Health Insurance Portability and Accountability Act (HIPAA), Privacy and Employee Information Protection

Mandatory Education Module

Privacy Matters:

Your Role in Protecting Patient and Employee Information

OUR PATIENTS
Their personal health information matters.

OUR EMPLOYEES
Their personal information matters.

OUR RESPONSIBILITY
Privacy. Security. Trust.

A SAFER, STRONGER MVHS TOGETHER

Privacy Matters

Protecting Information Is Everyone's Responsibility

Every employee has a responsibility to protect confidential information.

PATIENT

Protected Health Information (PHI)

Medical, billing, demographic, and other identifiable patient information.

EMPLOYEE

Personally Identifiable Information (PII)

Personal, employment, financial, and other confidential employee information.

ORGANIZATION

Confidential Organizational Information

Internal business, operational, financial, security, and other confidential information.

Protecting patient, employee, and organizational information starts with YOU.

Protecting Patient and Confidential Information Starts With You!

Privacy and confidentiality are everyone's responsibility.

Everyone has a responsibility to protect patient information, employee information, and MVHS confidential information—and to report a suspected violation.

PATIENT

Protect patient information

EMPLOYEE

Protect employee information

MVHS

Protect confidential organizational information

Regardless of your job title or where you work, every employee and individual associated with MVHS is accountable for reporting suspected violations.

PROTECT IT • SPEAK UP • REPORT IT

MVHS | mvhealthsystem.org

What is HIPAA and PHI?

HIPAA is a federal law that protects the privacy and security of individuals' PHI.

What is PHI?

PHI is any information that can identify a person and relates to their past, present, or future health care, treatment, or payment for care.

Examples of PHI

- Name, address, phone number
- Date of birth and medical dates
- Health conditions, diagnoses, test results
- Treatment information
- Photos or images

Where You May Find PHI

- Electronic medical records (e.g., Epic)
- Paper records and printed reports
- Emails and written communications
- Voicemail and phone conversations
- Mobile devices and removable media

HIPAA Permitted Uses and Disclosures

PHI

HIPAA permits PHI to be used or disclosed for specific purposes, including Treatment, Payment, and Health Care Operations (TPO).

Use reasonable safeguards and follow the minimum necessary standard when it applies.

TREATMENT

- Providing and coordinating patient care
- Consultations, referrals, and care coordination

PAYMENT

- Billing and claims activities
- Eligibility, coverage, and payment-related activities

HEALTH CARE OPERATIONS

- Quality, safety, compliance, and operational activities
- Certain training and administrative functions

TO THE PATIENT

- PHI may be disclosed to the patient, upon request
- Includes access to the patient's own health information

REQUIRED DISCLOSURES

- To the patient, when required
- To the Office of Civil Rights
- As otherwise required by law

OTHER PERMITTED DISCLOSURES

- With a valid authorization
- To a personal representative or facility directory
- For certain public-interest purposes

REMEMBER: A permitted disclosure does not mean unlimited disclosure—share only what is appropriate for the purpose.

MVHS | mvhealthsystem.org

Disclosure of PHI

Protect privacy whenever patient information is discussed or shared.

BEFORE YOU SPEAK

PAUSE

Be aware of who can hear.

PROTECT

Share only what is necessary.

VERIFY

Confirm who is receiving PHI.

01

Be Mindful of Your Surroundings

Avoid discussing PHI beyond what is necessary.

02

Keep Conversations Private

Keep your voice down and avoid discussing PHI in public areas.

03

Use Private Spaces

Use private spaces for discussions with faculty, clients, and patients.

04

Protect Phone Conversations

Use a private space and confirm the identity and authority of the recipient before discussing PHI.

05

Use PHI for an Appropriate Purpose

Discuss PHI for Treatment, Payment, and Operations.

06

Respect the Patient's Choice

Ask the patient if they want a visitor to stay before discussing PHI—regardless of who the visitor is.

When in doubt: move to a private area and share only what is necessary.

HIV Information & Confidentiality

New York State Public Health Law — Article 27-F

Article 27-F safeguards the privacy and confidentiality of information related to HIV/AIDS.

CONFIDENTIAL

HIV/AIDS Status Is Protected

A patient's HIV/AIDS status is confidential and should not be released unless disclosure is permitted under Article 27-F.

DISCLOSURE

Follow the Required Rules

Treatment-related disclosure is permitted and HIV information requires special confidentiality protections.

AUTHORIZATION

Use the HIV Release When Required

When authorization is required, use a valid, signed, and dated NYS HIV release form.

IMPORTANT: Unlawful disclosure may result in fines up to $5,000 and/or up to 1 year in jail.

MVHS | mvhealthsystem.org

When in doubt, protect the information and follow MVHS policy before disclosing.

Verifying Patients and Their Information

Always verify a patient's identity and confirm you are accessing, discussing, or disclosing the correct patient's information. This helps ensure patient safety, protects privacy, and prevents the release of information to the wrong person.

