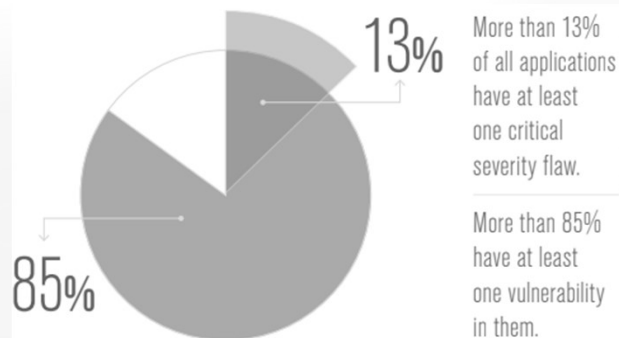


19

## Unpatched Assets: 20

*"Cybersecurity: One in three breaches are caused by unpatched vulnerabilities"*

ZDNet June 4, 2019



20

21

## Board Questions

- ▶ Is workforce training being done?
- ▶ Is there data to evidence improvement?
- ▶ Is there a process to monitor evolving threats?
- ▶ Are there secondary protections?
- ▶ If there is a breach...
  - ▶ How would we know?
  - ▶ How long would it take to find out?
  - ▶ Do we have a response plan?

21

22

## Key Performance Measures

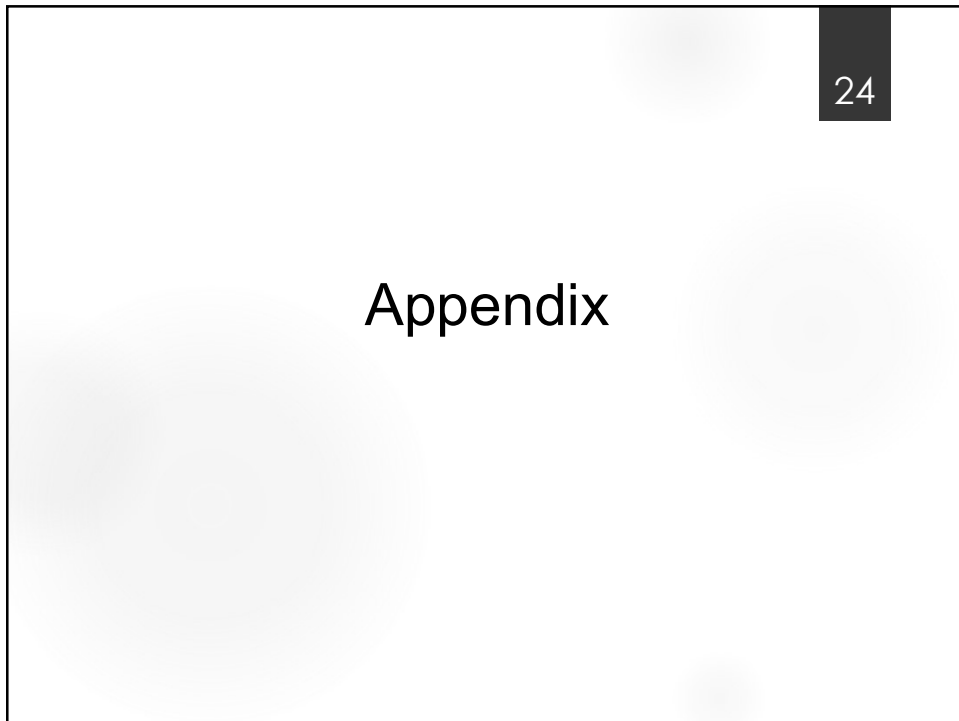
1. Security Management Visibility
2. Kill Chain Coverage
3. Incident Response Metrics
4. Quarterly Security Metrics
5. Constituent Engagement

22



23

23



24

24

25

## Board Privacy Risk Questions

1. Is there a process for reviewing information leaving the organization to determine whether it is PHI?
2. What is the current status of our Privacy Program
3. What were the results of the last Privacy Risk Assessment?
4. How many Reportable Breaches have we had?
  - ▶ What trends have been observed?
5. Have the sources of PHI leaving this organization been identified and what has been done to safeguard them?

25

26

## Board Security Risk Questions

1. Is there a process to terminate access of separated employees and contractors?
  - ▶ Has that been tested?
2. What were the results of the last Security risk assessment?
  - ▶ Has a plan been developed to address identified risks?

26

## Board Security Risk Questions (cont.)

3. Have we identified all the ways that an unauthorized person could get access to our data?
4. What is our level of encryption?
  - ▶ Link to PHI leaving the organization
5. What is the current status of our Security Program?