



HIPAA RULES FOR BEHAVIORAL HEALTH CARE PROVIDERS

COMPLIANCE EDUCATION

PRESENTED BY
PAUL R. HALES, J.D.





Behavioral Health HIPAA Compliance

PAUL R. HALES

ATTORNEY AT LAW

Health Information – HIPAA



The HIPAA E-Tool®

Protecting Patient Privacy is Our Job®

Legal Education – Not Legal Advice

AttorneyHales.com

[@hipaaetool](https://twitter.com/hipaaetool)

[314-534-3534](tel:314-534-3534)

PaulHales@AttorneyHales.com





Behavioral Health HIPAA Compliance

Behavioral Health Information Is Protected Health Information PHI – Subject to The HIPAA Rules





Behavioral Health HIPAA Compliance

The HIPAA Rules

Are Easy to Follow

Step-by-Step

When You Know the Steps





Behavioral Health HIPAA Compliance

The HIPAA Rules

Are a Blueprint

To Protect Patients

and Your Organization





Behavioral Health HIPAA Compliance

May 1, 2024

The New
York Times



[June 2023 OCR
Cybersecurity
Newsletter](#)

Senators Slam UnitedHealth's C.E.O. Over Cyberattack

Mr. Wyden said that UnitedHealth had failed to enforce the most basic kind of cybersecurity measure — so-called multifactor authentication.





Behavioral Health HIPAA Compliance

HHS Office for Civil Rights Opens Investigation of Change Healthcare Cyberattack

OCR's investigation of Change Healthcare and UHG will focus on whether a breach of protected health information occurred and Change Healthcare's and UHG's compliance with the HIPAA Rules.





Behavioral Health HIPAA Compliance

Tracking Technologies

Kaiser Permanente Notifying 13.4 Million of Tracker Breach

Incident Involves Health Plans' Prior Use of Online Tech in Websites, Mobile Apps

Kaiser Breach is the Largest So Far this Year

According to TechCrunch, the patient information compromised includes

- names and IP addresses
- information that could indicate if members were signed into a Kaiser Permanente account or service
- how members “interacted with and navigated through the website and mobile applications, and search terms used in the health encyclopedia.”





Behavioral Health HIPAA Compliance

What Are We Going to Cover?

Alerts – New HIPAA & SUD Rules – Medical Identity Theft

1. What is HIPAA?
 - A. HIPAA Law & The HIPAA Rules
2. Who must comply with HIPAA?
4. HIPAA Compliance Basics
 - A. Accountability: Responsibility & Delegation of Authority
 - B. Risk Analysis & Risk Management
 - C. Policies – Procedures – Training
5. Common HIPAA Violations
6. HIPAA Compliance is a Process
7. Questions and Discussion





Behavioral Health HIPAA Compliance

ALERT

2024 – SIGNIFICANT MODIFICATIONS TO HIPAA PRIVACY RULE & PART 2 RULE – SUBSTANCE USE DISORDER CONFIDENTIALITY





Behavioral Health HIPAA Compliance

Significant HIPAA Privacy Rule Modifications

HIPAA Privacy Rule to Support Reproductive Health Care Privacy

Effective Date: June 25, 2024

Compliance Date: December 22, 2024

Despite its name, the Final Rule contains two other significant Privacy Rule modifications; one modifies the Notice of Privacy Practices (NPP), and the second coordinates Part 2 substance use confidentiality with HIPAA.

Handout 2 – Fact Sheet 2024 Privacy Rule Modification





Behavioral Health HIPAA Compliance

Significant Part 2 Modifications

Substance Abuse Treatment and HIPAA are Better Aligned

Effective Date: April 16, 2024

Final Compliance Date: February 16, 2026

The new rule modifies the Confidentiality of Substance Use Disorder Patient Records regulations - commonly called 42 CFR Part 2 or simply Part 2 to be better aligned with HIPAA.

Promote care coordination & Reduce HIPAA & Part 2 Conflicts

Handouts 3 & 4 - 2024 Modifications & Fact Sheet 42 CFR Part 2 Final Rule





Behavioral Health HIPAA Compliance

The HIPAA Rules

Are Easy to Follow

Step-by-Step

When You Know the Steps

How to Find the Steps





Behavioral Health HIPAA Compliance

Significant Part 2 Modifications

The HIPAA E-Tool
Search Box



The screenshot shows the interface of 'The HIPAA E-Tool®'. At the top, there is a navigation bar with a home icon and the text 'The HIPAA E-Tool®' and 'HIPAA Compliant Organization'. Below this is a search box containing the text 'subs'. A dropdown menu is open, displaying search results under two categories: 'Documents:' and 'Glossary:'. Under 'Documents:', there is one result: '2024 Alert 2024 Privacy Rule & Substance Use Disorder Confidentiality Modifications'. Under 'Glossary:', there are three results: 'Substance Use Disorder (SUD)', 'Substance Use Disorder Record Confidentiality', and 'Substance Use Disorder Records'. The 'Substance Use Disorder Records' result is highlighted in blue, and a white arrow points to it from the left. Below the search box, there are several menu items: 'Privacy Rule' (with a green circle), 'Security Rule' (with a green circle), and 'Substance Use Disorder Records' (with a green circle). To the right of the search box, there is a text area that says 'Enter words or phrases about HIPAA in the Search Box above for explanations and live links to applicable Policies, Procedure' and 'Below is a brief video about your Basic HIPAA Compliance I HIPAA training for new staff and annual training for all. Exp: screen.'





Behavioral Health HIPAA Compliance

Significant Part 2 Modifications

Substance Use Disorder Records

Substance Use Disorder Records are Records of the identity, diagnosis, prognosis, or treatment of any patient maintained in connection with the performance of any program or activity relating to Substance Use Disorder education, prevention, training, treatment, rehabilitation, or research conducted, regulated, or directly or indirectly assisted by any department or agency of the United States. 42 C.F.R. Part 2, commonly referred to as “Part 2,” regulates the Confidentiality of Substance Use Disorder (SUD) Patient Records. Part 2 is administered by the U.S. Department of Health & Human Services (HHS) through the Substance Abuse and Mental Health Services Administration (SAMHSA). Part 2 regulations governing the Confidentiality, Use and Disclosure of an Individual’s SUD are separate from and more strict than HIPAA Rules governing Protected Health Information (PHI). HHS’s Office for Civil Rights (OCR) administers the HIPAA Rules. On February 8, 2024, HHS, SAMHSA and OCR announced modifications of Part 2 SUD Confidentiality regulations to reduce conflicts between Part 2 and HIPAA and promote coordinated care. On April 16, 2024, OCR announced HIPAA Privacy Rule modifications that, among other things, coordinate with the earlier Part 2 modifications.

Legal Authorities and References: 42 U.S.C. 290dd-2, 89 FR 12472, 89 FR 32976

Documents: [2024 Alert 2024 Privacy Rule & Substance Use Disorder Confidentiality Modifications](#)





Behavioral Health HIPAA Compliance

🏠 The HIPAA E-Tool®
📍 Change Location ↻ Update Organization Information 👤 Logout

- 1 Introduction
- 2 Basic HIPAA Policies ●
- 3 Risk Analysis - Risk Management
- 4 Privacy Rule ●
- 5 Security Rule ●
- 6 Breach Notification Rule ●
- 7 Business Associates ●
- 8 HHS Aligned Audit Protocols
- 9 Enforcement Rule
- 10 Index/Glossary

Support Hotline
📞 1-800-570-5879
✉ info@hipaaetool.com

Protecting Patient Privacy Is Our Job®

The HIPAA E-Tool® licensed for exclusive use by
HIPAA Compliant Organization

© 2014-2024 ET&C Group LLC

[← Privacy Rule](#)

2024 Alert: 2024 Privacy Rule & Substance Use Disorder Confidentiality Modifications

Handout 3

PDF Document

The HIPAA E-Tool®
Privacy Rule

2024 Privacy Rule & Substance Use Disorder Confidentiality Modifications

Page 1 of 1

Part 2 and The HIPAA Privacy Rule

Part 2

42 C.F.R. Part 2, commonly referred to as "Part 2," regulates the Confidentiality of Substance Use Disorder (SUD) Patient Records. Part 2 is administered by the U.S. Department of Health & Human Services (HHS) through the Substance Abuse and Mental Health Services Administration (SAMHSA). Part 2 regulations governing the Confidentiality, Use and Disclosure of an Individual's SUD are separate from and more strict than HIPAA Rules governing Protected Health Information (PHI). HHS's Office for Civil Rights (OCR) administers the HIPAA Rules.

Background

Part 2 regulations were created in 1975 when no other national privacy and security standards for health information existed. They impose strict Confidentiality protections to help address concerns that discrimination and fear of prosecution deter people from seeking SUD treatment.

The HIPAA Privacy Rule establishing permitted and required Uses and Disclosures of Protected Health Information (PHI) became effective in 2003.

Inconsistencies in the two health privacy regulations blocked Health Care Providers from sharing SUD information. This prohibited integration of significant behavioral health information with other medical records to improve patient health outcomes.

In 2020, Congress passed legislation requiring HHS to align certain aspects of Part 2 with the HIPAA Privacy Rule.





Behavioral Health HIPAA Compliance



WESTERN REGIONAL CONFERENCE ON GAMBLING AND GAMING HEALTH AWARENESS

FOCUS ON THE FUTURE

Convention Special – 25% off
Scan to Sign up for Free Online Demo



The HIPAA E-Tool[®]





Behavioral Health HIPAA Compliance

ALERT

MEDICAL IDENTITY THEFT





Behavioral Health HIPAA Compliance

ALERT

Medical Identity Theft – Criminal Black Market

UNCLASSIFIED



FBI CYBER DIVISION

Private Industry Notification

PIN #: 140408-009

Cyber criminals are selling the information on the black market at a rate of **\$50 for each partial EHR**, compared to **\$1 for a stolen social security number or credit card number**. EHR can then be used to file fraudulent insurance claims, obtain prescription medication, and advance identity theft. EHR theft is also more difficult to detect, taking almost twice as long as normal identity theft.





