MOHAWK VALLEY HEALTH SYSTEM

2024 Mandatory Education Module

HIPAA Privacy and Security

HIPAA Privacy and Security

Health Insurance Portability and Accountability Act ("HIPAA")

What is HIPAA?

- Health Insurance Portability and Accountability Act (HIPAA), is a federal law that protects patient health information from being disclosed, used, or accessed without the patients consent or knowledge.

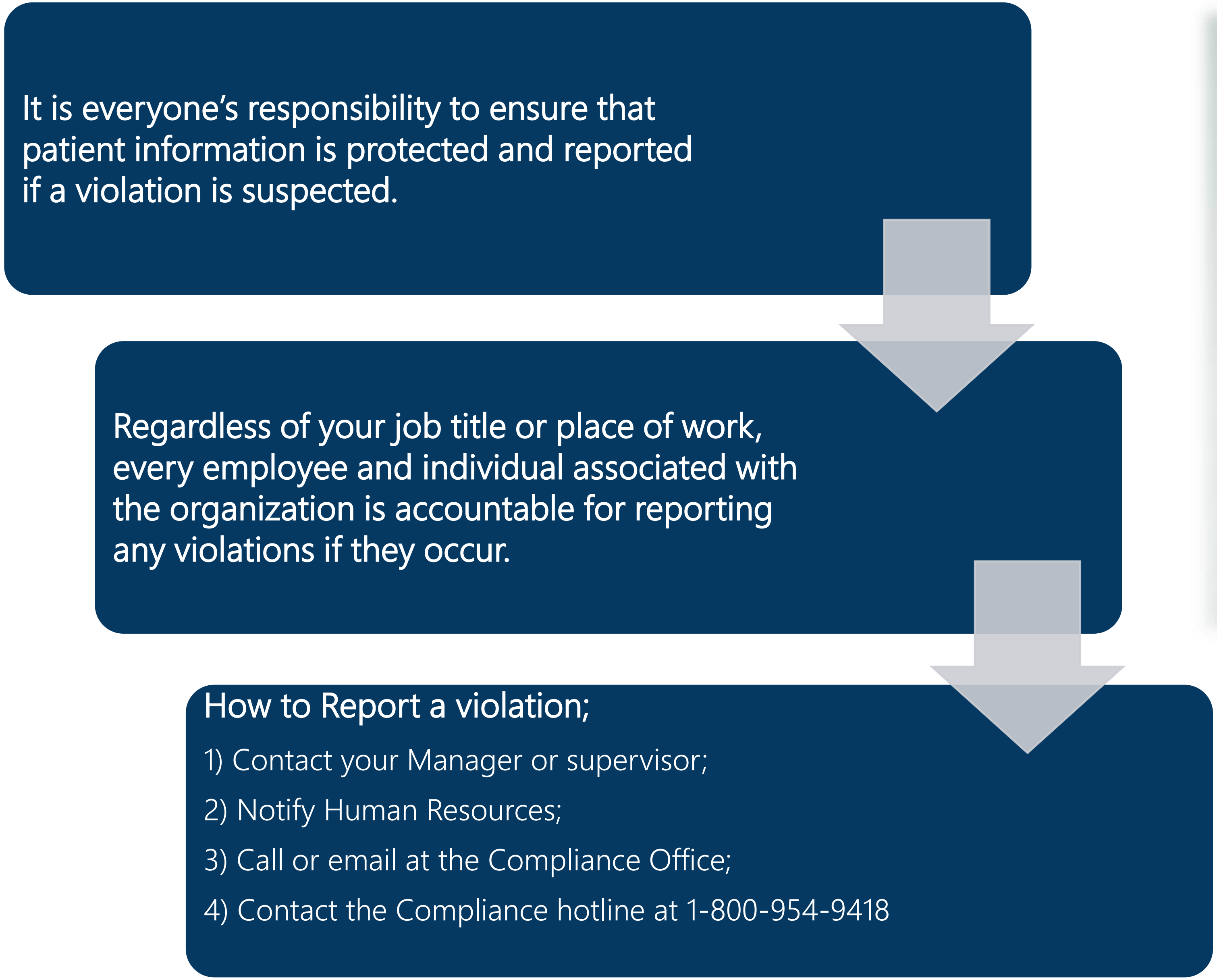
What is Protected Health Information (PHI)?

- Anything that can be used to identify an individual including;

Name
Social Security Number
Mailing Address
Credit Card / Bank Account Number
Phone Number
Billing Account Number
E-mail address
Insurance Subscriber Number
Date of Birth

Anything that can be used to identify the patient including a unique situation or full-face picture!

The responsibility of HIPAA and protecting PHI starts with you!



