

MODULE 03

HIPAA & Confidentiality

Protecting Patient Information — Every Day, Every Interaction

WHAT YOU'LL LEARN

Learning Objectives

- 01 Define Protected Health Information (PHI) and give three examples
- 02 Explain the Minimum Necessary standard and apply it to your role
- 03 Identify three situations where patient information may be shared without written authorization
- 04 Describe what to do if you suspect a PHI breach
- 05 List three HIPAA violations that could result in disciplinary action

THE LAW

HIPAA Is Not *Optional*

The Health Insurance Portability and Accountability Act protects every patient's health information.
Violations can result in **fines up to \$50,000**, termination, and criminal charges.

CORE CONCEPT

What Is PHI?

Protected Health Information is **any information** about a patient's health condition, care, or payment for care that could identify them.

PERSONAL IDENTIFIERS

Name, address, date of birth, phone number, Social Security number

CLINICAL INFORMATION

Medical diagnoses, medications, treatment plans, lab results

VISUAL INFORMATION

Photos of patients — even without names if they show identifiable features

DOCUMENTATION

Visit notes, schedules, care plans, billing records, intake forms

KEY STANDARD

The Minimum Necessary Rule

You should only access, use, or share the **minimum amount** of patient information needed to do your job. More access than necessary is itself a potential HIPAA violation.

EXAMPLE – COMPANION AIDE

- You **need**: patient name, address, schedule, relevant safety info
- You **don't need**: complete medical history, lab results, billing details

EXAMPLE – PERSONAL CARE AIDE

- You **need**: Care Plan tasks, mobility limitations, allergy info
- You **don't need**: psychiatric evaluation notes, family financial information

Only access what you need. Only share what is required. Nothing more.

EXCEPTIONS

When Can You Share PHI?

HIPAA allows sharing PHI **without written authorization** in only three categories. Everything else requires the patient's written consent.

1. Treatment

Telling the on-call nurse about a change in a patient's condition. Sharing observations with your supervisor for care coordination.

2. Payment

Billing for services rendered. Submitting documentation required by the payer.

3. Operations

Supervisor reviewing your visit note for quality purposes. Compliance audits.

THE STANDARD

When in Doubt, Don't Share

If you are unsure whether you can share information, the answer is **no**. Call your supervisor and let them make the determination.

DAILY PRACTICE

The Golden Rules for Caregivers

- 01 **Never discuss patients outside of work** — not with friends, family, neighbors, or on social media
- 02 **Never photograph patients** — not even for "personal memories"
- 03 **Lock your phone** — if you use it for scheduling, it contains PHI
- 04 **Don't leave paperwork visible** — schedule printouts, visit notes, and care plans contain PHI
- 05 **Don't discuss patients in public** — not in hallways, waiting rooms, parking lots, or restaurants
- 06 **Never text patient information** — unless using a secure, agency-approved platform
- 07 **Verify identity before sharing** — even with people who claim to be family or physicians

WARNING

Social Media Is the #1 HIPAA Risk

Posting anything about your work that could identify a patient — even without using their name — is a HIPAA violation.

EXAMPLE POST

"Just helped my sweet 90-year-old patient get dressed today. She always makes me smile."

This is a violation if anyone could identify who you mean — your friends, neighbors, or anyone who knows where you work and which patient you visit.

Don't post about patients. Period.

QUICK REFERENCE

HIPAA in Practice

✓ PERMITTED

- Reporting a condition change to your supervisor
- Documenting care in the visit note system
- Sharing Care Plan info with the on-call nurse
- Discussing a patient with the office for scheduling
- Verbal report to incoming caregiver at shift change

× NEVER PERMITTED

- Telling your spouse about a patient's diagnosis
- Posting anything work-related on social media
- Texting patient info to a coworker's personal phone
- Sharing info with a patient's neighbor who asks
- Looking up a patient's records out of curiosity

COMMON MISTAKE

Family Members & PHI

Being a family member does **not** automatically grant access to a patient's health information. HIPAA protects patient information from disclosure even to spouses, children, and siblings.

"I'd love to help, but I need to verify with my office that I'm authorized to share that information. Let me get back to you."

YOUR SCRIPTED RESPONSE

- Always verify authorization with your supervisor before sharing **any** patient information
- Check if the person is listed as an authorized contact in the Care Plan
- When in doubt, redirect them to the office: (740) 262-9845

DEVICE SECURITY

Your Phone Is a **PHI Risk**

If you use your personal phone for work — scheduling, GPS to a patient's home, communication with the office — your phone contains PHI.

REQUIRED PROTECTIONS

- Enable **screen lock** (PIN, fingerprint, or face ID)
- Set auto-lock to **2 minutes or less**
- Enable **remote wipe** capability
- Keep your phone on your person at all times

IF YOUR PHONE IS LOST OR STOLEN

- Report to your supervisor **immediately**
- Use remote wipe if available
- This is a **potential breach** that must be documented
- Do not wait — time matters

IF SOMETHING GOES WRONG

What Is a Breach?

