Next Exit

HIPAA Privacy and Security

Rochelle Steimel, HIPAA Privacy Officer
Judy Smith, Staff Development
June 2018

MUNSON HEALTHCARE

Progress Page

Back Next Exit

Goals and Objectives

Course Goal:
To introduce the staff of Munson Healthcare to the concepts of protecting patient confidentiality according to Munson Healthcare policy and HIPAA federal law.

Course Objectives:
After completing this course, the participant will be able to:

1. Comply with MHC policies related to HIPAA.
2. Describe disciplinary action related to HIPAA violations.
3. Identify how users can help protect the security of information within the Munson network.
4. State how to report privacy and security incidents.

Progress Page

Back Next Exit

Patient Privacy

Strict Federal HIPAA laws mandate patient privacy and computer security:

- To protect against inappropriate access to medical records.
- To prevent verbal breaches.
- To avoid any invasion of privacy.
- To keep computers and confidential information protected.

Progress Page

Back Next Exit

Avoid Privacy Complaints

Share and access information only if there is a specific job-related need to know.

Do not access a chart due to curiosity or concern.

Avoid discussing patient care where it can be overheard and avoid discussing patient information with other staff who have no job-related need to know.

Do not discuss patients with your family and friends!

Progress Page

Back Next Exit

Permission to Share

Can I share information with the family and friends of a deceased patient?

Talking with the family and friends of a deceased person is now more permissible with the 2013 guidelines.

- It helps with the grieving process.
- It helps the family to understand what has happened.

Information may be shared unless the patient previously stated that he/she did not want his/her medical information to be shared.

Progress Page

Back Next Exit

Keep Good Professional Boundaries

Do NOT access the electronic medical record of:

- Your children or step-children
- Your spouse or ex-spouse
- Victims in the news
- Your neighbors
- Your friends
- Your family
- Celebrities
- And especially your co-workers…

Unless there is a job-related need to know!

Progress Page

Back Next Exit

Job-Related Need to Know

Before accessing a medical record, ask yourself:

"Do I need this to do my job?"
"Will my supervisor agree with me?"
"Am I willing to lose my job over this?"

If no, then **STOP!**

Progress Page

Back Next Exit

Job-Related Need to Know *(cont.)*

When do I have a job-related need to know?

When it is for:

- Patient treatment
- Continuity of care
- Patient safety
- Payment
- Operations (e.g., quality assurance, peer review, reporting to the State of Michigan)

Progress Page

Back Next Exit

Permissible Access

Examples of permissible access:

- The record of a family member, but only if you have a job-related need; e.g., you are involved in their care at work
- The business, financial, or registration records of a family member or co-worker, but only if you have job-related need; e.g., payment-posting or billing

Progress Page

Back Next Exit

What Patient Information is Protected?

Protected Health Information (PHI) includes:

- Patient name and address
- Phone number, DOB
- Social security number
- All medical information
- Lab and test results
- STD information
- Mental health history
- Alcohol and drug history
- Patient medical record number
- Surgery and medications
- Patient presence in the hospital
- Electronic Medical Record (EMR)

All information learned from seeing or treating patients is protected!

Progress Page

Back Next Exit

Business Information

Munson's business information is also confidential.

Business information includes any information pertaining to:

- Physicians
- Financial operations
- Quality assurance
- Risk management
- Research
- Utilization review
- And more

Progress Page

Back Next Exit

Why is Privacy So Important?

Strict privacy rules:

- Protect against identity theft
- Protect against fraud
- Enhance public trust in MHC

Note: Patient rights dictate that you may release information ONLY to the patient's preferred phone number or e-mail address.

We all may be patients one day!

Progress Page

Why is Privacy So Important? *(cont.)*

Patients have the right to "opt out" of the facility directory.

- This will keep a person's presence in the hospital confidential.
- You may give information to a personal representative of the opted-out patient if he/she has a privacy code.

Example of a privacy code slip used at MMC:

The Privacy Code will serve as your authorization for us to communicate information about you to family members and friends of your choice. Any individual seeking information will need to provide the Privacy Code to the person they are speaking with before information about you may be shared.

The facility is not responsible for the distribution of this Privacy Code and will assume that you and anyone you share this number with are taking reasonable measures to protect it.

YOUR PRIVACY CODE FOR THIS VISIT IS:

_____ Form #6486 (10/03)

Why is Privacy So Important? *(cont.)*

Not all patients want visitors or co-workers to visit.

- Let patients invite you first, or check with the family, or the nurse.
- Do not "drop-in" to visit without checking patient preferences first.
- Don't ask! Don't pry! Avoid saying, "Why are you here?" to anyone!

