

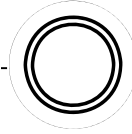
HIPAA Privacy and Security



Rochelle Steimel, HIPAA Privacy Official
Judy Smith, Staff Development
January 2012



Goals and Objectives



Course Goal:

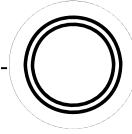
Can serve as annual HIPAA training for physician practice staff.

Course Objectives:

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

1. Comply with 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 practice's computer network.
4. State how to report privacy and security incidents.

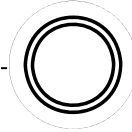
Patient Privacy



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.

Avoid Privacy Complaints



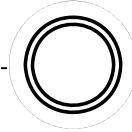
Share and access information only if there is a specific **job-related need to know**.

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**.



Keep Good Professional Boundaries



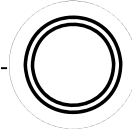
Do NOT access the electronic medical record of:

- 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...



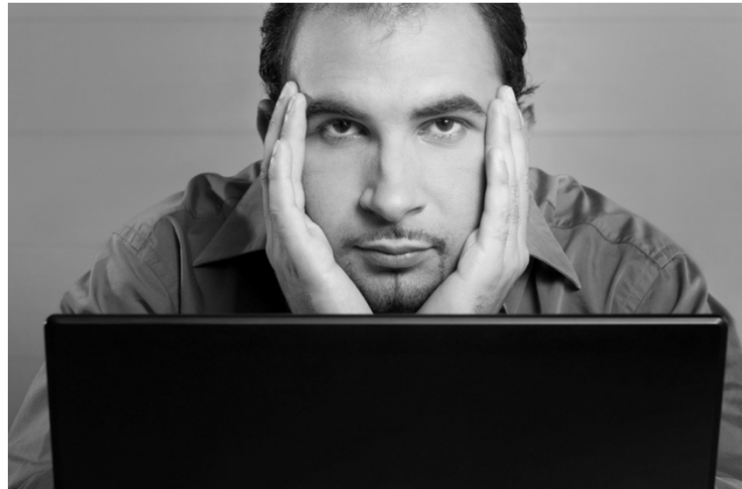
Unless there is a job-related need to know!

Job-Related Need to Know



Before accessing a medical record, ask yourself:

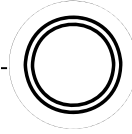
“Do I need this to do my job?”



Will your supervisor agree with you?
If no, then **STOP!**



Job-Related Need to Know



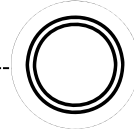
When do I have a job-related need to know?

Only 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)



What Patient Information is Protected?



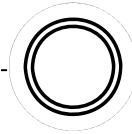
Protected Health Information (PHI) includes:

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



**All information learned from seeing
or treating patients is protected!**

Business Information



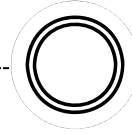
Practice's business information is also confidential.

Business information includes any information pertaining to:

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



Why is Privacy So Important?



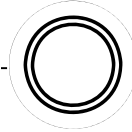
Strict privacy rules protect against identity theft and fraud related to:

- Diagnoses
- Social histories
- Personal information
- Social security numbers



We all may be patients one day!

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



Patients have the right to “opt out” or “restrict” callers.

- This will keep a person’s presence in the hospital confidential.
- If the patient is not “opted out,” ask callers if they have the patient’s privacy code before you give them information beyond a general status report.

Example of a privacy code slip:

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.

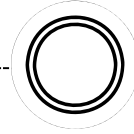
The facility is not responsible for the distribution of this Privacy Code and will assume that you and anyone you share this number with are taking reasonable measures to protect it.

YOUR PRIVACY CODE FOR THIS VISIT IS:

Form #6486 (10/03)

.....

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

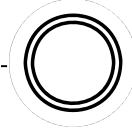


Not all patients want visitors or co-workers to visit.

- Let patients invite you first, or check with the family, or the nurse.
- Keep lists of patients scheduled for surgery confidential.
- Don't ask! Don't pry!



HIPAA Privacy Breaches



A **privacy breach** is a disclosure of any past, present or future medical information to people who do not have a job-related need to know.

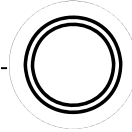
Privacy breaches:

- Harm patient trust.
- Are against federal HIPAA laws.
- Violate practice policy.



If you are sharing patient information, get a signed release from the patient, unless it is for treatment, payment, or operations.