It is everyone's responsibility to ensure that patient information is protected and reported if a violation is suspected.

Regardless of your job title or place of work, every employee and individual associated with the organization is accountable for reporting any violations if they occur.

How to Report a violation;

1) Contact your Manager or supervisor;

2) Notify Human Resources;

3) Call or email at the Compliance Office;

4) Contact the Compliance hotline at 1-800-954-9418

HIPAA Breach

- ✓ A Breach is an unauthorized acquisition, access, use or disclosure of unsecured PHI.

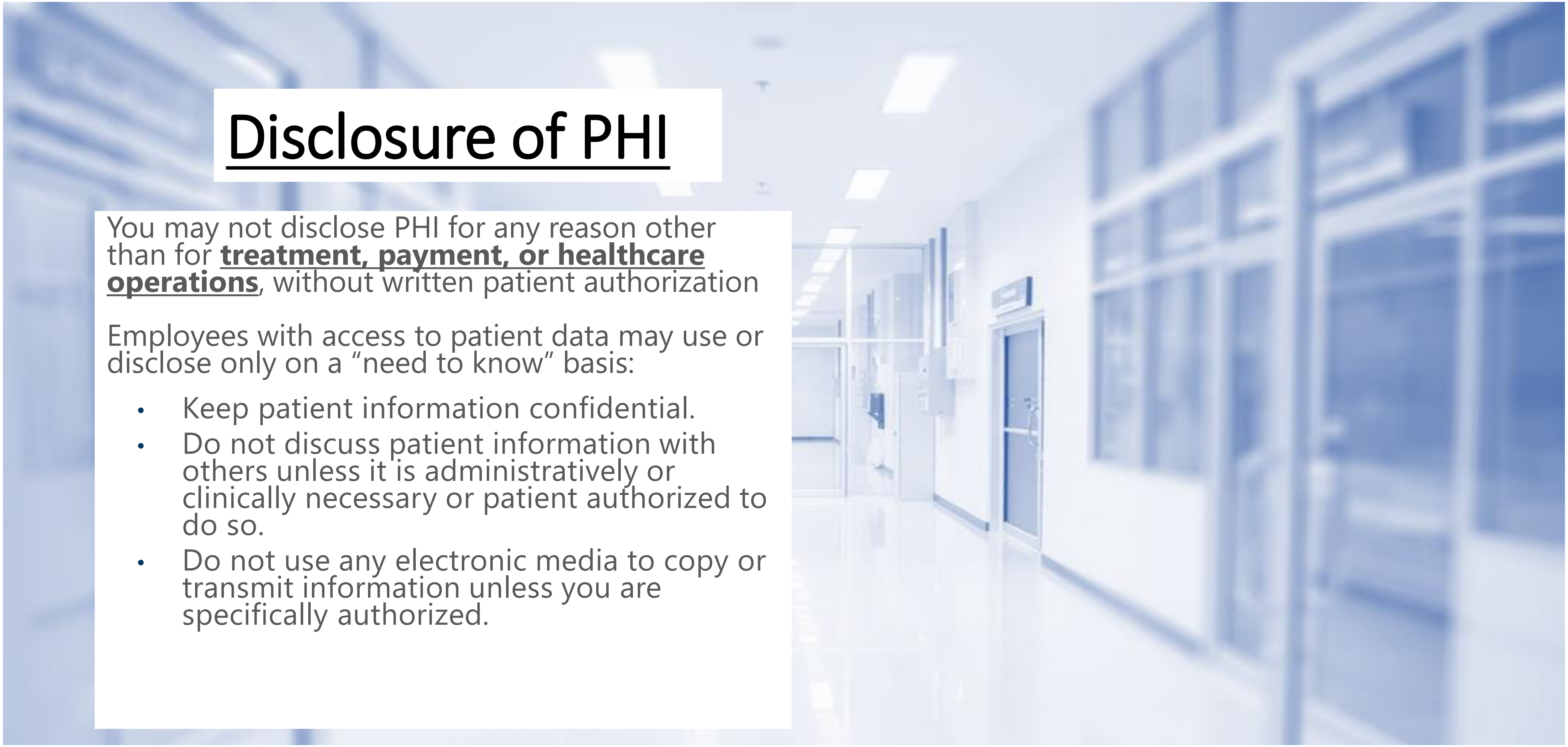
A breach could result from the following;

- Unauthorized access to PHI
- Accessing more than minimum necessary
- Improper disposal of confidential materials
- Failing to log of when leaving a workstation
- Sharing confidential information, including passwords

Disclosing PHI

When is it appropriate to share PHI?

- Generally, you may use or disclose PHI without an authorization for these purposes:
  - For treatment of a patient, including arrangements for transfer and referral care;
  - To get payment for healthcare services;
  - Approved healthcare operations such as quality review, competency activities, auditing for compliance programs, and mandatory reporting.