Verify Identity

Use at least two patient identifiers, such as name and date of birth, before accessing, discussing, or releasing patient information.

Confirm the Correct Patient

Check the patient's name, medical record number (MRN), and date of birth to ensure you are in the correct chart and viewing the right information.

Verify Requestors

Before sharing information, confirm the identity and relationship of the person requesting information, including authorized personal representatives.

Be Cautious in Conversations

Discuss patient information only with authorized individuals and in a private area. Avoid speaking where others may overhear.

Verify for Phone Requests

Confirm the caller's identity using established verification procedures before providing any patient information.

When in Doubt, Stop and Verify

If you are unsure, do not access, discuss, or release the information. Contact your supervisor or the appropriate department for assistance.

Safeguard Your Computer and Information

Help protect patients, employees, and MVHS information by keeping your computer, account, and data secure. Follow these best practices to prevent unauthorized access, loss of information, and potential breaches.

Lock Your Computer

Lock your screen whenever you step away, even for a short time. Press **Ctrl + Alt + Delete** and select **Lock**.

Secure Documents

Do not leave printed information on your desk or in shared areas. Keep PHI, employee information, and other confidential data secure.

Use a Strong Password

Keep your password confidential, use a strong password, and do not share it with anyone.

Be Cautious with Email

Do not send confidential information to the wrong recipient and be alert for phishing emails.

Keep Software Updated

Allow required updates to help protect against security threats and keep your system secure.

Report Issues

Report lost or stolen devices, suspicious activity, or potential security issues to IT immediately.

Caution: Releasing Sensitive Data

Some patient information is especially sensitive. Only release this information when permitted by law, policy, or with a valid authorization.

Behavioral Health

Mental health and substance use information has extra protections.

HIV-Related

HIV information is protected under New York State law (Article 27-F).

Reproductive Health

Information related to reproductive health may have additional legal protections.

Genetic Information

Genetic test results are sensitive and require special protections.

Other Sensitive Information

Information such as gunshot or stabbing injuries, prisoner status, or high-profile cases requires limited disclosure.

Follow Policy

Only release sensitive information when allowed and use the minimum necessary information.

Access to Protected Health Information (PHI)

You may only access patient information when it is necessary for your work duties and responsibilities and for a permitted purpose, such as Treatment, Payment, or Health Care Operations (TPO). Access is limited to the minimum necessary information.

Treatment

Access PHI to provide, coordinate, or manage a patient's care.

Payment

Access PHI for billing, claims, or to determine coverage.

Health Care Operations

Access PHI for quality improvement, audits, compliance, training, and other designated operations.

Minimum Necessary

Access only the minimum amount of information needed to do your job.

Includes Viewing

Accessing the medical record includes opening a record, searching, viewing, scrolling through, or "hovering" over information.

When NOT to Access PHI

- Do not access your own record.
- Do not access the records of family members, friends, co-workers, or anyone with whom you have a personal relationship.
- Do not access out of curiosity.
- Do not access any patient's medical record unless you are involved in their care.
- Do not access records because of a job change or out of interest in past patients.
- Do not share your login credentials or allow others to access records using your account.
- Report any inappropriate or unauthorized access to your supervisor, Compliance, or Privacy.

Social Media Guidelines

Patient and confidential information does not belong on social media.

Never post PHI or confidential patient or employee information on social media.

PROTECT PHI

- Never post PHI.
- A private or personal account does not make it appropriate to share patient information.

THINK BEFORE YOU POST

- Do not post patient or employee information, images, or identifying details.
- Look for PHI visible in photos, videos, screens, whiteboards, or backgrounds.

PROTECT THE WORKPLACE

- Do not post MVHS locations or workplace content when confidential information may be visible.
- Patient or employee images require appropriate permission or authorization.

REMEMBER: Even without a patient name, a photo, location, diagnosis, or other detail may identify the patient.

MVHS | mvhealthsystem.org

Images, Videos & Communication

Protect PHI when taking images, using personal devices, or communicating electronically.

Use only approved MVHS devices and communication methods when PHI is involved.

PATIENT IMAGES & VIDEOS

- Obtain appropriate authorization before taking patient photos or videos.
- Use an MVHS-issued or approved device.
- Upload images promptly to the medical record when required.

PERSONAL DEVICES

- Do not use a personal phone to photograph or record patients or PHI.
- Do not photograph computer screens, records, whiteboards, or other confidential information.
- Avoid FaceTime, speakerphone, or other unapproved methods when PHI may be heard or seen.

SECURE MESSAGING

- Use Epic Secure Messaging or another approved MVHS communication method.
- Do not send PHI through unapproved text messaging or personal messaging apps.
- Verify the recipient before sending confidential information.

REMEMBER: Personal devices should never be used to capture or transmit PHI.