Behavioral Health HIPAA Compliance

ALERT

Medical Identity Theft – Criminal Black Market



**FEDERAL TRADE COMMISSION
CONSUMER ADVICE**

What Is Medical Identity Theft?

Medical identity theft is when someone uses your personal information — like your name, Social Security number, health insurance account number or Medicare number — to see a doctor, get prescription drugs, buy medical devices, submit claims with your insurance provider, or get other medical care.

If the thief's health information is mixed with yours, it could affect the medical care you're able to get or the health insurance benefits you're able to use. It could also hurt your credit.





Behavioral Health HIPAA Compliance

ALERT

Medical Identity Theft – Criminal Black Market

PHI =





Medical Identity Theft – Criminal Black Market



HHS OIG Medical Identity Theft Video





Medical Identity Theft – Criminal Black Market



HHS OIG Medical Identity Theft Video





Medical Identity Theft – Criminal Black Market



Medical Identity Theft is the fastest growing form of Identity Theft





Behavioral Health HIPAA Compliance

ALERT

Medical Identity Theft – Criminal Black Market



Gary Cantrell

DEPUTY INSPECTOR GENERAL FOR INVESTIGATIONS

Only two things are needed for Medical Identity Theft:
Identity of a Patient – Identity of a Provider





Behavioral Health HIPAA Compliance

ALERT

Medical Identity Theft – Criminal Black Market

Criminals Attack People of All Ages & All Walks of Life

- Social Engineering
Clever Scripts & Messages
- Vishing
- Phishing






Behavioral Health HIPAA Compliance

ALERT

Medical Identity Theft – Criminal Black Market

Paul R. Hales

From: Microsoft account-security-noreply@accountprotectionmicrosoft.com
Sent: Monday, March 6, 2023 9:12 AM 
To: Paul Hales
Subject: Microsoft account security notification

Microsoft account

Your account is set to close on 5/5/2023

Dear Paul Hales,

Your account xxxxxxxxxxxx@xxxxxxxxxxxx.com is scheduled to be closed on 5/5/2023 due to account inactivity. Once your account is closed it will be deleted in accordance with the Microsoft Services Agreement. If you want to keep your account, just sign in between now and 5/5/2023. All your files, data and info will be just as you left them until then.

To learn more, click here <<https://go.microsoft.com/fwlink/?LinkId=2086738>> .

Thanks,

The Microsoft account team

Phishing





Behavioral Health HIPAA Compliance

ALERT

Medical Identity Theft – Criminal Black Market

Criminals Attack People of All Ages & All Walks of Life

- Social Engineering
Clever Scripts & Messages
- Vishing
- Phishing
- Smishing



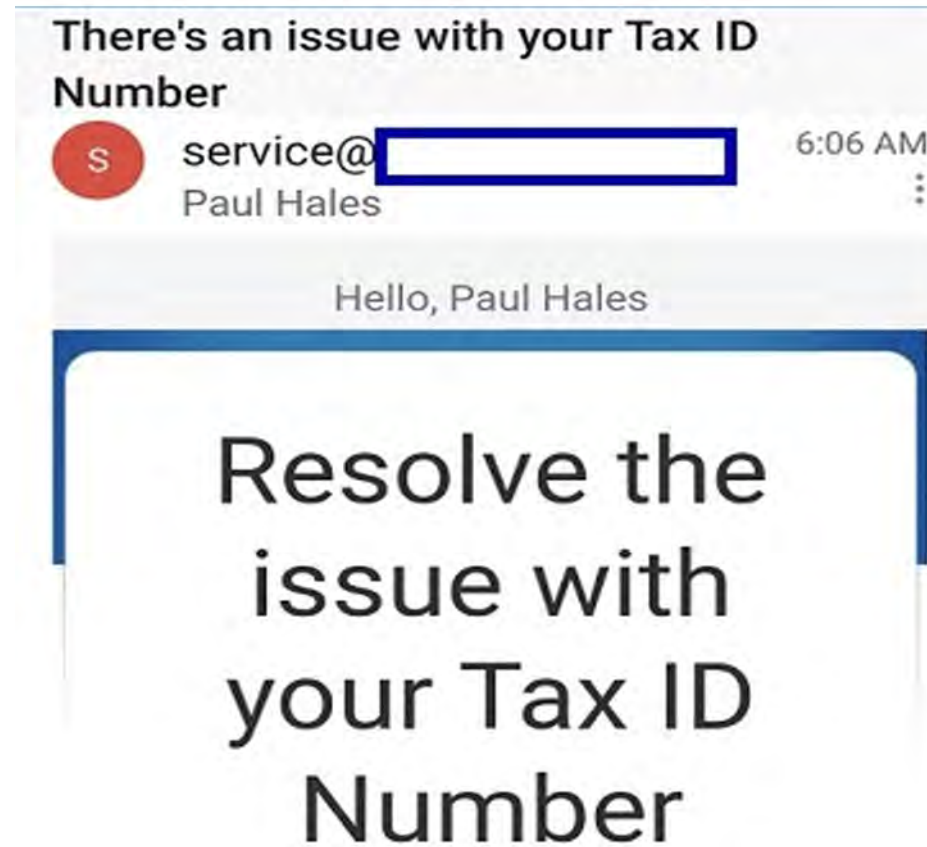


Behavioral Health HIPAA Compliance

ALERT

Medical Identity Theft – Criminal Black Market

Smishing





Behavioral Health HIPAA Compliance

ALERT

Medical Identity Theft – Criminal Black Market

Criminals Attack People of All Ages & All Walks of Life

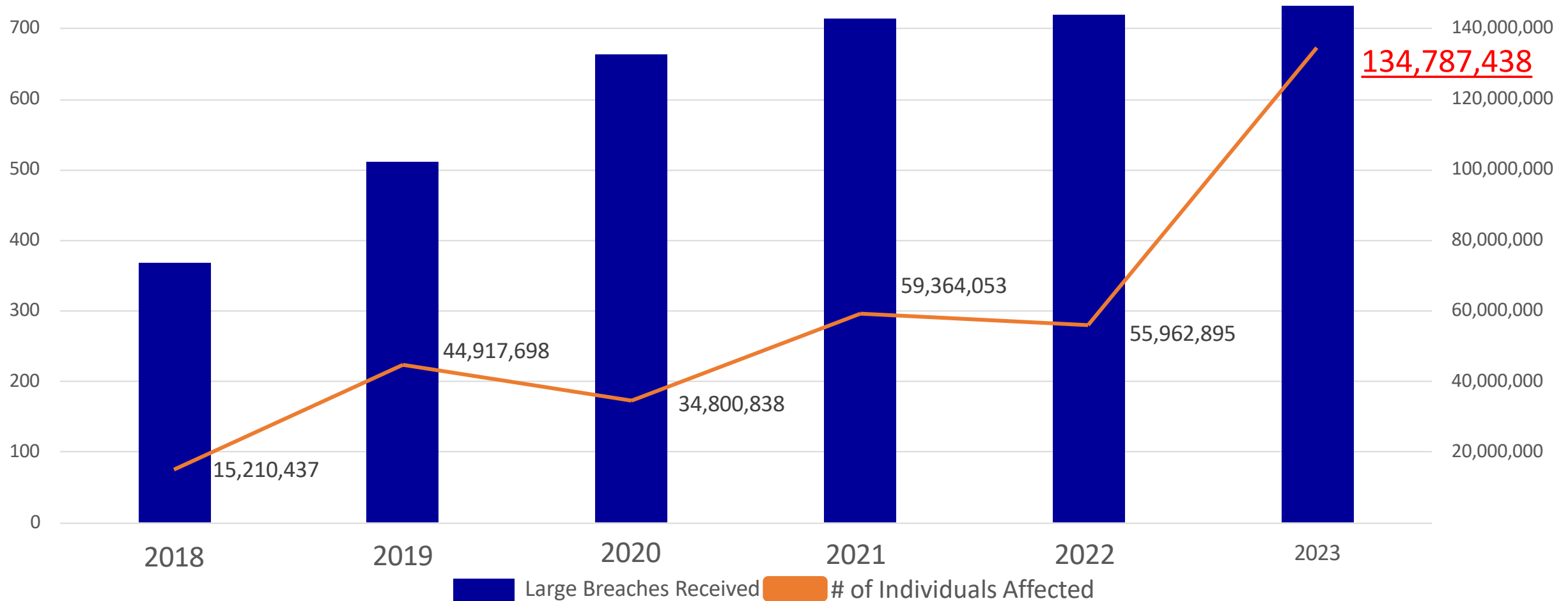
- Social Engineering
Clever Scripts & Messages
- Vishing
- Phishing
- Smishing
- Quishing – Malicious QR Codes – FBI





Behavioral Health HIPAA Compliance

Large Breaches Reported to OCR and # of Individuals Affected 2018 - 2023





Behavioral Health HIPAA Compliance

ALERT

INCREASED ENFORCEMENT OF HEALTH INFORMATION PRIVACY LAWS





Behavioral Health HIPAA Compliance

2023 - Health Privacy Enforcement got Serious - More to Come

HIPAA and OCR are not the only enforcers of Health Information Privacy Regulations

Newly active, aggressive enforcers are here now *

- Federal Trade Commission (FTC)
- Private Plaintiffs and Class Action Lawsuits
- State Regulators and Attorneys General

* Handout 5 – Health Information Privacy Enforcement Suddenly Got Serious





Behavioral Health HIPAA Compliance

WHAT IS HIPAA?