Disclosure of PHI

You may not disclose PHI for any reason other than for **treatment, payment, or healthcare operations**, without written patient authorization

Employees with access to patient data may use or disclose only on a “need to know” basis:

- Keep patient information confidential.
- Do not discuss patient information with others unless it is administratively or clinically necessary or patient authorized to do so.
- Do not use any electronic media to copy or transmit information unless you are specifically authorized.

Discussing PHI

- Only discuss for the purposes of Treatment, Payment and Operations.
- Be mindful of your surroundings and avoid discussing PHI beyond what's necessary.
- Keep voices down and avoid discussing PHI in public areas.
- Use private spaces for discussions with faculty, clients, and patients.
- Conduct phone conversations in private spaces and confirm the identity and authority of the recipient before discussing PHI.

Authorizations

Verbal Authorizations

In some cases, you can release or use information with the patient's verbal. Such as;

- When a patient asks that care and treatment information be shared with their family members or friends.
- Immunization records can also be released to a patient's school with a verbal authorization.

Written Authorizations

A written authorization should be obtained when the information is NOT;

- For treatment, payment, or healthcare operations.

Extra Caution! –

The sharing of confidential information related to certain diagnosis and treatment are afforded a higher level of protection under New York State Laws,

- Alcohol/Substance Abuse	- Mental Health
- Child Abuse	-Genetics
-HIV- AIDs Related Information	-Minors under the age of 18

Access to Protected Health Information

- Is based on your work duties and responsibilities.
- Are limited to only the minimum necessary information needed to do your work.
- Should only be done for Treatment, Payment, Operations.

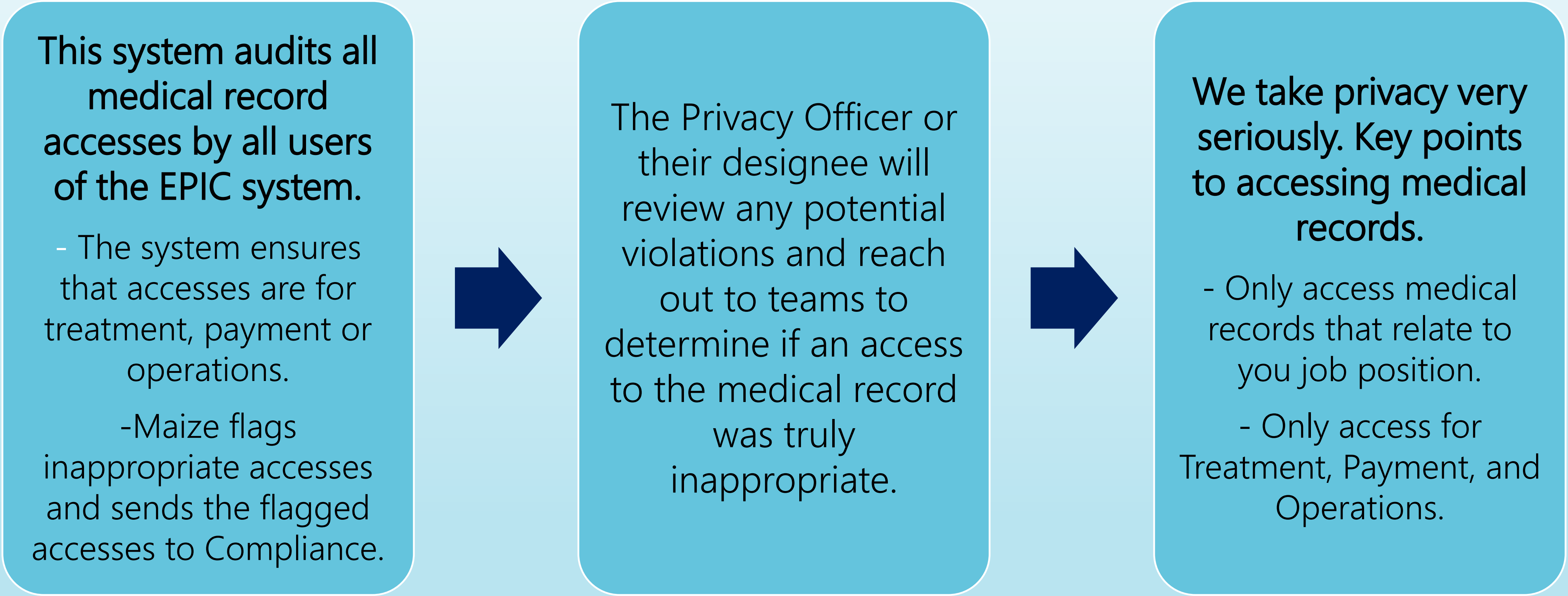
You may not access;

- Your children;
- Family members;
- Co-workers;
- Friends;
- Neighbors;
- High profile patients;
- Your own MR.

