Information Technology Security and HIPAA Privacy

2023 Mandatory Education

MVHS | mvhealthsystem.org

Information Technology Security

Learning Objectives

- Basic Information Technology security guidelines
- 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 NetMail Encrpt to securely transfer ePHI.
  Place secure in the subject line of your email.
- Here are some of the Novell Groupwise logos with which to familiarize yourself.
- MVHS does not allow anyone to access personal email on production devices.

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:

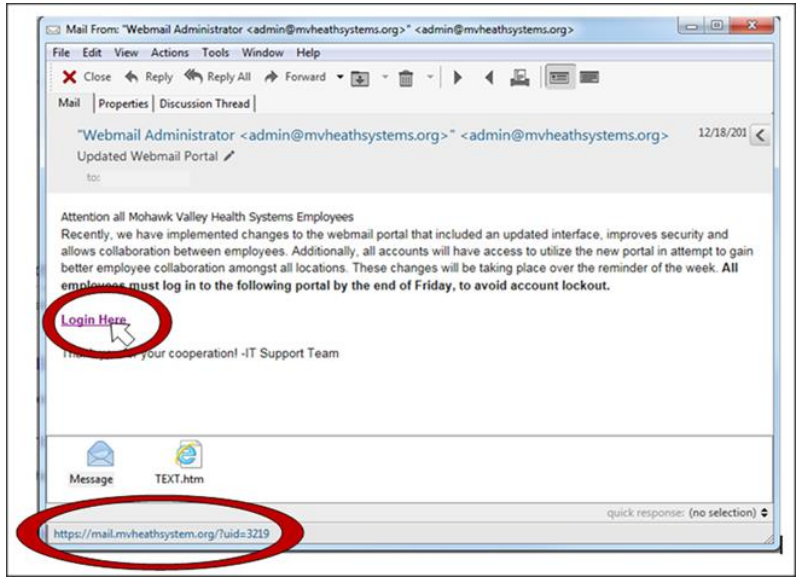
- An email directing someone to download an attachment.
- An email directing the recipient to enter personal details.
- An email warning the recipient that they have a computer virus.
- An email directing the recipient to call a help line to assist with their computer issues.

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

- **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”.



- Email & Suspicious Activity- What Ifs?

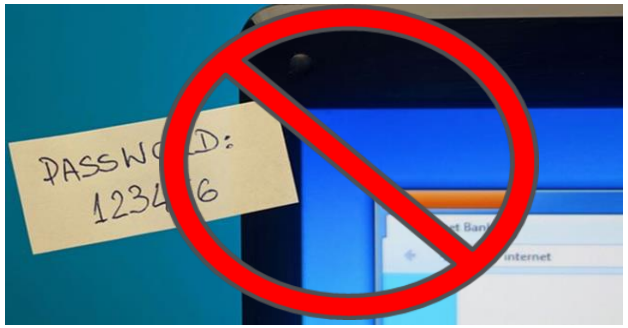
  If you have a suspicious email that may be a possible phishing email, the best action would be to “right click” on the email and assign it to Junk Mail, this will also delete the message from your mailbox. Another best practice when it comes to security is the “See something, Say something” approach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

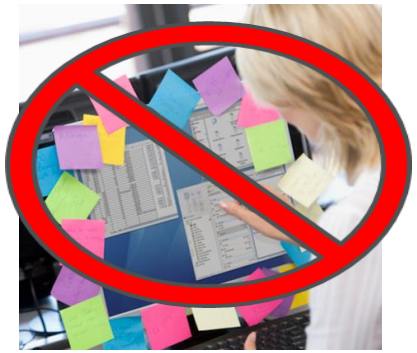
Password Management

- Make passwords easy to remember but hard to guess.
- Passwords need to be a minimum of 10 characters.
- Passwords need to include at least one 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.

MVHS | mvhealthsystem.org

Working From Home or Remotely?

Steps to take to secure your remote connection to the workplace

- 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 WiFi to work remotely, make sure you are connecting to a trusted source and not a public or unsecure WiFi. (i.e. coffee shop, or hotel wifi).
- Ensure you password protect, lock and secure any information that you may be working on at home.

HIPAA Privacy and Security

Keeping our Patients' Medical Information Confidential

Federal HIPAA Regulations

- The Federal HIPAA Privacy Rule was implemented in 2003. The Rule requires health care providers to develop and implement policies and procedures to protect patients' "protected health information" PHI.

- The Federal HIPAA Security Rule was implemented in 2005. The Rule requires health care providers to develop and implement policies and procedures in order to safeguard electronic health records.

Safeguards Used to Keep PHI Confidential/Secure-with Examples

Administrative Safeguards
- Policies and Procedures to implement privacy and security measures.
- Perform an annual Risk Assessment which is used to identify and analyze risks regarding securing PHI.
- Review unusual activity in the computer system.
- Require "Business Associates Agreements" with vendors who have access to the PHI of our patients.