Consequences of HIPAA Privacy Breaches

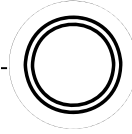


If you violate privacy, you may face big consequences:

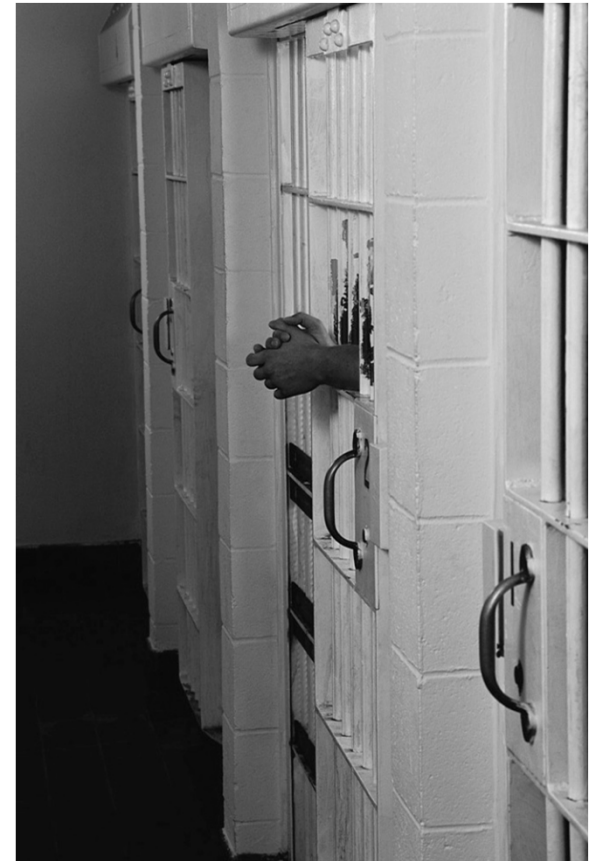
- You may get a written warning.
- You may be fined.
- Your practice may be fined.
- You may be sued.
- You may be jailed.
- You may lose your job.
- You may lose future access to PowerChart.
- You may lose your professional license in Michigan.
- You may be reported to the Office of Civil Rights.



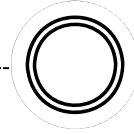
Examples: Civil/Criminal Fines and Penalties



- 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, 4 employees faced criminal prosecutions for looking in medical records out of curiosity.



It Happens Here!

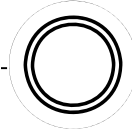


It Happens Here!

Several area health care employees have been fired for inappropriately accessing medical records of patients.



Report all Privacy Breaches



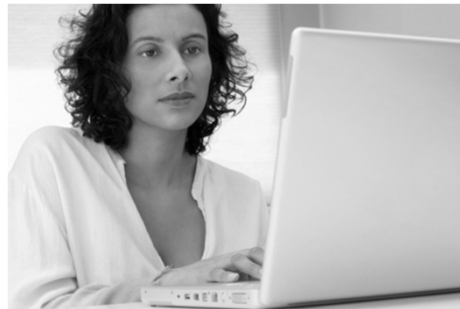
If you suspect or see a privacy breach:

- Tell your manager, or
 - Email or call Munson's Privacy Officer.
 - Fill out an occurrence report.

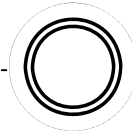
Do not be the person who tells the patient about the privacy breach.

By law, breaches must be disclosed to the patient by letter.

The Privacy Officer will investigate and compose the letter.



HIPAA – Computer Security



Computer security is as important as patient privacy issues.

Computer security must be maintained on:

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



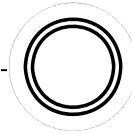
Maintain computer security while:

- Texting
- Emailing
- Using the Internet

Do not post information learned at work to any social networking site! (Facebook, Twitter, etc.)

If devices hold or send protected health information, call the Munson Help Desk at **(231) 935-5053** for assistance with encryption.

Audits – Computer Security

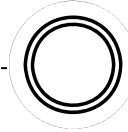


Your work computer may be audited, per Munson policy.

- 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.
- Emails sent from Munson equipment may also be audited.




Best Practices – Computer Security




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

If you have your own computer:

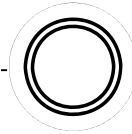
Lock your computer:

- 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:

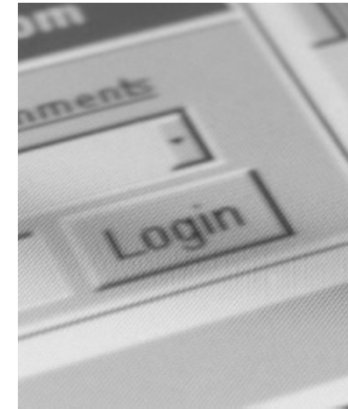
- Press the  button and then choose 'Log off (user ID)' followed by the 'Log Off' button.
- or
- Press these 3 keys at once: Ctrl + Alt + Delete and then select the '**Log Off**...option.

Best Practices – Computer Security

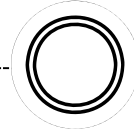


Never allow someone to use your password or your personal login!