**See policy HIPAA Manual- Employee Medical Record Access and Use Policy, MV-05-034.

MVHS | mvhealthsystem.org

Access Privacy Monitoring System Software - Maize



This system audits all medical record accesses by all users of the EPIC system.

- The system ensures that accesses are for treatment, payment or operations.

-Maize flags inappropriate accesses and sends the flagged accesses to Compliance.

The Privacy Officer or their designee will review any potential violations and reach out to teams to determine if an access to the medical record was truly inappropriate.

We take privacy very seriously. Key points to accessing medical records.

- Only access medical records that relate to you job position.

- Only access for Treatment, Payment, and Operations.

Make sure not to access medical records without a proper HIPAA authorization

Am I allowed to access my friends, family, and my medical record? I do have access to the electronic medical record.

No, HIPAA policies and procedures state that we should not access any medical records of anyone including our own, that is not part of our job!

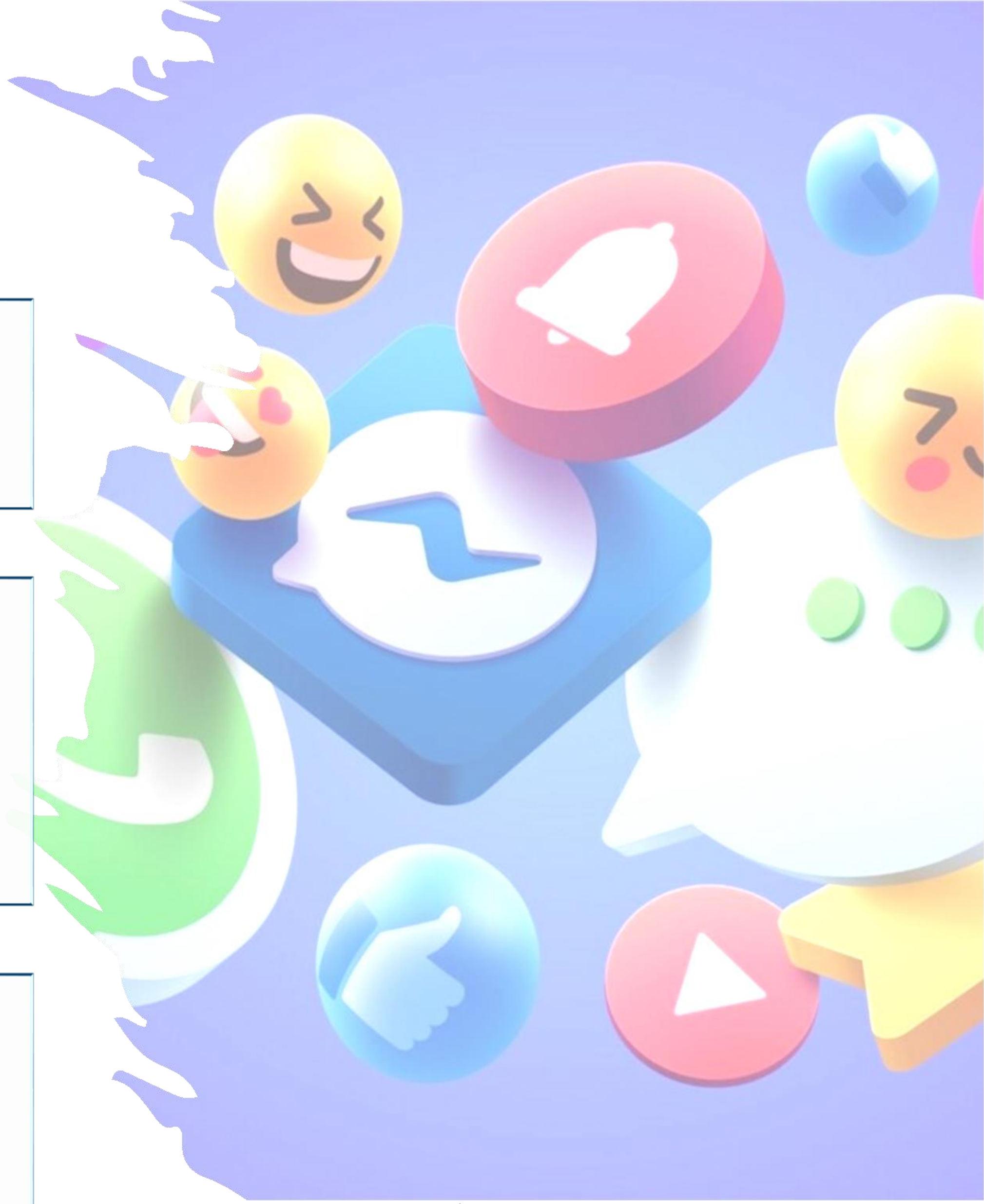
- Failure to follow the proper process may result in a HIPAA violation and can lead to disciplinary action up to termination.
- If access to a friend, family, dependent or yourself is required, reach out to the Medical Records department for assistance.

