# Focusing on HIPAA

## What?

Health Insurance Portability and Accountability Act;

a federal law that required the government to create nationwide standards to protect patient health information

## Why?

HIPAA was originally developed to:

- *Help modernize the flow* of healthcare information
- Solve issues regarding healthcare coverage and to *provide continuing healthcare* for people in-between jobs
- *Reduce healthcare fraud and protect patient information*
- *Update standard guidelines* of managing healthcare data and personal information

## Who?

Healthcare Professionals, Covered Entities, Business Associates, and Patients

**Protected Health Information (PHI)**

Any information that is personally identifiable to the patient.

**Electronic Protected Health Information (ePHI)**

Any PHI that is produced, saved, transferred in electronic form.

**Covered Entity**

Any health care provider, health insurance plan and clearinghouse required to follow HIPAA.

**Business Associate**

any organization that may have been hired to handle PHI on behalf of a CE or another business associate.

# Rules and Regulations

**Privacy Rule** addresses the use and disclosure of individuals' health information by entities subject to HIPAA. This rule also contains standards for individuals' rights to understand and control how their health information is used. The main objective of the Privacy Rule is to ensure PHI is properly protected while still allowing the flow of health information to promote high quality health care.

**Security Rule** safeguards protected health information (PHI), the Security Rule protects a subset of information covered by the Privacy Rule. This subset is all individually identifiable health information a covered entity creates, receives, maintains, or transmits in electronic form. This information is called "electronic protected health information" (e-PHI). The Security Rule does not apply to PHI transmitted orally or in writing.

**Enforcement Rule** provides standards for enforcing all rules within HIPAA. The regulation within this rule establishes how HHS regulators will determine liability and calculate fines for health-care providers found to have violated any of the HIPAA rules following an investigation and administrative hearing. Privacy complaints are investigated by regulators from the HHS Office for Civil Rights.

**Omnibus Rule** implements several provisions of the Hitech Act that strengthen the privacy and security for health information established within HIPAA which led to finalizing the next rule we will discuss. The Omnibus Rule was necessary because while the 2009 Health Information for Economic and Clinical Health (HITECH) Act addressed privacy, the requirements for notifying patients of data breaches had to be updated. This rule also covers the liability of business associates, such as technology providers, and business associate agreements (BAAs).

**Breach Notification Rule** requires Covered Entities and their Business Associates to provide notification for any breach of unsecured PHI. Following a breach of unsecured protected health information, covered entities must provide notification of the breach to affected individuals, the Secretary, and, in certain circumstances, to the media. In addition, business associates must notify covered entities if a breach occurs at or by the business associate.

# SAFEGUARDS

## Administrative

- ASSIGN OR DELEGATE SECURITY RESPONSIBILITY – CHIEF SECURITY OFFICER
- TRAIN EMPLOYEES ON SECURITY PRINCIPLES AND PRACTICE POLICIES/PROCEDURES
- TERMINATE ACCESS TO INFORMATION SYSTEMS
- REPORT AND RESPOND TO SECURITY BREACHES

## Physical

- LIMIT PHYSICAL ACCESS TO INFORMATION SYSTEMS
- PREVENT INAPPROPRIATE VIEWING OF ePHI ON COMPUTERS
- REMOVE ePHI FROM COMPUTERS BEFORE DISPOSING OR REUSING
- BACK UP ePHI PROPERLY

## Technical

- PROVIDE EMPLOYEES WITH UNIQUE ACCESS IDENTIFIERS
- PROCESSES FOR ACCESSING ePHI DURING AN EMERGENCY
- ENCRYPTING ePHI DURING TRANSMISSION
- AUTOMATICALLY LOG OFF WORK-STATIONS

## security risk assessment

- Gap Identification and Remediation
- Policies, Procedures and Training
- Employee Attestation and Tracking
- Business Associate Management
- Incident Management