*HIPAA LAW
THE HIPAA RULES*

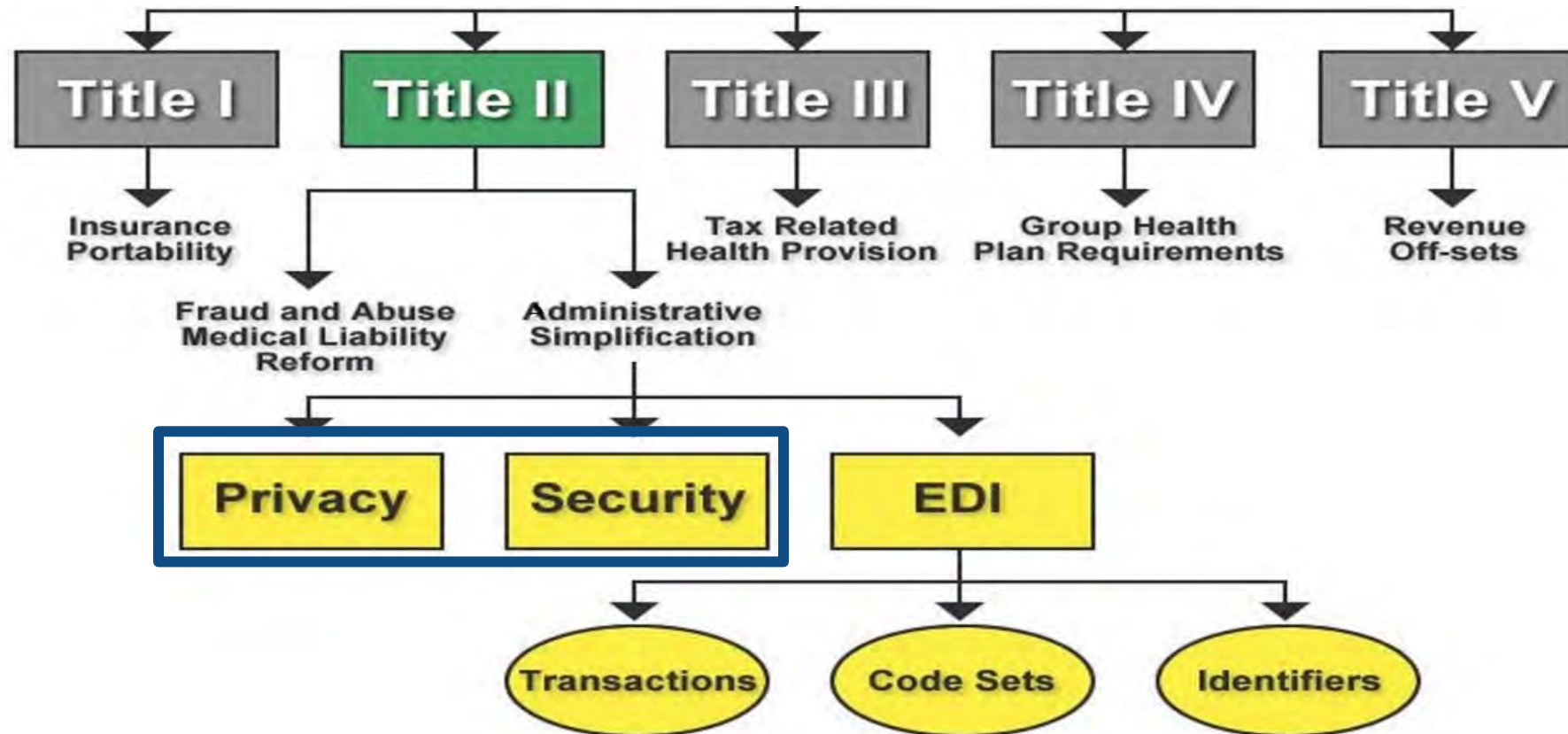




Behavioral Health HIPAA Compliance

HIPAA LAW AND THE HIPAA RULES

H e a l t h I n s u r a n c e P o r t a b i l i t y a n d A c c o u n t a b i l i t y A c t o f 1 9 9 6





Behavioral Health HIPAA Compliance

HIPAA LAW AND THE HIPAA RULES

H e a l t h I n s u r a n c e P o r t a b i l i t y a n d A c c o u n t a b i l i t y A c t o f 1 9 9 6

Directs the Secretary of the U.S. Department of Health and Human Services (HHS) to develop and implement regulations to protect the **Privacy** and **Security** of individually identifiable health information

The HIPAA Rules

HHS Office for Civil Rights (OCR) administers and enforces HIPAA Rules

Some violations of HIPAA Rules carry criminal penalties

The U.S. Department of Justice (DOJ) enforces HIPAA criminal violations





Behavioral Health HIPAA Compliance

HIPAA LAW AND THE HIPAA RULES

**Health Insurance Portability and Accountability Act of 1996
Health Information Technology for Economic and Clinical Health Act**

The HIPAA Rules

1. Privacy Rule ← *The Fundamental Rule*
2. Security Rule
3. Breach Notification Rule
4. Enforcement Rule





Behavioral Health HIPAA Compliance

HIPAA LAW AND THE HIPAA RULES

Health Insurance Portability and Accountability Act of 1996 Health Information Technology for Economic and Clinical Health Act

The Privacy Rule is made up of:

- **Standards** (rules, conditions or requirements with respect to the privacy of Protected Health Information (PHI) and
- **Implementation Specifications** (specific requirements or instructions for implementing a Standard)

Privacy Rule Standards cover three topics:

1. **Uses and Disclosures of Protected Health Information (PHI)**
2. **PHI Privacy Rights of an Individual**
3. **Administrative Technical and Physical Safeguards to protect PHI**





Behavioral Health HIPAA Compliance

HIPAA LAW AND THE HIPAA RULES

Health Insurance Portability and Accountability Act of 1996 Health Information Technology for Economic and Clinical Health Act

The Privacy Rule is the Fundamental Rule

Security Rule

Covered entities and business associates must ... protect against any reasonably anticipated uses or disclosures of electronic protected health information *that are not permitted or required under the Privacy Rule.*

45 CFR 164.306(a)(3)

Breach Notification Rule

Breach means the acquisition, access, use, or disclosure of protected health information *in a manner not permitted under the Privacy Rule* which compromises the security or privacy of the protected health information.

45 CFR 164.402 "Breach"





Behavioral Health HIPAA Compliance

HIPAA LAW AND THE HIPAA RULES

Health Insurance Portability and Accountability Act of 1996
Health Information Technology for Eeconomic and Clinical Health Act
4 HIPAA Rules



The HIPAA Rules are designed to work together
to Protect the
Privacy and Security of
Protected Health Information (PHI)