Social Media

- Do not share or post any information about patients on any social networking sites (Facebook, Instagram, Snapchat, Twitter).

- Individuals who post patient information or photos to social media are in a direct violation of MVHS policies and procedures as well as HIPAA privacy regulations.
- Those that are in violation of this policy can be subject to disciplinary action up to and including termination.

- Posting information, even without posting a patient's name, may be a violation because in many cases there is enough information that the name of the patient can be reasonably inferred.



Verifying Patients

Importance of Identifying Patients

- Identifying patients and their protected health information accurately is a critical factor of patient safety and prevents the potential for HIPAA Privacy violations.
- At minimum, a team member must check the name and date of birth of a patient at **every instance** of interaction with the patient.

Essential areas that identification of the patient MUST be performed is the following;

- When calling a patient and bringing them to a room
- When giving medications
- Before testing a patient
- While labeling specimens at the bedside
- When going over discharge instructions

HIPAA Do's and Don'ts

Do's	Don'ts
Get a new password if yours has been compromised.	Never let someone else use your password.
Excuse yourself from taking care of individuals with whom you have a personal relationship.	Access, view or print your own, friends or families medical record's.
Cover up any patient information so that others cannot view it.	Leave a paper copy of a document with medical information in public areas.
Make sure to use a fax sheet and verify fax numbers before faxing PHI.	Discuss patient information in public areas.
Use a soft voice when in earshot of other patients and visitors, if it is not possible to do so then use a private area for the conversation.	Leave a portable computer or device that contains PHI unsecured or unattended, especially when you are off premises.

HIPAA Breaches can lead to…

Employees violating HIPAA will be subject to disciplinary action up to and including **Termination**.

Office of Civil Rights can impose jail time and up to $250,000 in **personal fines**.

The individual(s) whose PHI was violated can take **civil action** against anyone who violates HIPAA .

Individual employees can be reported to licensing agencies for a HIPAA breach and may **lose their professional license**.

Information Technology Security

Information Technology Security

- Basic Information Technology Security
- Understand what phishing is
- How to manage and protect passwords
- Where to find HIPAA policies
- Information Technology Security Do’s and Don’ts

Be Technology Wise:

Be sure to not click suspicious links in your email.

Pay attention to suspicious activity when using electronic devices when accessing Electronic Protected Health. Information "ePHI."

Know HIPAA rules and policies to manage ePHI.

Email:

Only use GroupWise email and not your personal email.

MVHS uses GlobalCerts SecureMail Gateway to securely transfer ePHI.

Place secure in brackets [secure] in the subject line of your email to send a secure mail.

MVHS does not allow anyone to access personal email on production devices.

Safeguard Your Computer's Information

BEFORE YOU WALK AWAY…………..

LOCK YOUR DISPLAY

- ✓ Press the Ctrl, Alt, and Delete keys at the same time. Then click on 'Lock.'

****You are responsible for any information that is accessed or used inappropriately when you walk away from the computer*