- 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.

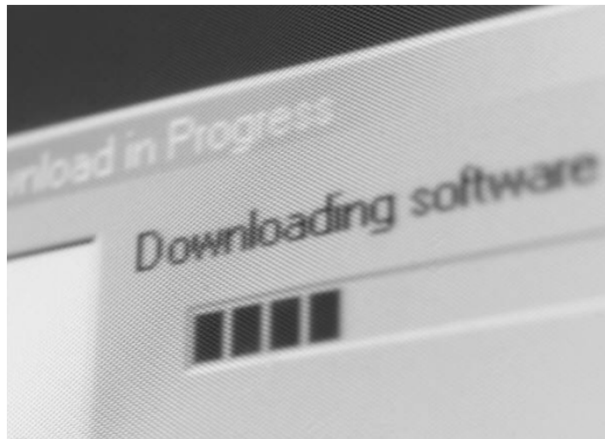


Best Practices – Computer Security *(cont.)*

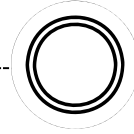


Do not download software to your work computer.

- Contact your practice manager or IT support for assistance with downloading software to your computer.
- Software may contain viruses.



Best Practices – Computer Security *(cont.)*



Media disposal:

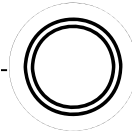
Contact the Munson Help Desk at (231) 935-6053 when you need to dispose of media containing Protected Health Information (PHI).

Examples of media include:

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



Best Practices – Computer Security *(cont.)*

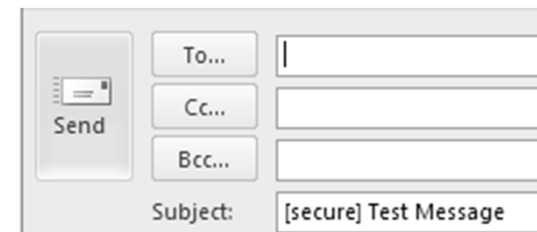


Encrypt and protect emails sent from your laptops, cell phone, and iPads.

Never transmit confidential information over the Internet (outside of your network) without first encrypting it. Encryption methods vary per device. Please call the Help Desk at (231) 935-6053 for specific advice.

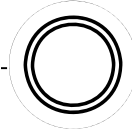
To encrypt an email sent from a Munson computer:

- Add '[secure]' to the subject line of your message. Be sure to use the “square” brackets only.
- The recipient will get this message: “You have received a SECURE message from (your email address) at Munson Healthcare. Click the link to view the secure web delivery.”
- In order to unlock the message, the recipient will have to create an account on the Secure Web Mail system.



Tip: See the “Secure Email Usage” link in the “In The Know” section on the MHC Intranet for more information.

Best Practices – Computer Security *(cont.)*

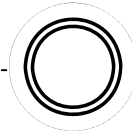


Faxes

Always use a cover sheet for every fax.
The cover sheet should included a
Confidentiality Statement.



Best Practices – Disposal of PHI

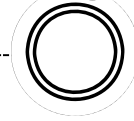


Gray Trash Bins

- Always shred or dispose of paper containing a patient's protected health information (PHI) into the gray trash bins.
- Examples of papers that may contain patient names or medical information:
 - 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.



Verify Identity and Share Minimum Necessary Information Only

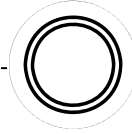


Always verify the identity of the person who is requesting patient information:

- Do you know to whom you are talking?
- When disclosing patient information:
 - Check with the patient for approval.
 - Disclose only **minimum necessary** information.



Law Enforcement and HIPAA

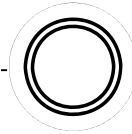


HIPAA allows certain disclosures to Law Enforcement.

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



Good Documentation



In complex cases, it may be necessary to document your disclosures:

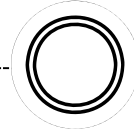
- To give an explanation, especially if it is not a simple black and white situation.
- When patient safety takes precedence over patient privacy.

Call Risk Management for assistance in documentation of complex cases.

- When in doubt about a disclosure and/or patient privacy issue, document your rationale.
- Be sure to note how actions were in the best interest of the patient.



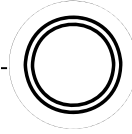
Confidentiality and Systems Usage Agreement



- Upon hire, employees sign the ‘Confidentiality and Systems Usage Agreement.’
- This agreement outlines the employee’s responsibilities for privacy and security.
- Employees are expected to know and follow all aspects of the agreement.



Questions?



The following resources can guide you through any privacy and security questions or problems:

- Your Manager
- Your Physician(s)
- Your Privacy Officer
- Munson's Privacy Officer
- Legal Counsel