PHI PRIVACY RULE

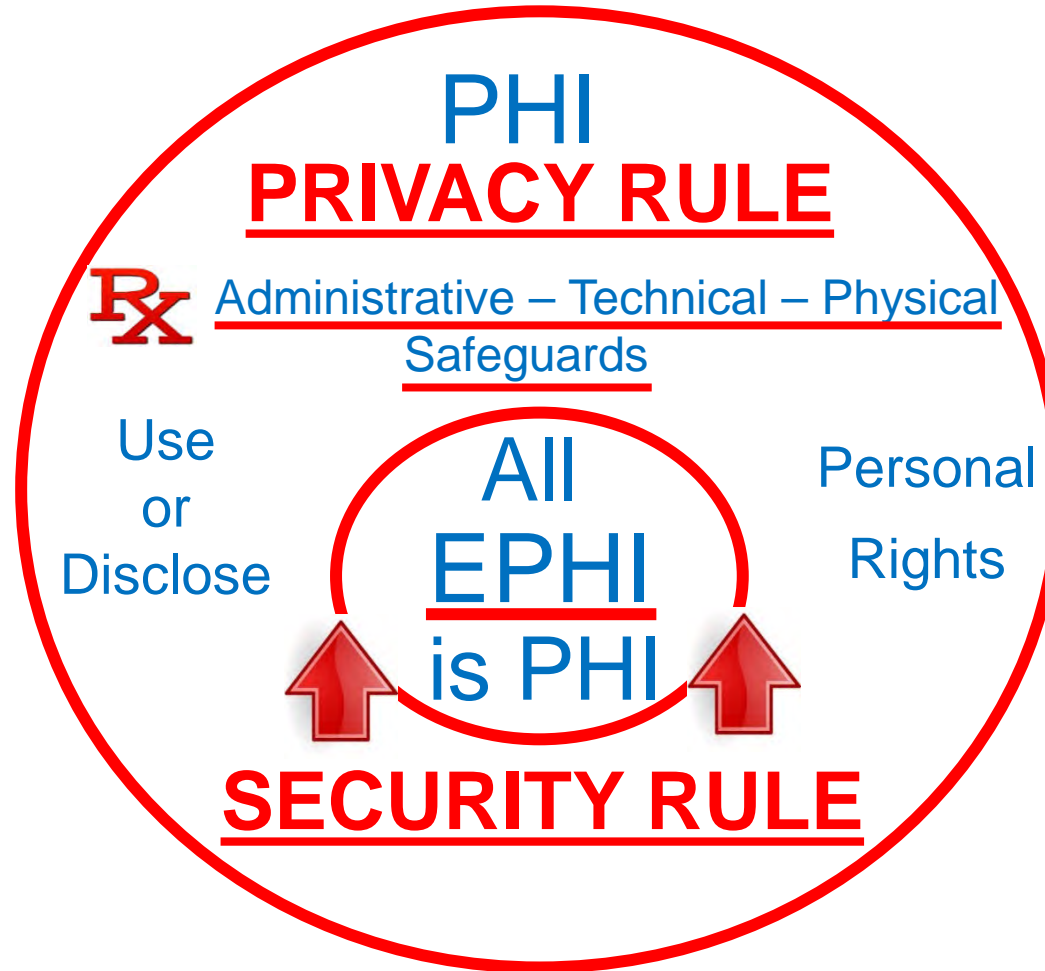


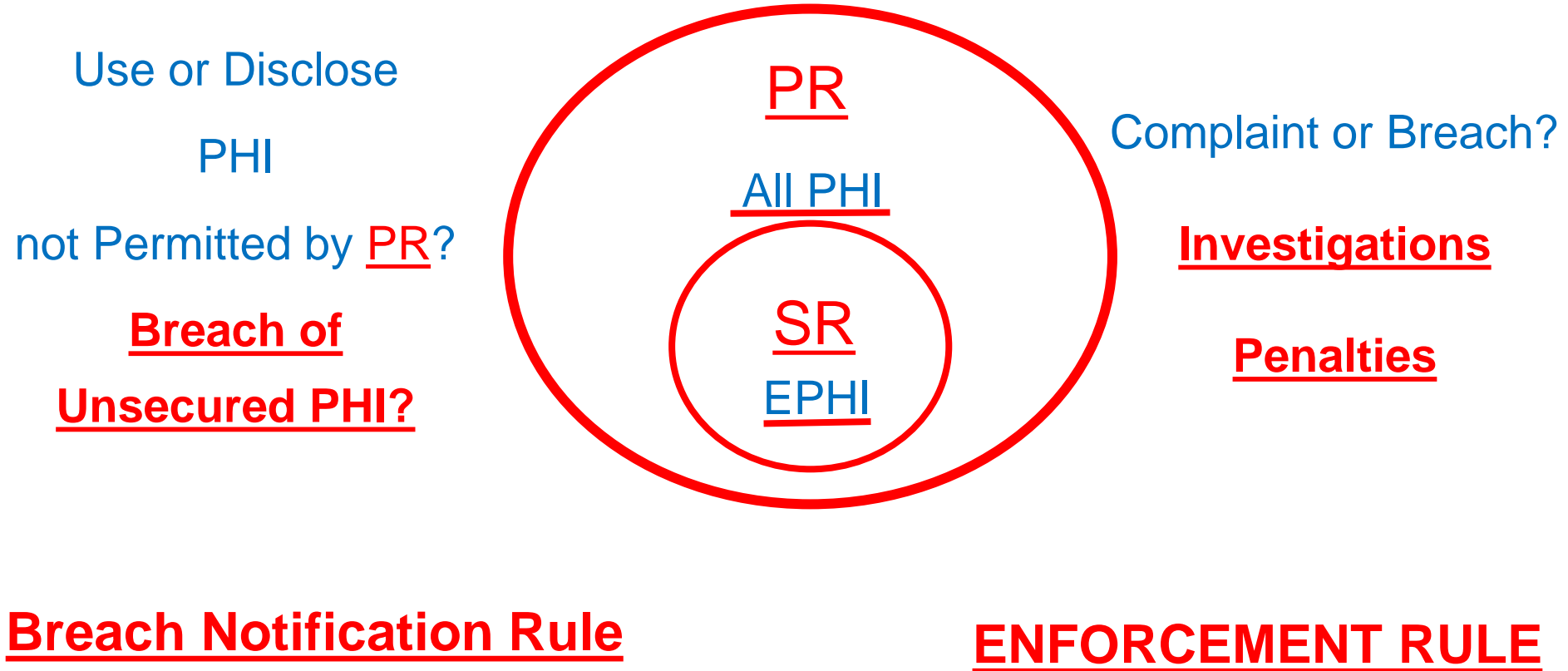
Administrative – Technical – Physical
Safeguards

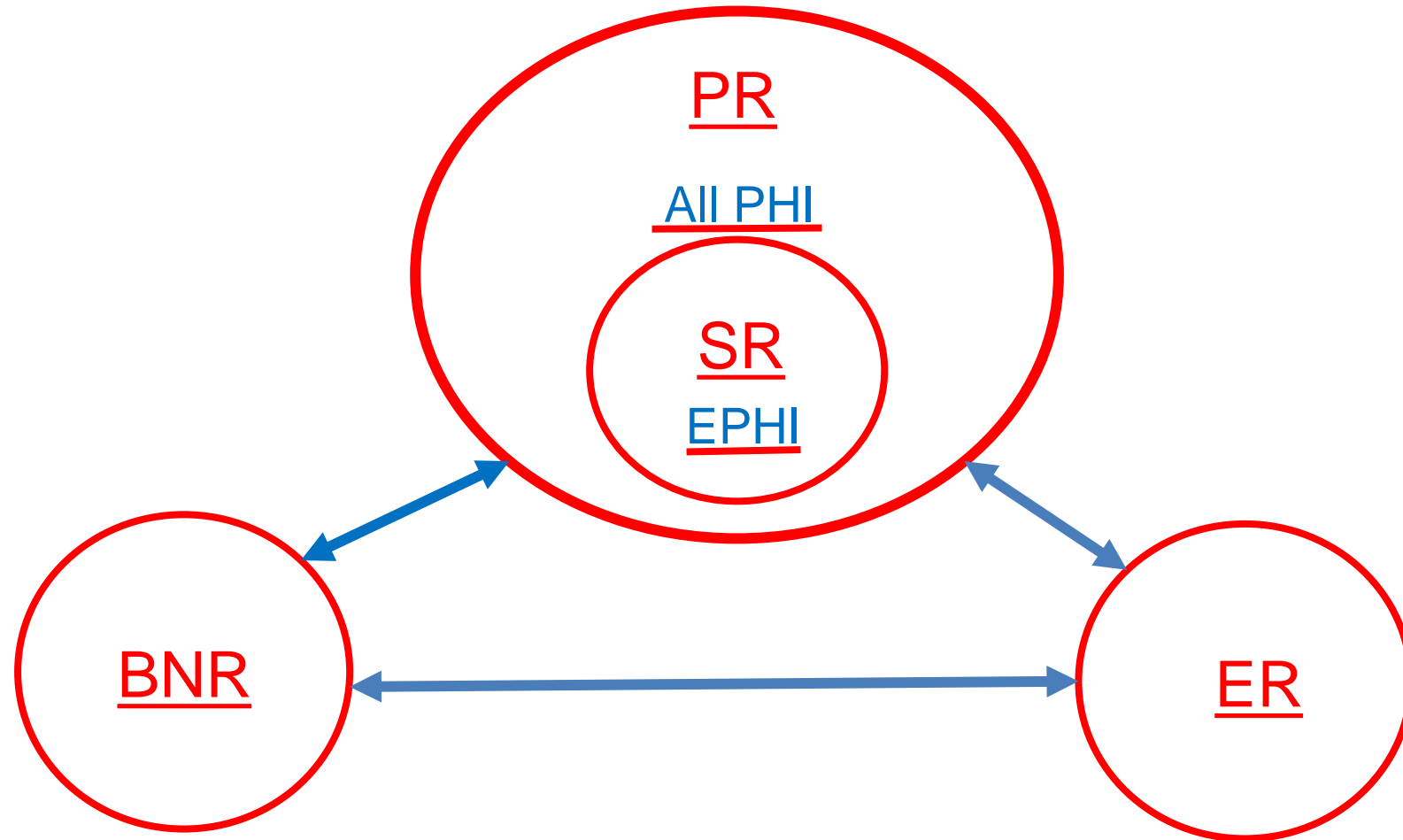
Use
or
Disclose

Personal
Rights









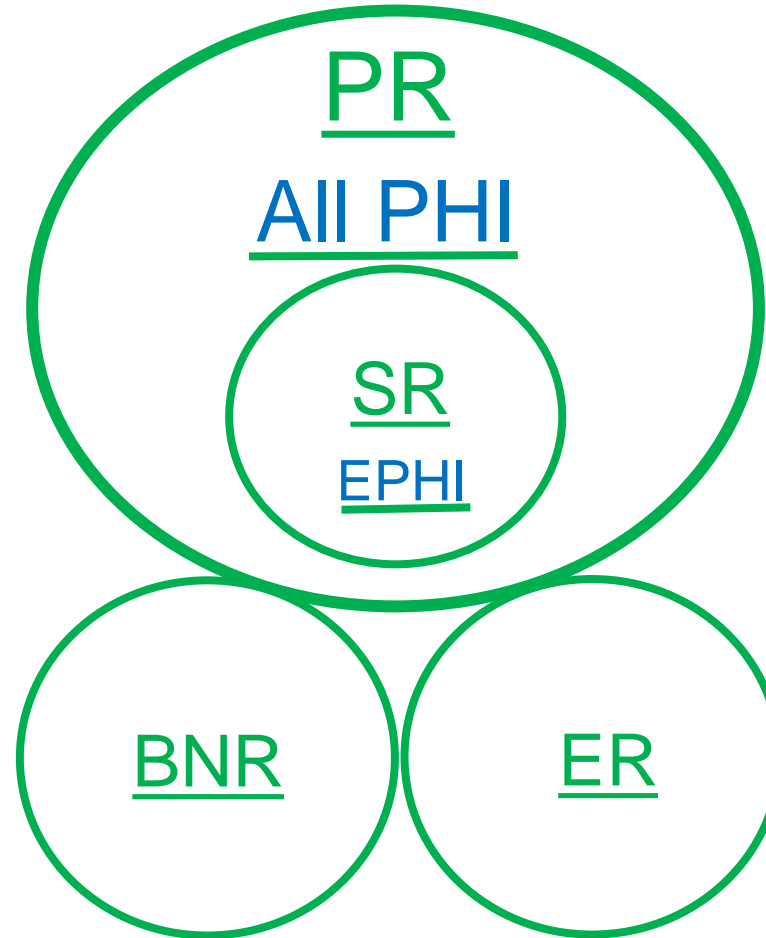


And That's It

Clear

and

Coordinated



HIPAA Rules – Easy to follow – When You Know the Steps





Behavioral Health HIPAA Compliance

WHO MUST COMPLY WITH HIPAA?