Back Next Exit

Disciplinary Consequences - HIPAA Privacy Breaches

Employees who breach privacy or security will face a written warning, up to and including termination.

If you violate privacy and work for Munson, you may face big consequences:

- You may get a written or final written warning.
- You may lose future access to PowerChart.
- You may lose your job.
- Munson may be fined.
- You may be fined.
- You may be sued.
- You may be jailed.
- You may lose your professional license in Michigan.
- You may be reported to the Office of Civil Rights.

Progress Page

Back Next Exit

Examples - HIPAA Privacy Breaches

- In California. employees in five hospitals were fined six fines totaling $675,000 for unauthorized access to sensitive information in patients' electronic medical records.
- In Arizona, three employees were fired for inappropriately accessing the electronic medical records of victims of a shooting spree.
- In Massachusetts, a hospital was fined $1 million after an employee took a chart home with her and left it on the subway train.

In other national cases, four employees faced criminal prosecutions for looking in medical records out of curiosity.

Progress Page

Back Next Exit

It Happens Here!

It Happens Here!

Each year, a number of employees are given warnings or terminated for inappropriately breaching patient information!

Progress Page

Back Next Exit

Report all Privacy Breaches

If you suspect or see a privacy breach:

- Tell your manager, AND
- E-mail or call the Privacy Officer listed in the employee directory, AND
- Complete a VOICE file to report the occurrence.

Do not be the person who tells the patient about the privacy breach.
The Privacy Officer will investigate and report the breach.

By law, the Privacy Officer must inform a patient with a Breach Notification letter.

Progress Page

Back Next Exit

HIPAA – Computer Security

Computer security is as important as patient privacy issues.

All protected health information must be encrypted and/or password protected on:

- Computers (at work and home)
- Thumb drives
- Cell phones
- Cameras
- Laptops
- iPads/tablets
- CDs

Maintain computer security while:

- Texting
- e-mailing
- Using the Internet

Munson Healthcare's Social Media policy prohibits posting identifiable patient pictures or medical information to social media (even if the name is not disclosed).

For help with computer security (encryption, disposal etc.), call the Help Desk (231-935-6053).

Progress Page

Back Next Exit

Audits – Computer Security

All electronic information is discoverable and subject to audit, per Munson policy.

- Your name and the date is electronically recorded every time you enter a medical record.
- Audits on chart access are done daily within PowerChart, STAR, and other applications.
- E-mails sent through the MHC network may also be audited.
- Fair Warnings Managed Services audits chart access on a daily basis to monitor for inappropriate access. Alerts for suspected non job-related access are forwarded to the manager and to the privacy office.

Progress Page

Back Next Exit

Best Practices – Computer Security

Lock or log off your computer every time you step away.

If you have your own computer - Lock your computer:

- Press the  and the 'L' key at the same time.

or

- Press these 3 keys at once: Ctrl + Alt + Delete and then select the '**Lock Computer**' option.

If you share a computer - Log Off:

- Press the  button and then choose 'Log off (user ID)' followed by the 'Log Off' button.

or

- Press these 3 keys at once: Ctrl + Alt + Delete and then select the '**Log Off…**option.

Please try locking your computer now.
Do not "Log off" because HealthStream will close!

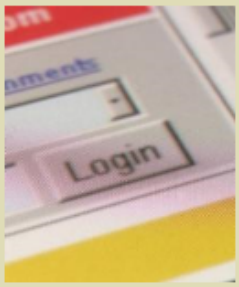
Progress Page

Back Next Exit

Best Practices – Computer Security *(cont.)*

Never allow someone to use your password or your personal login!

- Your login is your electronic signature.
- You are responsible for everything entered on your computer while you are logged in.
- Letting someone else use your computer while you are logged in attaches your name to everything that person does.
- Log off before you let someone use your computer.
- Do not share your passwords.
- Do not reuse passwords. Using the same password for both personal and work applications can make it easier to access lots of information through a single, compromised account.



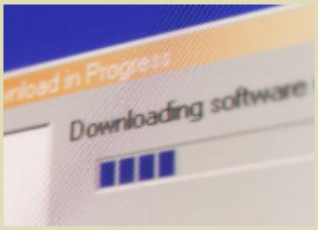
Progress Page

Back Next Exit

Best Practices – Computer Security *(cont.)*

Do not download software to your work computer.

- Call your facility's Help Desk for assistance with software.
- Software may contain viruses or introduce other security risks.



Progress Page

Back Next Exit

Best Practices – Computer Security *(cont.)*

Media disposal:

Contact your facilities Help Desk when you need to dispose of media containing Protected Health Information (PHI).