## privacy risk assessment

| 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|
| **Define Flow Of PHI Within Your Practice** | **Identify Flaws Within Your Flow Of PHI And Possible Threats** | **Analyze HIPAA Compliance Risk Level And The Potential Impact** | **Implement Security Measures Based On Risk Assessment** | **Repeat Step 4 for ALL Identified Risks** |
| Identify where PHI enters your practice | Identify vulnerabilities or flaws within your practice and procedures | Determine likelyhood of risk occuring within your practice | Document and understand your practice risks | After identifying high risks and security measures to resolve, repeat for medium and low risks |
| Identify what happens with PHI as it flows within your practice | Identify potential threats for a breach by a person or within software | Determine the impact that the risks could have on your practice | Identify the security measures to resolve the risk | Document every action made during this process show you have completed a through risk analysis |
| Identify how and when PHI is transferred to other practices | Identify risks that could potentially impact your practice | Assign each threat a high, medium, or low risk level | Implement security measures within 30 days of identifying the risk | Repeat this entire process as often as desired to ensure your practice is staying HIPAA compliant |

# notice of privacy practices

**CONTENT MUST INCLUDE**

- How the covered entity may use and disclose protected health information about an individual
- The individual's rights with respect to the information and how the individual may exercise these rights, including how the individual may complain to the covered entity
- The covered entity's legal duties with respect to the information, including a statement that the covered entity is required by law to maintain the privacy of protected health information
- Whom individuals can contact for further information about the covered entity's privacy policies

- NOTICE MUST HAVE EFFECTIVE DATE
- THE FOLLOWING STATEMENT: "THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY."
- PRACTICE CONTACT INFO
- CHIEF SECURITY OFFICER INFORMATION

NOTICE MUST BE AVAILABLE TO ANYONE WHO ASKS FOR IT

NOTICE MUST BE POSTED IN PROMINENT LOCATION WITHIN THE PRACTICE

NOTICE MUST BE POSTED TO WEBSITE

MUST PROVIDE THE NOTICE TO INDIVIDUAL ON FIRST DATE OF SERVICE

OBTAIN WRITTEN ACKNOWLEDGEMENT OF RECEIPT OF NOTICE

MUST PROVIDE AUTOMATICALLY IF FIRST COMMUNICATION IS VIATHE INTERNET, EMAIL, OR ELECTRONIC

EMAIL NOTICE IF INDIVIDUAL AGREES TO RECEIVE ELECTRONICALLY

FOLLOW ALL OF THESE SAME STEPS ANYTIME THE NPP HAS BEEN REVISED

## *Preventing Incidental Disclosure*

- Keep patient information to a minimum while discussing on phone
- Reduce unnecessary incidental disclosures during check-in process
- Do not discuss patients in public areas
- Keep voices low when discussing patient issues
- Position workstations away from the patient

*no written authorization required*

- treatment
- payment
- operations

# Minimum Necessary

*need to know*

### Implementing the Minimum Necessary Standard

1. Determine which information is needed for different roles and responsibilities
2. Make sure employees receive training on the types of information they are permitted to access and share; with or without authorization
3. Set up alerts and notify the compliance team or offices of unauthorized attempts to access PHI
4. Document any actions taken in response to cases of unauthorized access or accessing more information than is necessary and the sanctions that have been applied as a result.

## HIPAA *filing a complaint*

**Complaints, Violations, Consequences**

www.hhs.gov

## Common HIPAA Violations by Employee

- Removing PHI from the Office
- Leaving Files Unattended
- Not signing Off of Electronic Devices
- Emailing ePHI to Personal Emails which are non-HIPAA Compliant
- No Authorization on File for Release
- Releasing PHI for purposes other than treatment, payment or healthcare operations
- Authorization expired
- Must specify types of PHI on Authorization
- Unaware of Minimum Necessary Standards
- Unaware of Policies, Procedures, HIPAA Violations and the Consequences

## Top 10 HIPAA Violations

1. Snooping on Healthcare Records
2. Failure to Perform Risk Analysis
3. Failure to Manage Security Risks
4. Failure to Enter into a HIPAA Compliant BAA
5. Insufficient ePHI Access Controls
6. Failure to Use Encryption to Safeguard Portable Devices
7. Failure to Issue Breach Notification
8. Impermissible Disclosure of PHI
9. Improper Disposal of PHI after Retention Period Expired
10. Denying Patients Access to Health Records

**UNAWARE OF THE HIPAA VIOLATION**

**REASONABLE CAUSE THAT THE CE KNEW OF THE VIOLATION**

**WILLFUL NEGLECT OF HIPAA RULES WITH VIOLATION CORRECTED WITHIN 30 DAYS**

**WILLFUL NEGLECT OF HIPAA RULES AND ZERO EFFORT TO CORRECT THE VIOLATION WITHIN 30 DAYS**