TYPES OF ORGANIZATIONS LIABLE FOR HIPAA COMPLIANCE





Behavioral Health HIPAA Compliance

Organizations that must comply with HIPAA

Covered Entities

Health Care Provider – Health Plan – Health Care Clearinghouse

Business Associates

On behalf of a Covered Entity

- Creates, Receives, Maintains or Transmits Protected Health Information (PHI) for a function or activity regulated by the HIPAA Rules
- Provides Services involving disclosure of PHI from a Covered Entity or from another Business Associate

Subcontractor Business Associates

On behalf of a Business Associate

- Creates, Receives, Maintains or Transmits PHI for function or activity regulated by the HIPAA Rules

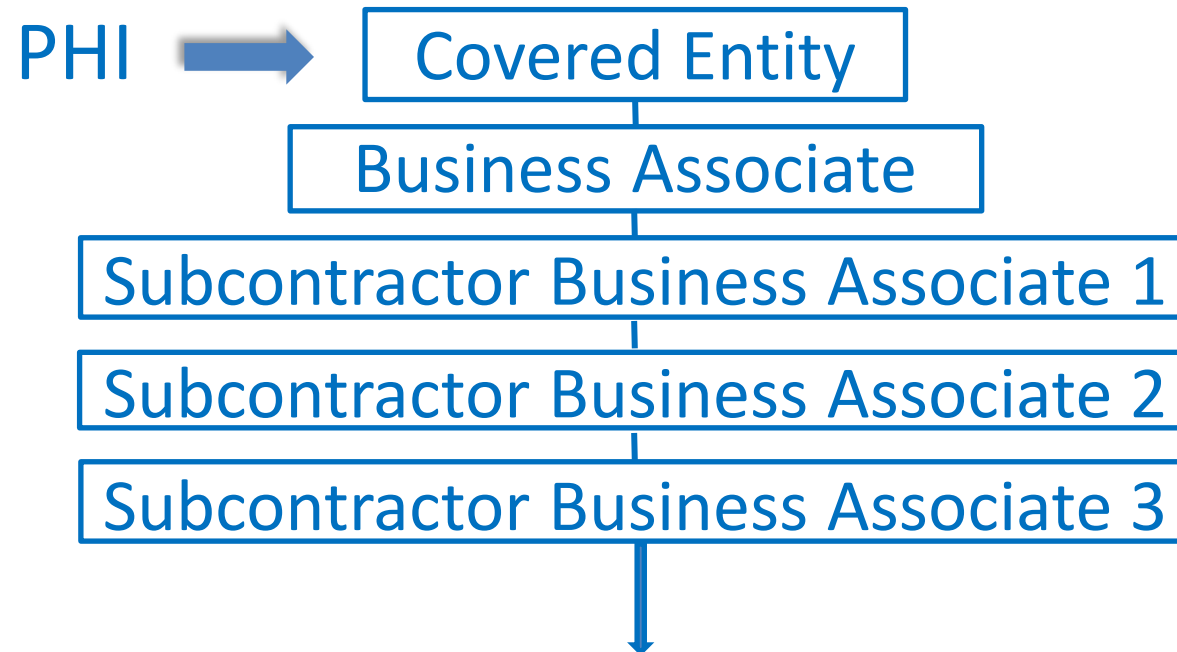




Behavioral Health HIPAA Compliance

Organizations that must comply with HIPAA

PHI Chain of Trust



Business Associate Agreement required at each link of Chain





Behavioral Health HIPAA Compliance

HIPAA COMPLIANCE BASICS

ACCOUNTABILITY: RESPONSIBILITY & DELEGATION OF AUTHORITY





Behavioral Health HIPAA Compliance Accountability

Senior Management is Responsible ←

- Senior Management may delegate Authority to develop and implement the organization's HIPAA Compliance Program
 - Privacy Official – (Privacy Officer)
 - Security Official – (Security Officer)
- Senior Management cannot delegate legal Responsibility





Behavioral Health HIPAA Compliance Accountability

Senior Management is Responsible ←

“We didn’t realize this violated HIPAA”

OCR’s position:

A Covered Entity or Business Associate cannot claim “lack of knowledge” because it failed to inform itself about compliance obligations

[75 FR 40878, July 14, 2010](#)





Behavioral Health HIPAA Compliance Accountability

OCR's [Corrective Action Plan](#) for iHealth Solutions is a roadmap to review, revise, develop and implement any organization's HIPAA Compliance Program

- An attestation signed by an owner or officer of iHealth stating that he or she has reviewed the Implementation Report, has made a reasonable inquiry regarding its content and believes that, upon such inquiry, the information is accurate and truthful.
- Risk Analysis and Risk Management
- HIPAA Policies and Procedures including management of identified Risks
 - Privacy Rule – Security Rule – Breach Notification Rule
- Workforce Training
 - Privacy, Security & Breach Notification Policies & Procedures

False Attestation is a Felony – [18 U.S.C. § 1001](#)





Behavioral Health HIPAA Compliance

Accountability

1. Make HIPAA Compliance a Core Value of the Organization

2. Designate a Privacy Official

Duties:

Develop and Implement organization's Privacy Rule and Breach Notification Rule HIPAA compliance Policies and Procedures

[45 CFR 164.530\(a\)\(1\)\(i\)](#)

2. Identify the Security Official

Duties:

Develop and Implement organization's Security Rule HIPAA compliance Policies and Procedures

[45 CFR 164.308\(a\)\(2\)](#)





Behavioral Health HIPAA Compliance Accountability

🏠 The HIPAA E-Tool®

[Change Location](#)
[Update Organization Information](#)
[Logout](#)

- 1 Introduction
- 2 **Basic HIPAA Policies** ●
- 3 Risk Analysis - Risk Management
- 4 Privacy Rule ●
- 5 Security Rule ●
- 6 Breach Notification Rule ●
- 7 Business Associates ●
- 8 HHS Aligned Audit Protocols
- 9 Enforcement Rule
- 10 Index/Glossary

HIPAA Compliant Organization

[Basic HIPAA Policies](#)

HIPAA-1: HIPAA Compliance Program

Update
PDF Document

Show Video

HIPAA Compliance Program of HIPAA Compliant Organization

Document Number: HIPAA-1		Page 1 of 3
Document Name: HIPAA Compliance Program		
Document Type: HIPAA Compliance Program Policy		Effective Date: 09/23/2013
		Date Last Review: 12/21/2023
Privacy Official	Pat Privacy	TEL: (314) 534-3535
Security Official	Sasha Security	TEL: (314) 534-3534

PURPOSE

The purpose of this Policy is to confirm that HIPAA Compliant Organization has established and maintains a HIPAA Compliance Program; provide a description of the purpose and content of the HIPAA Compliance Program and declare that compliance with the HIPAA Compliance Program of HIPAA Compliant Organization is a core value of this Organization.





Behavioral Health HIPAA Compliance

HIPAA COMPLIANCE BASICS

RISK ANALYSIS & RISK MANAGEMENT





Behavioral Health HIPAA Compliance Risk Analysis and Risk Management

HIPAA Rules – Easy to Follow

Step-by-Step

When You Know the Steps

No RA-RM Steps in the HIPAA Rules!

OCR/NIST Guidance





Behavioral Health HIPAA Compliance

Risk Analysis and Risk Management

OCR Risk Analysis Guidance – July 14, 2010

1. Scope of the Analysis
2. Data Collection
3. Identify and Document Potential Threats and Vulnerabilities
4. Assess Current Security Measures (Controls)
5. Determine the Likelihood of Threat Occurrence
6. Determine the Potential Impact of Threat Occurrence
7. Determine the Level of Risk
8. Finalize Documentation
9. Periodic Review and Updates

Guidance on Risk Analysis Requirements under the HIPAA Security Rule

Introduction

The Office for Civil Rights (OCR) is responsible for issuing annual guidance on the provisions in the HIPAA Security Rule.¹ (45 C.F.R. §§ 164.302 – 318.) This series of guidances will assist organizations² in identifying and implementing the most effective and appropriate administrative, physical, and technical safeguards to secure electronic protected health information (e-PHI). The guidance materials will be developed with input from stakeholders and the public, and will be updated as appropriate.

We begin the series with the risk analysis requirement in § 164.308(a)(1)(ii)(A). Conducting a risk analysis is the first step in identifying and implementing safeguards that comply with and carry out the standards and implementation specifications in the Security Rule. Therefore, a risk analysis is foundational, and must be understood in detail before OCR can issue meaningful guidance that specifically addresses safeguards and technologies that will best protect electronic health information.

The guidance is not intended to provide a one-size-fits-all blueprint for compliance with the risk analysis requirement. Rather, it clarifies the expectations of the Department for organizations working to meet these requirements.³ An organization should determine the most appropriate way to achieve compliance, taking into account the characteristics of the organization and its environment.

We note that some of the content contained in this guidance is based on recommendations of the National Institute of Standards and Technology (NIST). NIST, a federal agency, publishes freely available material in the public domain, including guidelines.⁴ Although only federal agencies are required to follow guidelines set by NIST, the guidelines represent the industry standard for good business practices with respect to standards for securing e-PHI. Therefore, non-federal organizations may find their content valuable when developing and performing compliance activities.

All e-PHI created, received, maintained or transmitted by an organization is subject to the Security Rule. The Security Rule requires entities to evaluate risks and vulnerabilities in their environments and to implement reasonable and appropriate security measures to

¹ Section 13401(c) of the Health Information Technology for Economic and Clinical (HITECH) Act.
² As used in this guidance the term "organization" refers to covered entities and business associates. The guidance will be updated following implementation of the final HITECH regulations.
³ The HIPAA Security Rule: Health Insurance Reform: Security Standards, February 20, 2003, 68 FR 8334.
⁴ The 800 Series of Special Publications (SP) are available on the Office for Civil Rights' website – specifically, SP 800-30 – Risk Management (Guide for Information Technology Systems). (<http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/securityruleguidance.html>)





Behavioral Health HIPAA Compliance

OCR and NIST RA-RM Guidance



Sources for
The HIPAA E-Tool®
RA-RM Procedures

[OCR Guidance – 2010](#)

OCR Published RA-RM
Resolution Agreements &
Corrective Action Plans

OCR Webinars &
Conference Presentations
Posted Guidance



[NIST Special Publication 800-30
Revision 1](#) ←

Guide for Conducting
Risk Assessments

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

JOINT TASK FORCE
TRANSFORMATION INITIATIVE

[NIST Risk Management Framework](#)

[NIST Special Publication 800-66 Rev. 2](#) ←

[NIST Special Publication 800-53 Rev. 5](#) ←

[NIST Special Publication 800-53A Rev. 5](#) ←





Behavioral Health HIPAA Compliance

How to do HIPAA RA-RM – Preview – OCR/NIST Guidance

It's just –

A 3 Act Play

Act 1 – Setup

Risk Analysis

1. Assemble Information
 - PHI Locations in your Information System
 - Workforce – Business Associates
 - Identify Threats, Vulnerabilities and Risks
2. Assess Level of Risks