Technical Safeguards
- Use of encryption software.
- Firewall software.
- Virus detection software.
- Use of usernames and passwords.

Physical Safeguards
- Use of locks on doors where PHI is stored (paper records, computer rooms).
- Use of cameras for secure areas.
- Fire doors / special fire extinguishers for main computer systems.

MVHS | mvhealthsystem.org

What is Considered Protected Health Information (PHI)?

- Any (Past, Present, or Future) physical or mental health information regarding the patient whether in electronic, paper, or oral format, including healthcare treatment information. Billing and payment information for healthcare services.

- **Information that can be used to identify the patient:**

- 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.

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.

Verbal Authorization - In some cases, you can release or use information with the patient's verbal authorization. A common example of this would be 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 Authorization Needed - A written authorization should be obtained when not using information for treatment, payment, or healthcare operations, and when verbal authorization is not sufficient.

Authorizations are usually required when copies of records are requested. Regulations relating to the release of patient information are **extensive** and many HIPAA violations are due to inappropriate release of records or not releasing records when it is required. For any questions you may contact the Privacy Officer or the Health Information Management Department (HIM).

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, for example:

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

How Does MVHS Protect Patient Information?

Electronic Information:

- Access is controlled by requiring the use of a username and password. (Don't share your password, or post it visibly in your work area).
- Restricting user access to functions based upon their Job Description in order to meet the Minimum Necessary standard.
- Keeping electronic PHI on a secure network.
- Requiring PHI stored on PC's and USB drives to be encrypted.
- Back up tapes are stored in a secure locked area.
- Physical access to the main computer systems are locked and monitored 24/7.
- Users should not leave a computer unattended without logging out of the program that they are using.
- Audits of user access.

Paper Charts:

- Should be locked up when unsupervised.
- Visitors should not be allowed into a Medical Record area unsupervised.
- Charts on the nursing unit need to stay with the patient.
- Documents should never be left in public view.
- Ensure proper disposal (place in a locked shred bin).

Verbal Information:

- Do not discuss patient information in public areas such as hallways, elevators, or lunch room.
- **Visitors should be asked to leave the room before talking to a patient about PHI, unless the patient agrees that the visitor may stay.**

The Minimum Necessary Requirement

- Minimum necessary means using or disclosing the least amount of information you need to perform your job.
- Even though you may have access to specific databases of information, the information within those databases should only be accessed because your job requires you to for treatment, payment, or healthcare operations.

<u>Ask yourself before looking at any patient information</u>

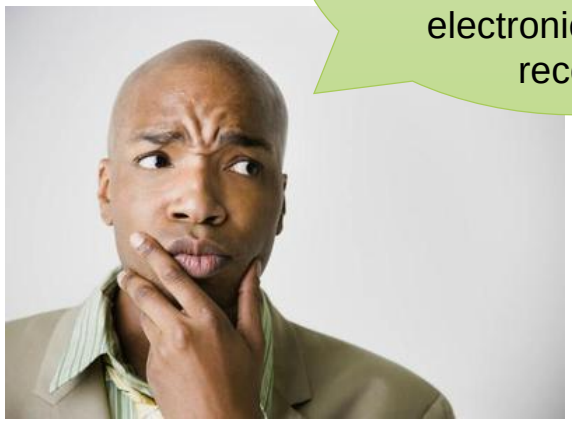
- Do I need this in order to do my job or provide patient care?
- What is the least amount of information I need to share with a person in order for them to do their job?
- What are the steps to take to release PHI?
  - The Health Information Management Department (HIM) is responsible for Release of Information (ROI) functions within both facilities.

