

# HIPAA BASICS

*Top privacy & security priorities*  
for compliance with federal regulations

**MyHIPAA Guide**  
**2022**

*Presented by Diane Evans & Michelle  
Bermea*

# AGENDA

## HIPAA Overview

- What Is Private Information?
- What Is Required Under Federal Regulation?

## Administrative Safeguards

## Technical Safeguards

- Do This First List

## Physical Safeguards

## Questions & Contact Us

# WHAT IS HIPAA?

*privacy & security of information*

- ❑ HIPAA is a federal law that protects the private information of those served by healthcare providers - which includes I/DD agencies
- ❑ Through federal regulations & requirements, HIPAA provides a baseline security plan to manage individuals' data and protect their privacy

**40% PRIVACY**

**60% DATA SECURITY**

# WHAT IS PRIVATE INFORMATION

*what information is considered protected?*

- Private or **protected health information (PHI)** is any information that is individually identifiable
- This includes:
  - ◆ Names
  - ◆ Addresses
  - ◆ Financial & Insurance Information
  - ◆ Medications
  - ◆ Diagnoses
  - ◆ Photographs & Videos

# Why protect information?

- it's the law
- to uphold the trust of those served
- HIPAA incentivizes compliance efforts

With good-faith compliance efforts:

→ Maximum fine of \$25k per violation, per year

Without any demonstrable compliance:

→ **\$1.7 million maximum per violation, per year**

[\(view 2019 update\)](#)

**Note:** \$1.7m reflects inflationary increase

# THE 3 RULES OF HIPAA

*The breakdown of privacy and security regulations*

**01**

---

**The Privacy Rule**

**02**

---

**The Security Rule**

**03**

---

**The Breach Reporting Rule**

# THE SECURITY RULE

*Three categories of required safeguards*

The HIPAA **Security Rule** establishes the standards for protecting PHI that is created, received, used or maintained, requiring the following safeguards:

## ADMINISTRATIVE

- Policies & Procedures
- Risk Assessment
- Staff Training
- Forms and Agreements
- Breach Reporting & Breach Response
- Security Management

## TECHNICAL

- Audit & Monitoring Controls
- Login Credentials & Passwords
- Network Security
- IT Systems Maintenance
- Information Systems
- IT Assets & Devices

## PHYSICAL

- Facility Access Controls
- Workstation Security
- Building Security
- Storage of Paper Documentation of PHI

# ADMINISTRATIVE SAFEGUARDS

*Lay the foundation for an effective privacy & security framework*

1. Privacy & Security Policies and Procedures

2. Risk Assessment and Risk Mitigation

3. Staff Training

4. Forms and Agreements  
Including Notice of Privacy Practices

5. Breach Reporting and Breach Response

6. Appoint a Compliance Officer



# POLICIES AND PROCEDURES

*A critical HIPAA requirement*

A documented set of **Privacy & Security Policies and Procedures** is a requirement under HIPAA.

These Policies and Procedures serve as the cornerstone for any organization's HIPAA compliance program, establishing:

- Expectations and accepted behavior
- Prohibitions and limits
- Procedures to protect private information and maintain security
- Disciplinary consequences for violating any policy

Administration

Employee Responsibilities

Privacy Rights

Building Security

IT Security

Network Access

Identification and Authentication

Access Controls

Audit and Monitoring

Data Integrity

Change Management

PRIVACY & SECURITY  
POLICIES AND  
PROCEDURES

REQUIRED  
CATEGORIES

Records Retention

Contingency Plan

Emergency Operations Plan

Emergency Access Plan

Risk Assessment

Security Awareness Training

Sanctions

Exclusion Screenings

Breach Notification

Breach Response

Business Associates

# RISK ASSESSMENT

*A critical HIPAA requirement*

HIPAA requires **enterprise-wide** routine assessment of risks to *all* private information in *all* potential locations where it is created, maintained, received, and/or transmitted

Risk assessment findings will become the foundation for an organization's compliance program

## 1. PREPARE

Create documentation processes that will guide managers in identifying risks while assessing the security of all places where private information may be accessible

## 2. ASSIGN

Give specific duties to managers to evaluate their respective departments for risk and set deadlines for their completion

## 3. CORRECT

Address [bad practices](#) that pose high risks and make corrections to the extent possible and that have the highest impact on security

# RISK ASSESSMENT

*Seven categories to assess privacy & security vulnerabilities*

- 1. Organizational & Administrative Foundation
- 2. Compliance Management & Oversight
- 3. Staff Training & Awareness
- 4. Physical Safeguards
- 5. Technical Safeguards
- 6. Breach Response & Prevention
- 7. Enforcement