Behavioral Health HIPAA Compliance

How to do HIPAA RA-RM – Preview – OCR/NIST Guidance

It's just –

A 3 Act Play

Act 2 – Confrontation

Risk Management Actions

Reduce Risks to Reasonable and Appropriate Level

Act 3 – Resolution

Risk Management Program

Active – Documented – In Place





The HIPAA E-Tool®

HIPAA Compliant Organization Change Location Update Organization Information Logout

Search

- Introduction
- Basic HIPAA Policies
- Risk Analysis - Risk Management**
- Privacy Rule
- Security Rule
- Breach Notification Rule
- Business Associates
- HHS Aligned Audit Protocols
- Enforcement Rule
- Index/Glossary

Support Hotline
1-800-570-5879
info@hipaaetool.com

Protecting Patient Privacy Is Our Job®

The HIPAA E-Tool® licensed for exclusive use by HIPAA Compliant Organization

Risk Analysis - Risk Management

Introduction - HIPAA Risk Analysis -Risk Management

RA-1 HIPAA Risk Analysis-Risk Management Policy and Procedures

[HIPAA Risk Analysis-Risk Management Step-by-Step Instructions](#) ←

Risk Analysis Part 1: Assess Risks - EPHI and Non-EPHI Locations, Workforce, Business Associates

RA-1.A Locations and Potential Risks to EPHI and Non-EPHI

RA-1.B Workforce Roster - PHI Access - Training

RA-1.C Business Associate Roster - Due Diligence and BAA

Risk Analysis Part 2: Assess Risks - Security Rule Standards, Implementation Specifications

RA-2.A Security Rule Checklist

Risk Analysis Part 3 Identify Threats and Vulnerabilities

RA-3.A Threats to EPHI/Non-EPHI - Related Vulnerabilities

Risk Analysis Part 4 Assess Risk Level of Each Threat/Vulnerability Pair

RA-4.A Risk Assessment - Each Threat/Vulnerability Pair

Risk Management Actions

RA-5.A Risk Management Actions - Locations of EPHI and Non-EPHI
Risks identified in RA-1.A, Locations and Potential Risks to EPHI and Non-EPHI

RA-5.B Risk Management Actions - Risks Identified by Security Rule Checklist
Risks identified in RA-2.A, Security Rule Checklist

RA-5.C Risk Management Actions - Risks Caused by Threat/Vulnerability Pairs
Threat/Vulnerability Pair Risks identified in RA-3.A and RA-4.A

Risk Management Documentation

RA-6.A Risk Management - Locations of EPHI and Non-EPHI

RA-6.B Risk Management - Workforce Training

RA-6.C Risk Management - Business Associate Due Diligence, BAA

RA-6.D Risk Management - Security Rule Checklist Completion

RA-6.E Risk Management - Threat/Vulnerability Pairs

RA-6.F Supplemental Risk Analysis - Risk Management Documentation

Act 1

Risk Analysis 4 Steps

Act 2

Risk Management Actions

Act 3

Risk Management Plan





🏠 The HIPAA E-Tool®
HIPAA Compliant Organization
📍 Change Location
🔄 Update Organization Information
🚪 Logout

1 Introduction

2 Basic HIPAA Policies ●

3 Risk Analysis - Risk Management

4 Privacy Rule ●

5 Security Rule ●

6 Breach Notification Rule ●

7 Business Associates ●

8 HHS Aligned Audit Protocols

9 Enforcement Rule

10 Index/Glossary

Support Hotline

Risk Analysis - Risk Management Dashboard

Risk Analysis Risks Identified	Risk Management Actions Assigned	Risk Management Documented
<p>Act 1</p> <div style="border: 2px solid #007bff; border-radius: 50%; width: 80px; height: 80px; margin: 0 auto; display: flex; align-items: center; justify-content: center;"> <div style="width: 100%; height: 100%; border: 1px solid #007bff; border-radius: 50%;"></div> <div style="font-size: 2em; font-weight: bold; color: #007bff;">88%</div> </div>	<p>Act 2</p> <div style="border: 2px solid #007bff; border-radius: 50%; width: 80px; height: 80px; margin: 0 auto; display: flex; align-items: center; justify-content: center;"> <div style="width: 100%; height: 100%; border: 1px solid #007bff; border-radius: 50%;"></div> <div style="font-size: 2em; font-weight: bold; color: #007bff;">90%</div> </div>	<p>Act 3</p> <div style="border: 2px solid #007bff; border-radius: 50%; width: 80px; height: 80px; margin: 0 auto; display: flex; align-items: center; justify-content: center;"> <div style="width: 100%; height: 100%; border: 1px solid #007bff; border-radius: 50%;"></div> <div style="font-size: 2em; font-weight: bold; color: #007bff;">66%</div> </div>
<p>EPHI/Non-EPHI Locations 18</p> <p>Workforce Training 6</p> <p>Business Associate - BAAs 4</p> <p>Security Rule Checklist 15 of 57</p> <p>Identify Threats & Vulnerabilities 7</p> <p>Risk Level - Threat/Vulnerability Pairs 14</p> <p>Suggestion: Security Rule Checklist</p>	<p>EPHI/Non-EPHI Location Actions 14 of 14</p> <p>Security Rule Checklist Actions 11 of 15</p> <p>Threat/Vulnerability Pair Actions 14 of 14</p> <p>Suggestion: Security Rule Checklist Actions</p>	<p>EPHI/Non-EPHI Location Management 12 of 14</p> <p>Workforce Training Management 2 of 3</p> <p>Business Associate BAAs Management 2 of 2</p> <p>Security Rule Checklist Management 3 of 15</p> <p>Threat/Vulnerability Pair Management 8 of 14</p> <p>Suggestion: EPHI/Non-EPHI Location Management</p>

Click this Button to:

[Start or Continue](#)

- Start your RA-RM or Continue an RA-RM in progress
- Revise or supplement an RA-RM in progress that has not been archived
- Start a new RA-RM pre-populated with data from your last archived RA-RM

Click this Button to create an archive copy of a completed RA-RM

[Create Archive](#)

- Your completed, archived RA-RM will be available for download as a PDF
- Forms for your next RA-RM are pre-loaded with the data from your archived RA-RM
- If you do not want to pre-load forms with archived data click the "Brand New Start" Button





Behavioral Health HIPAA Compliance

HIPAA COMPLIANCE BASICS

POLICIES – PROCEDURES – TRAINING





Behavioral Health HIPAA Compliance

Policies – Procedures – Training

1. A covered entity must implement Policies and Procedures with respect to protected health information that are designed to comply with the standards, implementation specifications, or other requirements of the Privacy Rule and Breach Notification Rule

[45 CFR 164.530\(i\)\(1\)](#)

2. A covered entity or business associate must implement reasonable and appropriate Policies and Procedures to comply with the standards, implementation specifications, or other requirements of the Security Rule ←

[45 CFR 164.316\(a\)](#)





Behavioral Health HIPAA Compliance

Policies – Procedures – Training

HIPAA Compliance Policies and Procedures must cover
All Standards and Implementation Specifications of the
Privacy Rule
Breach Notification Rule
Security Rule

And be customized when necessary and appropriate to:


- Address specific circumstances unique to your organization
- Reduce identified risks to the privacy and security of your organization's PHI to a reasonable and appropriate level
- Incorporate changes in HIPAA Rules or other applicable law
- Address changed circumstances in your organization





Behavioral Health HIPAA Compliance

Policies – Procedures – Training

1. A covered entity must train all members of its workforce on the policies and procedures with respect to protected health information required by the Privacy Rule and Breach Notification Rule as necessary and appropriate for the members of the workforce to carry out their functions  Role-based Training
45 CFR 164.530(b)(1)
2. A covered entity or business associate must implement a security awareness and training program for all members of its workforce (including management).
45 CFR 164.308(a)(5)(i)





Behavioral Health HIPAA Compliance

COMMON HIPAA VIOLATIONS

EASY TO FIND – EASY TO CORRECT





Behavioral Health HIPAA Compliance

COMMON HIPAA VIOLATIONS – HIGHLY VISIBLE

Notice of Privacy Practices

Not Posted Prominently on the Organization's Home Page

HIPAA Privacy Rule

45 CFR §164.520 (c)(3)(i)

A covered entity that maintains a web site that provides information about the covered entity's customer services or benefits must prominently post its notice on the web site





Behavioral Health HIPAA Compliance

COMMON HIPAA VIOLATIONS – HIGHLY VISIBLE

Notice of Privacy Practices

Not Posted Prominently on the Organization's Home Page

HHS Phase 2 HIPAA Compliance Audit

Audit Inquiry

Determine whether the entity maintains a web site. If so, observe the web site to determine if the notice of privacy practices is prominently displayed and available.

An example of prominent posting of the notice would include a direct link from homepage with a clear description that the link is to the HIPAA Notice of Privacy Practices.





Behavioral Health HIPAA Compliance

COMMON HIPAA VIOLATIONS – HIGHLY VISIBLE

Notice of Privacy Practices

Not Posted Prominently on the Organization's Home Page

Covered Entity Web Site NPP Link correctly posted on Home Page

Contact Information | Nondiscrimination Policy | Terms of Use
Privacy Policy | HIPAA Notice of Privacy Practices





Behavioral Health HIPAA Compliance

COMMON HIPAA VIOLATIONS – HIGHLY VISIBLE

Communicating with Patients using Regular Email & Texts

Without following 3 Step Safeguard

1. Notify “Duty to Warn”

Some level of risk information in an Unencrypted Email or Text Message can be read by someone else

2. Let the Patient Decide

If the Patient prefers Unencrypted Email or Text Message the Patient has the right to receive them

Privacy Rule [78 FR 5634, Jan. 25, 2013](#)

Security Rule [79 FR 7302, Feb. 6, 2014](#)





Behavioral Health HIPAA Compliance

COMMON HIPAA VIOLATIONS – HIGHLY VISIBLE

Communicating with Patients using Regular Email & Texts

Without following 3 Step Safeguard

1. Notify “Duty to Warn”

Some level of risk information in an Unencrypted Email or Text Message can be read by someone else

2. Let the Patient Decide

If the Patient prefers Unencrypted Email or Text Message the Patient has the right to receive them

3. Document

Your Warning and Patient’s Decision to receive Unencrypted Email or Text Message
[45 CFR 164.530\(j\)\(1\)](#)





Behavioral Health HIPAA Compliance

COMMON HIPAA VIOLATIONS – HIGHLY VISIBLE

Communicating with Patients using Regular Email & Texts Without following 3 Step Safeguard

If individuals are notified of the risks and still prefer unencrypted email, the individual has the right to receive protected health information in that way, and covered entities are not responsible for unauthorized access of protected health information while in transmission to the individual based on the individual's request.