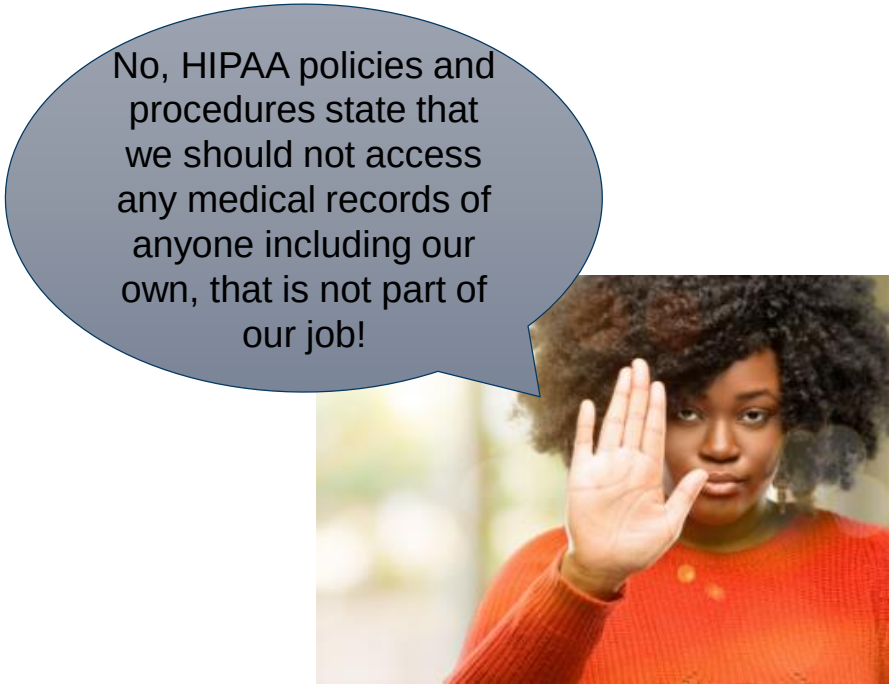
HIPAA and Social Media

- 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 are violating HIPAA privacy regulations and MVHS privacy policies and are subject to disciplinary action up to and including termination.**

- Even discussing or posting information about a patient without referring to their name may be a violation because in many cases there is enough information that the name of the patient can be reasonably inferred.
- Any postings to official MVHS websites or social media sites must be pre-approved and have patient authorization / release forms signed by the patient prior to posting.

- Make sure not to access the following records without a proper HIPAA authorization or going through the proper process by going to the Medical Records department.





Failure to follow the proper process may result in a HIPAA violation and can lead to disciplinary action up to termination.

HIV/AIDS Disclosures

- With very limited exceptions, a patient's HIV/AIDS status is confidential and shall not be disclosed to anyone without a written consent signed by the patient.
- One of the few exceptions where a patient's HIV/AIDS status may be disclosed without written consent is in the case where a provider taking care of the patient needs the information in order to manage the patient's care.
- Never disclose a patient's HIV/AIDS status to a visitor in the room without the patient's written consent.

HIV/AIDS

- **Article 27–F of the NYS Public Health Law protects the confidentiality and privacy of *anyone* who:**
    - Has HIV infection or HIV/AIDS-related illness; has been tested for HIV; has been treated for HIV/AIDS-related illness; or has been exposed to HIV.

- **The General Rule is No Disclosure**. A patient's HIV-related information is confidential and shall not be disclosed to anyone unless the patient or their legally authorized representative has signed a HIV-related information release form (DOH 2557). There are only a few exceptions where the law allows disclosure of HIV-related information without a patient HIV-related information release form.

- **There are *very few* Exceptions to the "No Disclosure" Rule** where a signed patient release for a disclosure is not required.

- Examples:
    - Providers taking care of the patient – but only as necessary to provide appropriate care or treatment.
    - Hospital staff, review organizations or government agencies – but only those authorized to access medical records and then only if the information is necessary to supervise, monitor of administer a health or social service.
    - The patient's insurance company – but only if there is a signed general release and then only if the information is necessary to pay for medical care.
    - Disclosure per a court order – but only if the order specifically directs the release HIV-related information and is signed by a judge.

If you have any questions about whether you may disclose HIV-related information without having a patient release, please contact your supervisor or the Privacy Officer

What information is protected by Article 27-F? "Confidential HIV-related information", which is any information showing a person:

a) Had an HIV-related test such as a HIV antibody, PCR, CD4 for HIV, or a viral load test.
b) Has been exposed to HIV.
c) Has an HIV infection, HIV-related illness, or AIDS (such as PCP pneumonia or Kaposi's Sarcoma – even without the mention of HIV or AIDS).
d) Has any of these conditions and has information on any of their sexual or needle-sharing contacts.

HIV / AIDS – continued

- In order to release any HIV/AIDS related information, a valid **HIV Release Form** is required to be signed and dated by the patient, or if the patient lacks capacity to consent, by a qualified person under section 18 of the Public Health Law or by a person authorized by law to consent to healthcare for the patient. The release must specifically authorize the disclosure of HIV-related information; and must contain: The names of the protected person, the provider and the recipient, the reason for the disclosure and the time frame the consent is effective.

- Do not have a discussion about a patient's HIV status or history in front of a visitor. Do not assume that the visitor is aware of the patient's HIV status. Do not assume that the patient consents to your notifying anyone of his/her HIV status. Ask visitors to leave the room.

- It is not permissible to disclose an individual's HIV-related information to other health care providers solely for infection control purposes. Casual contact creates no risk of HIV transmission, and any risk of direct occupational exposure to HIV that may be encountered by health care workers can be effectively minimized through universal infection control precautions.