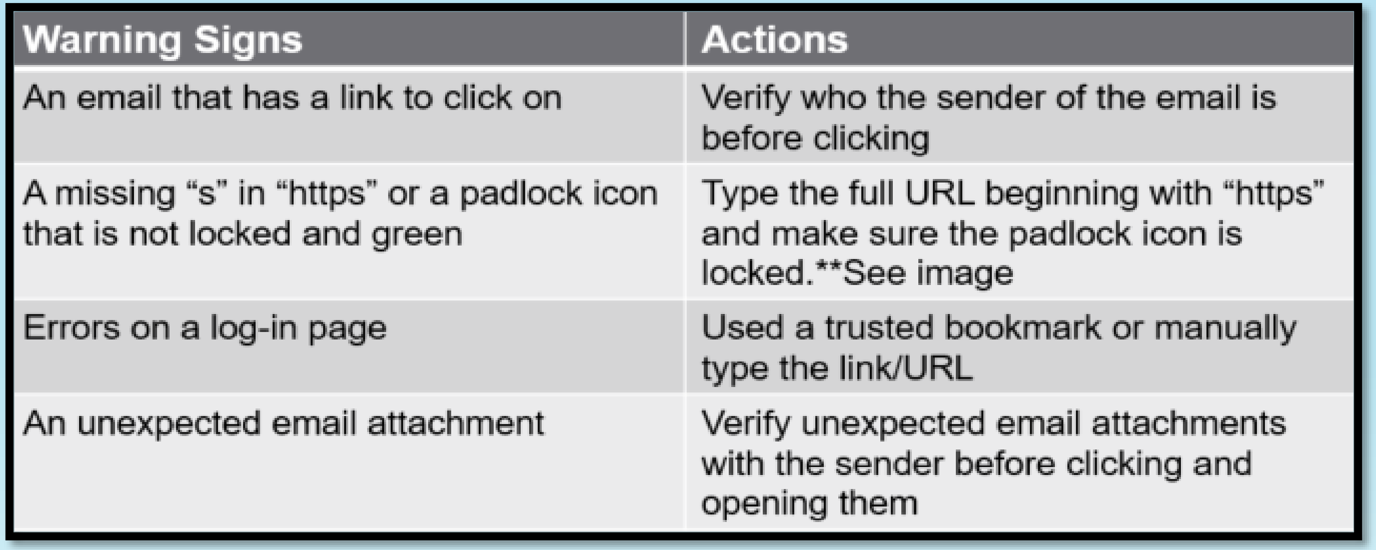
What is Phishing?

- Phishing is the fraudulent practice of sending emails claiming to be from reputable sources in order to induce individuals to reveal personal information such as usernames and passwords.

Examples of Phishing:

- An email directing someone to download an attachment.
- An email directing the recipient to enter personal details.
- An email warning the recipient that they have a computer virus.
- An email directing the recipient to call a help line to assist with their computer issues.

How to Defeat Phishing:

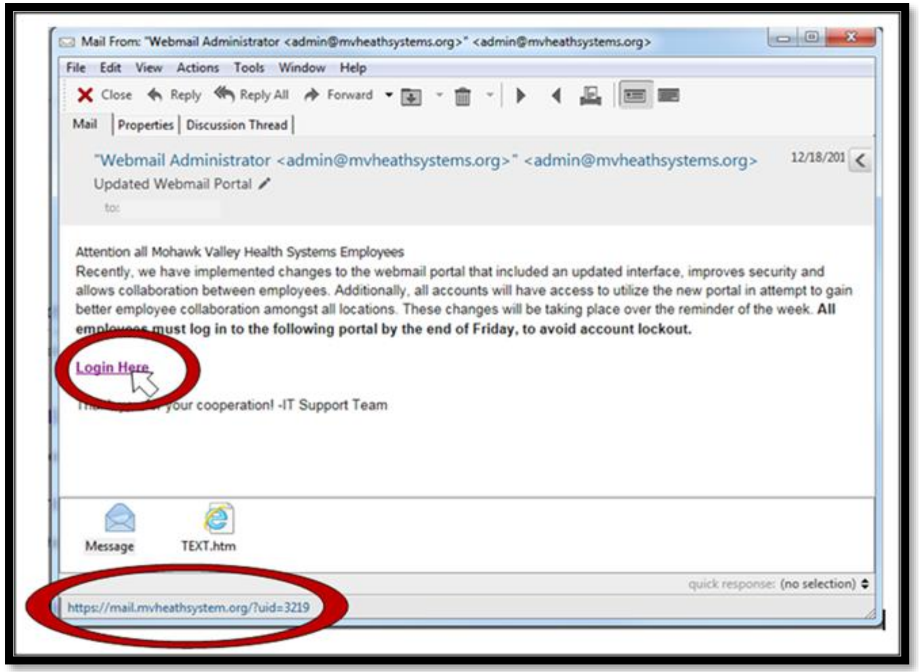


Warning Signs	Actions
An email that has a link to click on	Verify who the sender of the email is before clicking
A missing "s" in "https" or a padlock icon that is not locked and green	Type the full URL beginning with "https" and make sure the padlock icon is locked.**See image
Errors on a log-in page	Used a trusted bookmark or manually type the link/URL
An unexpected email attachment	Verify unexpected email attachments with the sender before clicking and opening them

MVHS | mvhealthsystem.org

How to Verify Where Links Will Take You:

Hover your mouse curser over where the Email wants you to click, it will generate the actual web address that the link will take you to in the lower left-hand corner as shown below. This might not always say “Login Here” it might say “Click Here”.