Examples of media include:

- CDs
- Thumb drives
- Computers
- Fax machines
- Copiers

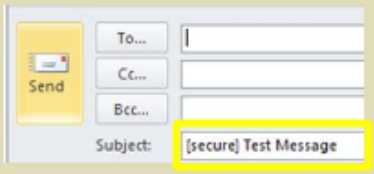
Progress Page

Back Next Exit

Security for Sending PHI by e-mail

Attention: Audits show multiple Munson e-mail HIPAA violations!
Encrypt and protect e-mails sent from your Munson e-mail accounts on your laptops, cell phones, and iPads.

To encrypt an e-mail:
Add '**[secure]**' to the subject line of your message.
Be sure to use the "square" brackets only.



Never send Protected Health Information (PHI) over the Internet to an e-mail address that does not end in "@mhc.net" without first adding the word '[secure]" to the subject line.

Progress Page

Back Next Exit

Fax Security

Faxes

Always use a **cover sheet** for every fax. This cover sheet should have the Confidentiality Statement printed on it.

- Verify that the fax number is correct.
- Report PHI fax violations in VOICE.

Access the fax cover sheet from Microsoft Word. Go to File>New>My templates>FAX Munson Healthcare.dotx or FAX Munson Medical Center.dotx

Click below to get a printable copy of the FAX cover sheet:

MHC MMC

Progress Page

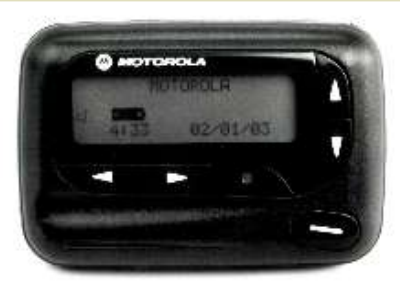
Back Next Exit

Pager Security

Pagers are not secure! To protect yourself from privacy breaches:

- Protect your pager - like you would protect your cell phone.
- Limit the content of a page - to what is absolutely necessary.
- Delete the message as soon as possible.

Delete any messages you no longer need.



Progress Page

Back Next Exit

Social Media and/or Photos

To protect yourself from privacy breaches:

- Do not post any patient information on Facebook or other web sites, even if you do not mention a patient by name.
- Do not take photos of patients, unless you have their written consent.
- You have the right to prevent visitors from using their personal cell phones to take photos of staff or other patients.

Progress Page

Back Next Exit

Best Practices – Disposal of PHI

Gray trash bins

Always shred or dispose of paper containing a patient's protected health information (PHI) into the gray trash bins.

Examples:

- Labels
- Lab reports
- Census sheets
- Hand written notes
- Printouts from charts
- Financial documents
- Patient registration documents

All papers put into the gray bins get shredded.

Progress Page

Back Next Exit

Verify Identity and Share Minimum Necessary Information Only

Always verify the identity of the person who is requesting patient information:

Do you know to whom you are talking?
To verify, ask the caller to:

- Put his/her request in writing, AND
- Put the request onto agency letterhead, AND
- Fax the request to you.

When disclosing patient information:

- Check with the patient for approval whenever you are uncertain or have a question, AND
- Disclose only **minimum necessary** information.

Progress Page

Back Next Exit

Law Enforcement and HIPAA

HIPAA allows certain disclosures to law enforcement

Please call Risk Management or the Privacy Officer for consultation regarding disclosures to law enforcement.

- Verify the legal identity of the officer.
- Provide only the discharge date and time, if appropriate.
- Do not disclose medical information to anyone other than to prison personnel or to jail healthcare workers.
- HIPAA allows staff to disclose patient name, demographic information, and physical descriptors in certain situations.

Progress Page

Back Next Exit

Good Documentation

Document your disclosures:

- Sometimes patient safety may be a more immediate need than privacy.
- When in doubt, note how your actions serve the patient's best interests.
- Call Risk Management or the Privacy Officer for consultation as needed.

Progress Page

Back Exit

Questions?

MHC offers many resources to guide you through any privacy and security questions or problems:

- Your manager
- HIPAA Security Officer
- Risk Management
- Administrative Supervisor
- Legal counsel
- Privacy Officers:
  - Munson Healthcare Cadillac Hospital, Acacia Holmes
  - Munson Healthcare Grayling Hospital, Loretta Wingard
  - Paul Oliver Memorial Hospital, Brenda Nye
  - Kalkaska Memorial Health Center: Judy Spoor
  - Otsego Memorial Hospital, Nancy Kussrow
  - Charlevoix Area Hospital, Chris Wilhelm
  - West Shore Medical Center, Sonja Ganger
  - Mackinac Straits Hospital, Koreen Troyer
  - Munson Medical Center and MHC Systems Privacy Coordinator, Rochelle Steimel

Progress Page