- If you are concerned about the patient possibly transmitting HIV to a partner or other person due to sharing of needles, there are specific New York State privacy requirements that must be followed. Do not notify a patient's partner or contact. Please contact your supervisor or the Privacy Officer or the Legal Department for guidance.

- **Criminal penalties for violations.** Under State law, anyone who illegally discloses confidential HIV-related information may be punished by a fine of up to $5,000 and a jail term of up to one year.

- **Questions?** For more information about HIV confidentiality, please contact the Privacy Officer or the New York State Department of Health HIV Confidentiality Hotline.

Verbal Disclosures

- Patients have the misconception that incidental disclosures are HIPAA violations. Taking care of the patient is primary.
- HIPAA requires hospitals to take “reasonable precautions” to prevent incidental disclosures.

Recommendations

- If there are visitors or relatives that are with the patient, do not assume that the patient wants the visitor or relative to know about their medical information. Ask the visitors in the room to leave so that you can have a private conversation with the patient. If the patient states that it is OK for the visitor or relative to be involved in conversations related to the patient’s medical information, then that is fine. Document the patient’s verbal agreement / refusal. Be careful discussing a patient’s mental health status with visitors.
- HIV/AIDS related disclosures require a signed written authorization (DOH Form 2557). Do not discuss HIV/AIDS information in front of any visitors.
- In certain limited situations the Provider may disclose medical information to a patient’s care giver, without the patient’s permission. This is left to the Provider’s discretion and should only be used in a situation to prevent harm to the patient or others.
- Pay attention to who may overhear a conversation about a patient’s medical condition. Talk with a hushed tone. Avoid talking over other individuals to communicate unless it is urgent to the patient’s care.

Paper Disclosures

- **Make sure to review all papers that are being handed to or mailed to a patient in order to make sure that all of the papers are for the intended patient. This is one of the more common HIPAA violations at MVHS.**
- This is especially relevant to discharge papers and test results.
- Don’t just replace an incorrect patient’s information with a patient label. Create a new document if the information has the wrong patient’s demographics on it.
- Always use a cover sheet when sending a fax, even to an internal department, place your fax number on the cover sheet. Verify the fax number to which you are sending information. Always dial 9 first when faxing to a number outside of the hospital.

Telephone Conversations

- If a relative or friend of the patient calls, you should try to verify who the caller is by asking some basic questions to verify their identity.
- If the patient is able to communicate coherently, ask the patient if it is OK to share their medical information with the person calling, over the phone.
- You can give the patient's location and general condition (Fair, Serious, Critical) without asking the patient, unless they have opted out of the hospital's directory. All Psychiatric Inpatients and Prisoners are automatically opted out of the Directory.
- If the patient is not able to give consent, use your professional judgment when providing information about the patient to others.

Reasonable Safeguards

- Speak quietly when discussing a patient's condition with family members in a waiting room or other public area.
- Avoid using patients' names in public hallways and elevators, and post signs to remind employees to protect patient confidentiality.
- Isolate or lock file cabinets or record rooms.
- Provide additional security, such as passwords, on computers maintaining information.

(Taken directly from information provided by the Office of Civil Rights, who enforces HIPAA Compliance)

Computer Terminals

- While the Hospital has appropriate safeguards in place (computer time outs) you should never use a computer unless you are logged on using your own user name and password.
- Log out of a computer when you leave for more than a few minutes.
- If leaving the computer for only a minute you may minimize the screen without logging off.

New Auditing of Records

- There will be a new system implemented June 2023 called Maize.
- This system will audit all medical record accesses to ensure that our team members are being HIPAA compliant.
- The Privacy Officer or their designee will review any potential violations and reach out to teams to determine if it was truly an appropriate access of medical records.
- We take HIPAA very seriously, only access medical records that relate to your job position.

HIPAA Do's and Don'ts

Do's	Don'ts
Get a new password if yours has been compromised.	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 medical record or those of a friend or family unless you are treating them.
Cover up patient information your are working on when someone approaches your desk.	Leave a paper copy of a document with medical information in public areas.
Make sure to use a fax cover sheet and verify fax numbers before faxing PHI.	Discuss patient information in public places.
Use a soft voice when in earshot of other patients and visitors, if it is not possible to use a private area.	Leave a portable computer or device that contains PHI unsecured or unattended, especially when you are off premises.

Report a Suspected Violation

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

Privacy Violations:

The Privacy Officer
The Legal/Compliance Department

Security Violations:

The Security Officer
IT Help Desk

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.

MVHS | mvhealthsystem.org

EXIT

Click the **Take Test** button when you are ready to complete the requirements for this course.

Please submit any questions or feedback on this presentation via email to Kathy Fiesthumel, KFIESTHU@mvhealthsystem.org. Please include the module title with your message.