Mail From: "Webmail Administrator <admin@mvheathsystems.org>" <admin@mvheathsystems.org>

"Webmail Administrator <admin@mvheathsystems.org>" <admin@mvheathsystems.org> 12/18/201

Updated Webmail Portal

to:

Attention all Mohawk Valley Health Systems Employees
Recently, we have implemented changes to the webmail portal that included an updated interface, improves security and allows collaboration between employees. Additionally, all accounts will have access to utilize the new portal in attempt to gain better employee collaboration amongst all locations. These changes will be taking place over the reminder of the week. **All employees must log in to the following portal by the end of Friday, to avoid account lockout.**

Login Here

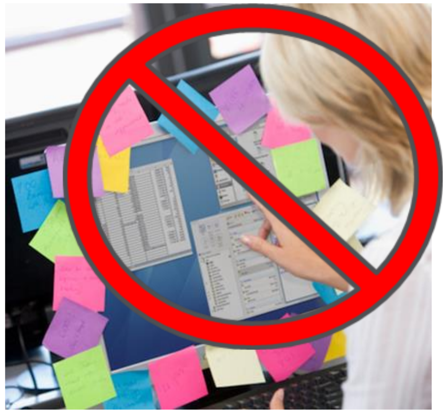
Thank you for your cooperation! -IT Support Team

quick response: (no selection)

https://mail.mvheathsystem.org/?uid=3219

If you have a suspicious email that may be a possible phishing email, the best action would be to “right click” on the email and assign it to Junk Mail, this will also delete the message from your mailbox. Another best practice when it comes to security is the “See something, Say something” approach and mention suspicious activity to the I.T. Helpdesk at 315-917-9600 or email at helpdesk@mvhealthsystem.org.

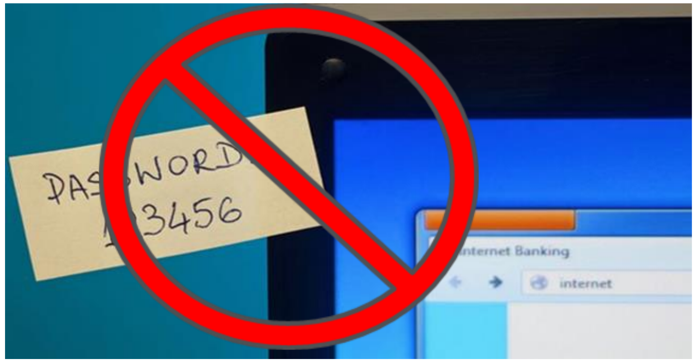
Password Management



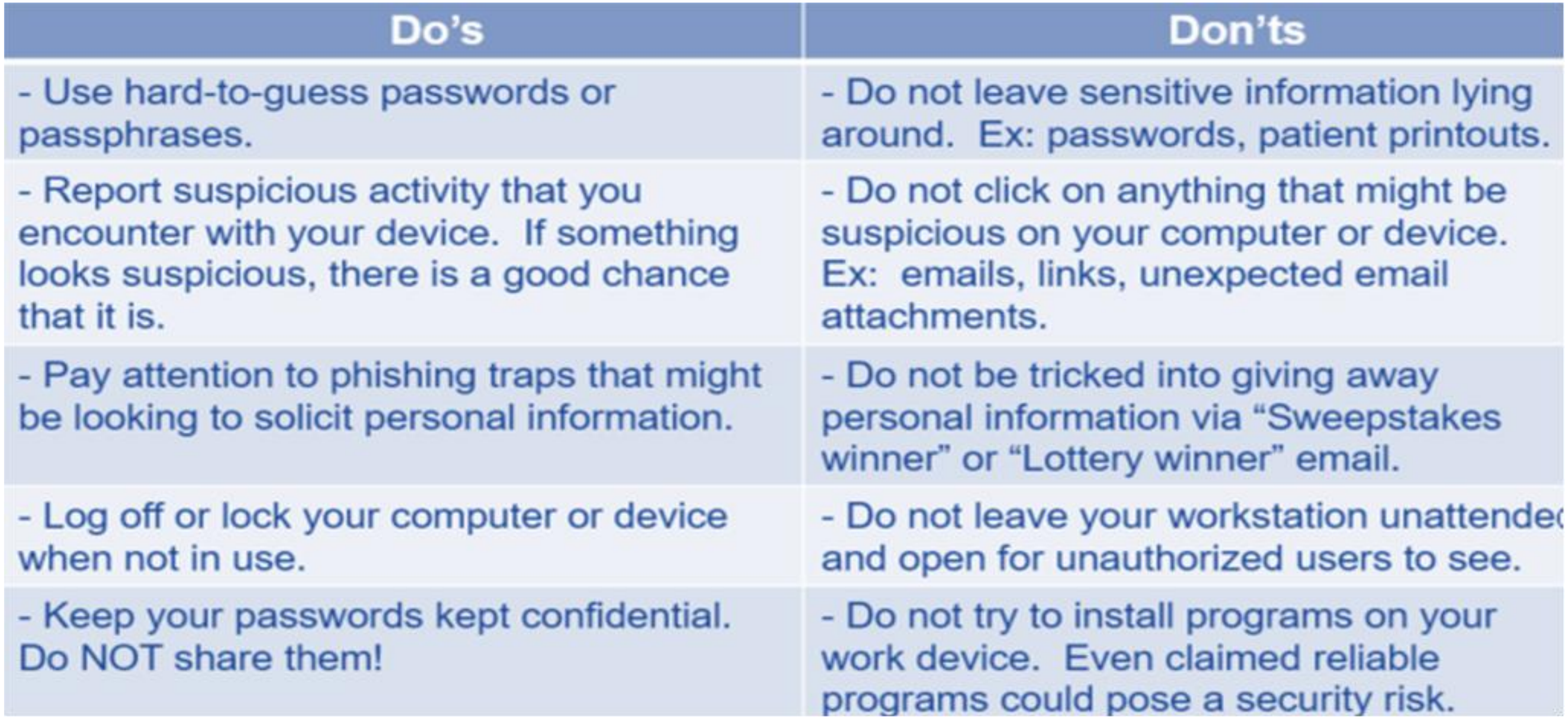
- Make passwords easy to remember but hard to guess.
- Passwords need to be a minimum of 10 characters.
- Passwords need to include at least three of the following: uppercase letter, lowercase letter, symbol and number.
- Passwords will need to be changed every 365 days.
- Users should also change their password if they feel it is known to someone else or has been compromised.