MVHS | mvhealthsystem.org

Using Artificial Intelligence (AI) Responsibly

AI tools can be helpful for work, but they must be used responsibly. Do not enter, upload, or share any Protected Health Information (PHI), Confidential MVHS Information, or Employee Personally Identifiable Information (PII) into AI tools.

- Do not enter, upload, or share PHI, confidential MVHS information, or employee PII into AI tools.
- Use only AI tools that have been reviewed and approved by MVHS.
- Do not include patient names, employee names, or other identifiers in AI prompts.
- Follow MVHS policies and any required training for AI use.
- Use AI only for appropriate work-related purposes.
- Be aware that information entered into public AI tools may not be private or secure.
- Do not use AI to generate or summarize clinical documentation using PHI unless specifically approved.
- Report any suspected or unintended disclosure of confidential information related to AI use.

What Is a HIPAA Breach?

A breach is an unauthorized acquisition, access, use, or disclosure of unsecured PHI.

UNAUTHORIZED ACCESS

- Accessing a patient record without a work-related need
- Viewing more PHI than needed to perform your job

OTHER EXAMPLES

- Improperly sharing confidential information
- Improper disposal of PHI
- Failing to secure a workstation
- Sharing passwords or login information

WHAT HAPPENS NEXT?

- Privacy/Compliance reviews the incident
- Notification to external entities may be required
- Disciplinary standards may apply

REMEMBER: Report suspected privacy incidents promptly so they can be investigated.

Information Blocking

WHAT IS INFORMATION BLOCKING?

Information blocking means unnecessarily preventing or delaying access to electronic health information.

The goal: support appropriate access while protecting patients when a valid reason exists.

WHEN INFORMATION MAY NEED TO BE WITHHELD

1. **Identify the concern**
   There may be a significant reason to restrict information, such as potential harm to the patient or another person.

2. **Follow the approved process**
   Do not independently block or delay information. Escalate the concern for appropriate review.

3. **Document the reason**
   If information is withheld, clearly document why the note or information is being blocked.

REMEMBER: If you are unsure whether information can be withheld, Contact Compliance or Health Information Management.

MVHS | mvhealthsystem.org

HIPAA Breaches can lead to...

A HIPAA breach is a violation of the privacy, security, or confidentiality of PHI. Breaches can have serious consequences for you and the organization.

Disciplinary action
up to and including termination.

Personal fines
or jail time.

Potential loss
of a professional license if you hold one.

DO'S AND DON'TS OF HIPAA

Everyone at MVHS plays a role in protecting the privacy, security, and confidentiality of PHI. Follow these do's and don'ts to help keep patient information safe.

DO

- Get a new password if yours has been compromised.
- Excuse yourself from taking care of individuals with whom you have a personal relationship.
- Cover up any patient information so others cannot view it.
- Use a fax sheet and verify fax numbers before faxing PHI.
- Use a soft voice when discussing patients and visitors. If not possible, move to a private area.

DON'T

- Never let someone else use your password.
- Access, view or print your own, friends or families medical records.
- Leave a paper copy of a document with medical information in public areas.
- Discuss patient information in public areas.
- Leave a portable computer or device that contains PHI unsecured or unattended, especially when you are off premises.

Employee Information Is Confidential Too!

PII

Personally Identifiable Information (“PII”) is information that can identify or be associated with an individual.

This may include employee information or any other information that could be used to personally identify an individual.

Employee information may include, but is not limited to:

- NAME — **Name**
- HOME — **Home address**
- PHONE — **Telephone number**
- EMAIL — **Personal email**
- DOB — **Date of birth**
- SSN — **Social Security number**
- ID — **Employee ID number**
- PAY — **Payroll information**
- BANK — **Banking/direct deposit**
- TAX — **Tax information**

MVHS | mvhealthsystem.org

Protecting Employee Information

Protect employee information just as you would protect patient information.

- Access information only when needed for their job.
- Use approved systems.
- Keep employee information confidential.
- Do not take screenshots or pictures of employee personally identifiable information.
- Do not share personally identifiable information without a job-related reason.
- Protect passwords.
- Lock computers.
- Secure paper documents.
- Verify recipients.
- Avoid discussing confidential information in public.
- Report suspected unauthorized access or disclosure to employee information.

Your Responsibility

Every MVHS individual is responsible for protecting confidential information whether it is a patient or employee's information.

Before You Act – Ask Yourself:

- Do I need this information?
- Am I authorized to access this information?
- Does the person receiving this information need it?
- Am I using an approved method?
- Would I be comfortable explaining why I accessed this information?

Reporting Non-Compliance
Compliance Is Everyone's Responsibility!

Promptly report any concerns or violations:

- **Privacy Violations:**
  The Privacy Officer at (315) 624-5117.
  The Legal/Compliance Department at (315) 624-5050.
- **Security Violations:**
  IT Help Desk at (315) 917-9600.
- **Anonymous Reports:**
  Compliance Hotline at 1-800-954-9148 or
  www.mvhealthsystem.ethicspoint.org.