Further, covered entities are not responsible for safeguarding information once delivered to the individual.

78 FR 5634, Jan. 25, 2013





Behavioral Health HIPAA Compliance

COMMON HIPAA VIOLATIONS – HIGHLY VISIBLE

Communicating with Patients using Regular Email & Texts

Without following 3 Step Safeguard

If individuals are notified of the risks and still prefer unencrypted email, the individual has the right to receive protected health information in that way, and covered entities are not responsible for unauthorized access of protected health information while in transmission to the individual based on the individual's request.

Further, covered entities are not responsible for safeguarding information once delivered to the individual.

78 FR 5634, Jan. 25, 2013

NO HIPAA VIOLATION
Safe Harbor





Behavioral Health HIPAA Compliance

COMMON HIPAA VIOLATIONS – HIGHLY VISIBLE

Communicating with Patients using Regular Email & Texts

Without following 3 Step Safeguard

2013 Privacy Rule – effective September 23, 2013 **“Duty to Warn”**

January 25, 2013 – [78 FR 5634](#)

2014 Security Rule – Encryption Reasonable & Appropriate Safeguard

Unencrypted Email permitted *if Individual warned of risks prefers Unencrypted Email*

February 6, 2014 – [79 FR 7302](#)

2016 Privacy Rule Access Guidance – Reviewed by OCR - January 5, 2024

<https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html>

2018 Text Message **“Duty to Warn” Confirmation**

OCR Director Roger Severino – HIMSS Annual Conference

March 6, 2018





Behavioral Health HIPAA Compliance

COMMON HIPAA VIOLATIONS – HIGHLY VISIBLE

Communicating with Patients using Regular Email & Texts
Without following 3 Step Safeguard



Recorded exchange between attendee and OCR Director

Q. Do OCR guidelines for Unencrypted Email apply to Unencrypted Text Messages – if a patient is educated and agrees to the risk and doesn't want to use secure texting?

A. “I don't see a difference.” – between an Unencrypted Email and an Unencrypted Text Message

Q. “I guess I have to avoid the secure texting vendors who may want to shoot me now.”





Behavioral Health HIPAA Compliance

COMMON HIPAA VIOLATIONS – OCR INVESTIGATIONS

Tracking Technologies

Major New HIPAA Web Site Liability

[June 16, 2022 The Markup article](#)

[Facebook Is Receiving Sensitive Medical Information from Hospital Websites](#)

[December 1, 2022 updated March 28, 2024 OCR Bulletin](#)

[Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates](#)

[Tracking technologies are used to collect and analyze information about how users interact with regulated entities' websites or mobile applications \(“apps”\).](#)





Behavioral Health HIPAA Compliance

COMMON HIPAA VIOLATIONS – OCR INVESTIGATIONS

Tracking Technologies

Major New HIPAA Web Site Liability

Key Points

- Tracking Technologies are complex
- There are many types of Tracking Technologies
- Until 2022, Tracking Technology functions and risks were largely unknown to Health Care Provider senior management and compliance officials





Behavioral Health HIPAA Compliance

COMMON HIPAA VIOLATIONS – OCR INVESTIGATIONS

Tracking Technologies

Major New HIPAA Web Site Liability

How to Avoid Tracking Tech Liability

- *Risk Analysis & Risk Management*
- Identify Tracking Technology Locations
- Assemble Multi-Specialty Team
 - Senior Management
 - Outside Experts – Business Associates with BAAs
 - Information Technology – Security – Legal – Others





Behavioral Health HIPAA Compliance

COMMON HIPAA VIOLATIONS – OCR INVESTIGATIONS

Patient’s Right of Access to their PHI

OCR Update and 2024 Priorities

Right of Access Initiative

Melanie Fontes Rainer
OCR Director
February 27, 2024

- HIPAA Privacy Rule gives individuals a right to timely access to their health records (30 days with a possibility of one 30-day extension), and at a reasonable, cost-based fee
- OCR receives many complaints alleging denial or no access to health records
- Announced Enforcement Initiative in February 2019
 - OCR Enforcement Priority
 - Investigations launched across the country
 - To date; forty-four settlements and two CMPs





Behavioral Health HIPAA Compliance

COMMON HIPAA VIOLATIONS – OCR INVESTIGATIONS

Patient's Right of Access to their PHI

Using the Wrong Form

As explained elsewhere in the guidance, a HIPAA authorization is not required for individuals to request access to their PHI, including to direct a copy to a third party – and because a HIPAA authorization requests more information than is necessary or that may not be relevant for individuals to exercise their access rights, requiring execution of a HIPAA authorization may create impermissible obstacles to the exercise of this right.

Privacy Rule Access Guidance – Reviewed by OCR - January 5, 2024





Behavioral Health HIPAA Compliance

COMMON HIPAA VIOLATIONS – OCR INVESTIGATIONS

Patient's Right of Access to their PHI

Use Correct Form

CONFIDENTIAL - This Form Contains Protected Health Information
HIPAA Compliant Organization

Request for Access to Protected Health Information (PHI)

Today's Date: _____

First Name: _____ Middle Initial: _____ Last Name: _____

Name at Time of Treatment (if different than above): _____

Last 4 numbers of Social Security Account Number: _____

Date of Birth (MM/DD/YYYY): _____ Phone: _____ Email (optional): _____

Street Address: _____ City: _____ State: _____ Zip: _____

What records do you want? (Check appropriate boxes below):

States of Service: from _____ to _____

Complete Health Record Complete Billing Records Test Results (X-Rays, Lab/Petechae Results) Other Describe Below: _____

I request that PHI specified above be provided:

To me in the way I choose (i.e. U.S. Mail or another reasonable agreed upon manner)

To the following person/entity - Enter name and address of person/entity you want to receive your PHI: _____

Access Requested: Inspect Onsite at no cost Get Copies - a reasonable, cost-based fee may be charged - see Fees below

if Copies - Choose Form: Paper CD USB Attached to regular unencrypted Email to the Email Address listed below

Regular Email: I acknowledge that I have been informed there is some level of risk that information in a regular unencrypted email can be intercepted and seen by others. I understand proper unencrypted email does accept this risk.

Email Address: _____

Important Information about Sensitive PHI
The PHI you have requested may include sensitive information such as test results and/or diagnosis and treatment information concerning substance use/abuse, psychiatric/behavioral health information, genetic information, AIDS/HIV, and sexually transmitted diseases and other PHI that you believe to be sensitive. Copies will be provided unless you tell us not to by checking a box below.

Do not provide copies of my PHI related to:

Alcohol, Drug and Substance Use/Abuse

Psychiatric/Behavioral Health

Genetic Information

AIDS/HIV testing or sexually transmitted diseases

Other - please specify in box below: _____

Fees: We may charge a reasonable, cost-based fee to provide copies of requested health information to cover cost of labor, supplies and/or postage. If mailed to you, you may also request an explanation or summary of the PHI and we may charge a reasonable, cost-based fee to prepare the explanation or summary.

The fee for your request is \$ _____

Signature Required to Submit Request

Signature of Individual or Personal Representative: _____

Signer's Printed Name: _____

If Personal Representative: Title/Authority to Act: _____

A Personal Representative's Authority to Act for the Individual must be verified. Documentation such as a health care power of attorney, court order or other documentation may be requested to accept and process a Request for Access submitted on behalf of an individual by a Personal Representative.

PH-4-A Request for Access to Protected Health Information (PHI)
Page 1 of 2

CONFIDENTIAL - This Form Contains Protected Health Information
HIPAA Compliant Organization

Request for Access to Protected Health Information (PHI)

For Office Use Only

Identity of the individual verified

Personal Representative's Identity and Authority to Act Verified

Fee for Requested Access explained, provided and agreed to

Documentation provided to verify Personal Representative's Identity and Authority to Act

Method of Delivery of Records Requested and Agreed to by Individual

U.S. Mail

Individual will pick up at Facility

Attach to Email - Individual Informed email is insecure and prefers Email

Other: _____

HIPAA Compliant Organization

By: _____

Signature _____ Printed Name and Title _____

PH-4-A Request for Access to Protected Health Information (PHI)
Page 2 of 2





Behavioral Health HIPAA Compliance



COMMON HIPAA VIOLATIONS – OCR INVESTIGATIONS

Risk Analysis - Risk Management

OCR Update and 2024 Priorities

Risk Analysis Initiative

Melanie Fontes Rainer
OCR Director
February 27, 2024

- New Enforcement Initiative 
- Focus on compliance with key HIPAA Security Rule requirement
- Most OCR large breach investigations reveal a lack of a compliant risk analysis 
- Drive better practices to protect electronic protected health information (ePHI)
- Better overall security of data





Behavioral Health HIPAA Compliance

COMMON HIPAA VIOLATIONS – OCR INVESTIGATIONS

Risk Analysis - Risk Management

HHS Phase 2 HIPAA Compliance Audit

Risk Analysis

1. Providers commonly submitted documentation of some security activities of a third party security vendor

Responsibility for Risk Analysis rests with the Entity

2. Entities offered third party template policy manuals that contain no evidence of entity-specific review or revision and no evidence of implementation

Risk Management

1. Because audited Entities largely failed to conduct appropriate Risk Analyses, they were unable to link their security plans to management of identified risks
2. Most Entities failed to produce policies and procedures, or implement security measures, sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level





Behavioral Health HIPAA Compliance

COMMON HIPAA VIOLATIONS

Hybrid Entity

This applies to an organization which is a single legal entity with functions that do not involve health care but has components that do provide health care services regulated by HIPAA.