Password Protection

- Never share your password(s) with ANYONE (ex) IT Staff, Managers, Vendors etc.
- Never write passwords down.
- Never write passwords down and post them on your screen or hide them in a desk drawer.



General Information Technology Security Do's and Don'ts



Do's	Don'ts
- Use hard-to-guess passwords or passphrases.	- Do not leave sensitive information lying around. Ex: passwords, patient printouts.
- Report suspicious activity that you encounter with your device. If something looks suspicious, there is a good chance that it is.	- Do not click on anything that might be suspicious on your computer or device. Ex: emails, links, unexpected email attachments.
- Pay attention to phishing traps that might be looking to solicit personal information.	- Do not be tricked into giving away personal information via "Sweepstakes winner" or "Lottery winner" email.
- Log off or lock your computer or device when not in use.	- Do not leave your workstation unattended and open for unauthorized users to see.
- Keep your passwords kept confidential. Do NOT share them!	- Do not try to install programs on your work device. Even claimed reliable programs could pose a security risk.

E-Mail and Internet Access

Email

- Your MVHS e-mail account may have your name as the account owner, but it is the property of MVHS.

- DO NOT use personal emails to send protected health information

- E-mail accounts are monitored for proper use.

- Do not send patient information to an external e-mail account unless it is encrypted typing “[Secure]” in the subject line. Contact the IT Department with any questions.

- Viruses, Malware, Trojans, Worms, and Key Stroke Trackers are all forms of malicious software used to corrupt computer systems.

- Do not install any malicious software onto an MVHS computer.

- Ransom Ware is a form of malicious software that has become more prevalent in the Healthcare Industry and is costing healthcare more losses each year. Do not click on a link or attachment from an external e-mail account sent to you by someone that you do not know.

- All e-mails should contain a confidentiality statement.

Internet

- Applications for internet access must be completed and signed by your Department Manger and Vice President.

- The internet is to be used for MVHS business purposes only.

- Internet accounts are audited for improper use.

Working From Home or Remotely?
Securing your remote connection

- Verify your PC or laptop is running the current and most up to date operating system and security patches.
- Check to make sure your PC or laptop is running current and up to date with Antivirus software.
- When connecting to the internet or Wi-Fi to work remotely, make sure you are connecting to a trusted source and not a public or unsecure Wi-Fi. (i.e. coffee shop, or hotel Wi-Fi).
- Ensure you password protect, lock and secure any information that you may be working on at home.

MVHS | mvhealthsystem.org

Reporting a Suspected HIPAA OR Security Violation

You can report a suspected violation of our patients' privacy to:

Privacy Violations:

The Privacy Officer at (315) 624-5117.

The Legal/Compliance Department at (315) 624-5050.

Security Violations:

The Security Officer at (315) 624-5823.

IT Help Desk at (315) 917-9600.

Anonymous Reports:

Compliance Hotline at (800) 954-9148 or www.mvhealthsystem.ethicspoint.org.

It is your responsibility to read this training and abide by the official privacy and security policies of Mohawk Valley Health System.

The information contained in this slideshow is used for educational purposes for orientation and annual mandatory education. For the official policies of MVHS, refer to PolicyStat.