A breach is any unauthorized access to or disclosure of PHI. Breaches have strict legal deadlines for notification.

ACCIDENTAL DISCLOSURE

Leaving a care plan at a patient's home visible to visitors

MISDIRECTED COMMUNICATION

Sending a text about a patient to the wrong phone number

LOST DEVICE

Losing a phone with patient schedules or addresses on it

VERBAL DISCLOSURE

Discussing a patient's condition in a public place where others can hear

BREACH PROTOCOL

If You Suspect a Breach

Do **not** try to assess or handle it yourself. Report immediately. Breach notification has strict legal deadlines.

- 01 **Stop the disclosure** — if ongoing, take immediate steps to contain it
- 02 **Call your supervisor immediately** — (740) 262-9845
- 03 **Document what happened** — who, what, when, where, and how
- 04 **Do not discuss** the breach with anyone other than your supervisor
- 05 **Cooperate fully** with the investigation that follows

Compliance Officer: compliance@noblecareohio.com

ACCOUNTABILITY

HIPAA Violation Consequences

HIPAA violations are taken seriously by NobleCare, the state of Ohio, and the federal government. The consequences are real.

1

Verbal Warning & Retraining

Minor, unintentional incident — first offense

2

Written Corrective Action

Repeated minor violation or moderate incident

3

Immediate Termination

Intentional violation, social media post, or willful disregard

4

Criminal Prosecution & Fines

Federal penalties: \$100 — \$50,000 per violation, up to \$1.5M annually

DAILY HABITS

Protecting PHI Every Day

IN THE PATIENT'S HOME

- Never leave documents where visitors can see them
- Don't discuss one patient's info at another patient's home
- Keep your phone screen hidden from family visitors
- Shred or secure any paper notes before leaving

IN YOUR PERSONAL LIFE

- Never tell anyone where you work today (address)
- Don't vent about work using details that identify patients
- Don't save patient photos or documents to your personal phone
- If someone asks about your patients, redirect: "I can't discuss that"

WHAT WOULD YOU DO?

Scenario

SITUATION

Linda is a home health aide. After a tough shift where her patient had a particularly difficult day, she posts on Facebook: *"Some days this job is heartbreaking. You really bond with your patients and it's hard to watch them struggle. Today was one of those days."*

Several of Linda's Facebook friends live in the **same neighborhood** as her patient.

- A) This is fine — she didn't use the patient's name
- B) This is fine — it's just a general expression of emotion
- C) This is a potential HIPAA violation — people may be able to identify the patient**
- D) This would only be a violation if she tagged the patient's location

Even Without a Name, It Can Be a Violation

If the post could enable identification of the patient, it may constitute **impermissible disclosure of PHI**. Friends who know where Linda works and which patient she visits can connect the dots.

THE LESSON

- Not using a name does **not** automatically protect you
- Context matters — friends, neighbors, and coworkers can identify patients from timing and details
- The momentary relief of venting is not worth your job or a **\$50,000 fine**
- If you need to process emotions, talk to your supervisor or a counselor — not social media

When in doubt, don't post.

WHAT WOULD YOU DO?

Scenario

SITUATION

You receive a call from someone claiming to be your patient's **physician**. They say: *"I need an update on Mrs. Johnson's condition. How has she been doing this week?"*

- A) Share the information — physicians are treatment providers
- B) Verify the call with your supervisor before sharing any information**
- C) Refuse entirely since you don't have written authorization
- D) Share only the patient's name and address since that's not clinical info

✓ CORRECT ANSWER: B

Always Verify Before Sharing

WHY THE OTHERS ARE WRONG

- **A – You cannot verify** the caller's identity over the phone. This could be anyone.
- **C – Not entirely wrong**, but too rigid. Treatment providers can receive PHI — through proper channels.
- **D – Name and address ARE PHI**. There is no category of "safe" patient information to share freely.

CORRECT RESPONSE

- 01 Thank the caller professionally
- 02 Explain you need to verify with your office
- 03 Call your supervisor: (740) 262-9845
- 04 Let the supervisor handle verification and information sharing

REVIEW

Knowledge Check

1. Which is an example of PHI?

A visit note listing a patient's diagnosis and medication list

2. Someone claiming to be a patient's physician calls for an update. You should:

Verify the call with your supervisor before sharing any information

3. You accidentally text a patient's medication list to the wrong number. What do you do?

Report it immediately to your supervisor as a potential breach

4. Which is permitted under HIPAA without written patient authorization?

Telling your supervisor about a change in a patient's condition (Treatment exception)

5. What does the Minimum Necessary standard mean?

Only access and share the minimum PHI needed to do your specific job

MODULE 03 COMPLETE

HIPAA & Confidentiality

KEY TAKEAWAYS

- PHI = any identifiable health info — names, diagnoses, visit notes, photos
- Minimum Necessary: only access what your job requires
- Share only for Treatment, Payment, or Operations
- Social media = #1 risk. Don't post about patients. Ever.
- Suspected breach? Report immediately to your supervisor
- When in doubt, don't share — call the office

Next → Module 4: Infection Control & PPE