Examples are:

- A County Government that has a Health Department
- A manufacturing company that has a health clinic for employees
- A non-profit organization that provides many types of community services but also provides some HIPAA-covered health care services
- A federally recognized Indian Tribe that provides HIPAA-covered health care services

HIPAA defines the entire organization as a Covered Entity that is responsible for HIPAA compliance.

To avoid HIPAA compliance liability for non-health-related activities, the organization must designate itself as a Hybrid Entity, and identify its Health Care Components that must comply with HIPAA.





Behavioral Health HIPAA Compliance

COMMON HIPAA VIOLATIONS – HYBRID ENTITY

The HIPAA E-Tool®

hybr| Start typing in Search Box

Documents:

- 1 HIPAA-7 Hybrid Entity

Glossary:

- 2 Hybrid Entity

3 **Risk Analysis - Risk Management**

4 **Privacy Rule**

HIPAA Compliant Organization

Welcome

Welcome to *The HIPAA E-Tool®*, your web-based HIPAA

Navigation Tabs in the menu on the left side of your screen lead to each Section. The Tab for Section 1 - Introduction highlights the use of this Software as a Service product.

Enter words or phrases about HIPAA in the Search Box to find explanations and live links to applicable Policies, Procedures, and Notices of Privacy Practices.





Behavioral Health HIPAA Compliance

COMMON HIPAA VIOLATIONS – HYBRID ENTITY

Search Results

Hybrid Entity

Hybrid Entity means a single legal entity that is a Covered Entity whose business activities include both Covered Functions and non-covered functions that identifies components that perform Covered Functions and designates them as Health Care Components.

Legal Authorities and References: 45 CFR § 164.103, 45 CFR § 164.105

Documents: [HIPAA-7 Hybrid Entity](#) , [HIPAA-7.A Designation of Health Care Component](#) , [Section 2 Introduction - HIPAA Compliance Program Basic Policies](#)





Behavioral Health HIPAA Compliance

COMMON HIPAA VIOLATIONS – HYBRID ENTITY

🏠 The HIPAA E-Tool®
📍 Change Location 🔄 Update Organization Information 🚪 Logout

1 Introduction

2 **Basic HIPAA Policies**

3 Risk Analysis - Risk Management

4 Privacy Rule

5 Security Rule

6 Breach Notification Rule

7 Business Associates

8 HHS Aligned Audit Protocols

9 Enforcement Rule

10 Index/Glossary

Support Hotline
📞 1-800-570-5879
✉ info@hipaaetool.com

Protecting Patient Privacy Is Our Job®
The HIPAA E-Tool® licensed for exclusive use by
HIPAA Compliant Organization
© 2014-2024 ET&C Group LLC

» Basic HIPAA Policies

HIPAA-7: Hybrid Entity

Update
PDF Document

HIPAA Compliance Program of HIPAA Compliant Organization

Document Number: HIPAA-7		Page 1 of 2
Document Name: Hybrid Entity		
Document Type: HIPAA Compliance Program Policy and Procedures		Effective Date: 12/01/2019
		Date Last Review: 12/21/2023
Privacy Official	Pat Privacy	TEL: (314) 534-3535
Security Official	Sasha Security	TEL: (314) 534-3534

PURPOSE
The purpose of this Policy is to designate HIPAA Compliant Organization as a Hybrid Entity in compliance with the Privacy Rule because it is a single legal entity with different components, one or more of which are Health Care Components that conduct Covered Functions regulated by HIPAA.

Definitions

Hybrid Entity Hybrid Entity means a single legal entity that is a Covered Entity whose business activities include both Covered Functions and non-covered functions that identifies components that perform Covered Functions and designates them as Health Care Components.

Health Care Component Health Care Component means a component or combination of components designated by a Hybrid Entity that perform Covered Functions. HIPAA applies only to a Health Care Component designated by the Hybrid Entity.

Covered Functions Covered Functions mean those functions of a Covered Entity whose performance makes the entity a health plan, health care provider, or health care clearinghouse.





Behavioral Health HIPAA Compliance

COMMON HIPAA VIOLATIONS – HYBRID ENTITY

The screenshot shows the interface of 'The HIPAA E-Tool'. The top navigation bar includes 'HIPAA Compliant Organization', 'Change Location', 'Update Organization Information', and 'Logout'. A left sidebar contains a search bar and a menu with 10 items: Introduction, Basic HIPAA Policies (highlighted with a green circle), Risk Analysis - Risk Management, Privacy Rule (green circle), Security Rule (green circle), Breach Notification Rule (green circle), Business Associates (green circle), HHS Aligned Audit Protocols, Enforcement Rule, and Index/Glossary. At the bottom of the sidebar is a 'Support Hotline' with the number 1-800-570-5879.

The main content area displays 'Basic HIPAA Policies' and 'HIPAA-7.A: Designation of Health Care Component'. There are two buttons: 'Word Document' and 'PDF Document'. Below these is a form titled 'HIPAA Compliance Program of HIPAA Compliant Organization' with the following fields:

Document Number:	HIPAA-7.A	Page 1 of 1
Document Name:	Designation of Health Care Component	

About this Designation
This designation is only for a single legal entity with different components, one or more of which are Health Care Components that conduct Covered Functions regulated by HIPAA that has designated itself as a Hybrid Entity in accordance with HIPAA-7, Hybrid Entity.

Instructions

1. Download this form as a Word Document.
2. Enter the name of each designated Health Care Component below.
3. Clearly identify each component. You may add specific information such as the component's location and contact information or other information.
4. Place the Designation with the business records and organizing documents of HIPAA Compliant Organization.
5. Revise this Designation as necessary.
6. Retain a copy of each Designation with the Organization's business records. Each is a document





Behavioral Health HIPAA Compliance

HIPAA COMPLIANCE IS A PROCESS

ONGOING AND ADJUSTED WHEN NECESSARY





Behavioral Health HIPAA Compliance

HIPAA Compliance is a Process

For example

The OCR Risk Analysis Guidance – July 14, 2010 calls for “... a truly integrated risk analysis and management process...”

“Performing the risk analysis and adjusting risk management processes to address risks in a timely manner will allow the covered entity to reduce the associated risks to reasonable and appropriate levels.”

Guidance on Risk Analysis Requirements under the HIPAA Security Rule

Introduction

The Office for Civil Rights (OCR) is responsible for issuing annual guidance on the provisions in the HIPAA Security Rule.¹ (45 C.F.R. §§ 164.302 – 318.) This series of guidances will assist organizations² in identifying and implementing the most effective and appropriate administrative, physical, and technical safeguards to secure electronic protected health information (e-PHI). The guidance materials will be developed with input from stakeholders and the public, and will be updated as appropriate.

We begin the series with the risk analysis requirement in § 164.308(a)(1)(ii)(A). Conducting a risk analysis is the first step in identifying and implementing safeguards that comply with and carry out the standards and implementation specifications in the Security Rule. Therefore, a risk analysis is foundational, and must be understood in detail before OCR can issue meaningful guidance that specifically addresses safeguards and technologies that will best protect electronic health information.

The guidance is not intended to provide a one-size-fits-all blueprint for compliance with the risk analysis requirement. Rather, it clarifies the expectations of the Department for organizations working to meet these requirements.³ An organization should determine the most appropriate way to achieve compliance, taking into account the characteristics of the organization and its environment.

We note that some of the content contained in this guidance is based on recommendations of the National Institute of Standards and Technology (NIST). NIST, a federal agency, publishes freely available material in the public domain, including guidelines.⁴ Although only federal agencies are required to follow guidelines set by NIST, the guidelines represent the industry standard for good business practices with respect to standards for securing e-PHI. Therefore, non-federal organizations may find their content valuable when developing and performing compliance activities.

All e-PHI created, received, maintained or transmitted by an organization is subject to the Security Rule. The Security Rule requires entities to evaluate risks and vulnerabilities in their environments and to implement reasonable and appropriate security measures to

¹ Section 13401(c) of the Health Information Technology for Economic and Clinical (HITECH) Act.
² As used in this guidance the term “organization” refers to covered entities and business associates. The guidance will be updated following implementation of the final HITECH regulations.
³ The HIPAA Security Rule: Health Insurance Reform: Security Standards, February 20, 2003, 68 FR 8334.
⁴ The 800 Series of Special Publications (SP) are available on the Office for Civil Rights’ website – specifically, SP 800-30 – Risk Management (Guide for Information Technology Systems). (<http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/securityruleguidance.html>)





Behavioral Health HIPAA Compliance

HIPAA Compliance

Is about Fundamentals

A Core Value of Your Organization

Risk Analysis and Risk Management

Policies – Procedures – Training





Behavioral Health HIPAA Compliance

The HIPAA Rules

Are Easy to Follow

Step-by-Step

When You Know the Steps





Behavioral Health HIPAA Compliance

The HIPAA Rules

Are a Blueprint

To Protect Patients

and Your Organization





Behavioral Health HIPAA Compliance



WESTERN REGIONAL CONFERENCE ON GAMBLING AND GAMING HEALTH AWARENESS

FOCUS ON THE FUTURE

Convention Special – 25% off
Scan to Sign up for Free Online Demo



The HIPAA E-Tool®





Behavioral Health HIPAA Compliance

Your Questions Please

Paul R. Hales, J. D.

PaulHales@AttorneyHales.com

www.AttorneyHales.com

[314-534-3534](tel:314-534-3534)





Behavioral Health HIPAA Compliance

Thank You



Paul Hales, J. D.

HALESLAWGROUP

 HEALTH INFORMATION PRIVACY

PaulHales@AttorneyHales.com

[314-534-3534](tel:314-534-3534)

HALESLAWGROUP
 HEALTH INFORMATION PRIVACY

 **The HIPAA E-Tool[®]**