# PRIORITY ADMINISTRATIVE DUTIES

*Do this first to get started*

## → ESTABLISH MANAGEMENT

Appoint a Compliance Officer and assign privacy and security duties appropriately  
Ensure adequate resources and budget are assigned to privacy and security efforts

## → EXECUTE PRIVACY NOTICES

Prioritize the rights of the individuals served by communicating them via a Notice of Privacy Practices  
Establish a procedure for staff to follow and a template form for individuals to sign for the release of information

## → SET REPORTING PROCESSES

Put breach reporting chain of command in place and communicate to staff their duty to report incidents  
Establish breach response and investigation procedures

# TECHNICAL SAFEGUARDS

*Be prepared to face new emerging threats to cybersecurity*

U.S. Department of Homeland Security has issued new [“Shields Up” Alert](#) in response to new threats from Russia:

*“Every organization—large and small—must be prepared to respond to disruptive cyber incidents.”*

## WHAT’S AT RISK?

### → OPERATIONAL UNCERTAINTY

All it takes is one cyber attack to disrupt operations, costing the agency time, resources, and money, and potentially inflict irreparable damage

### → OUTDATED or MISMANAGED CYBERSECURITY can result in:

- Identity theft & fraud, targeting individuals served
- Ransomware
- Schemes soliciting payment to bad actors disguised as known vendors or contractors
- Lasting reputational and/or financial harm

# PRIORITY TECHNICAL DUTIES

*Do this first to get started*

From the White House: [“What We Urge You to Do Now” Memo](#), FIVE BEST PRACTICES to do first to protect your cybersecurity

1. DATA  
BACKUP
2. UPDATE  
SOFTWARE &  
APPLY  
PATCHES
3. TEST  
INCIDENT  
RESPONSE  
PLANS
4. SEGMENT  
NETWORKS
5. CHECK YOUR  
IT TEAM'S  
WORK!

**NOTE:** In addition to these five best practices, the White House also recommends the following:

- multi-factor authentication
- endpoint detection & response
- encryption
- a skilled, empowered security team

# DO-THIS FIRST

# DATA

# BACKUP

## TO DO:

- ❑ Back-up data, system images, and configurations regularly  
*Data includes protected health information!*
- ❑ Regularly test your backups to ensure they are maintained offline  
*And not connected to operational networks*

**Remember:** if backups are connected to networks, a hacking could result in a loss of that data, too!



# DO-THIS FIRST UPDATE SOFTWARE & APPLY PATCHES

## TO DO:

- ❑ Maintain the security of operating systems, applications, and firmware through regular software updates
- ❑ Establish a centralized patch management system to ensure timely corrections and updates

Check to see if you have outdated, unsupported software or systems. Make plans to migrate to new when possible.

# DO-THIS FIRST

# TEST INCIDENT RESPONSE PLANS

## TO DO:

- ❑ First, develop an incident response plan if you do not already have one
- ❑ Focus on how you would maintain operations in the event of a systems failure
- ❑ Test your plan! Identify any gaps & inadequacies

# DO-THIS FIRST SEGMENT NETWORKS

## TO DO:

- ❑ If you have multiple facilities, segregate networks to the extent possible
- ❑ Create “Guest” networks so individuals served and/or the public are never connected to your business operations network
- ❑ When not in use, turn off connected devices (i.e., fax machines, copiers) to avoid network infiltration

# DO-THIS FIRST CHECK YOUR IT TEAM'S WORK

## TO DO:

- ❑ Use a third-party penetration tester to check the security & defenses of your IT systems
- ❑ Ask for reports on software updates, firewall effectiveness, access controls, data backups, and latest best practices
- ❑ Set expectations, based on pen test results and risk assessment findings

# PRIORITY PHYSICAL SECURITY

*Do this first to get started*

Aim for **situational awareness** amongst staff; be aware of their surroundings and how they are securing information!

## POINTS OF ENTRY

- Single-door access
- Visitor procedures, including check-in/badges
- Access controls via locks, keys, keycards, etc.

## SECURE WORKSTATIONS

- Clean desk policy
- Screen locks, password-protected
- No sharing of passwords

## PHYSICAL DOCUMENTS

- Storage
- Transportation of documentation
- Destruction & disposal of paper documents
- Mailboxes, fax machines, daily use

# BENCHMARKS

*For successful HIPAA compliance management*



Compliance starts from the top down and everyone in the organization understands protecting privacy and security is their responsibility



Expectations and duties are clearly documented; clearly communicated for all staff to understand their privacy and security responsibilities; and, enforced



Active, preemptive management and planning to stay on top of emerging risks and threats

# QUESTIONS?



[devans@myhipaaguide.com](mailto:devans@myhipaaguide.com)



[www.myhipaaguide.com](http://www.myhipaaguide.com)



MyHIPAA  
GUIDE.COM