Annual Patient Confidentiality Agreement
Compliance Module DENT_Comp101

University of Michigan School of Dentistry

Content Area Expert:
Compliance Officer (ddd-compliance@umich.edu)

Protecting Patient Information

- Our patients expect us to safeguard their information as if it were our own.
  - Giving a patient’s health information to the wrong person (an employer, relative, etc.) could cause the patient serious social or professional harm.
- We are legally obligated to protect information about a patient’s health by:
  - State laws
  - Federal HIPAA Privacy and Security Rules federal regulations
- The privacy requirements are so important that UMSD requires you to review them upon hire and annually, thereafter.

Each of us has a responsibility to protect patient privacy!
What is Protected Health Information (PHI)?

- Sensitive data sent or stored in any form that may be used to identify the patient.
- Information we have to protect.
- Includes:
  - A patient’s past, present or future treatment.
  - A patient’s payment of services.
  - A patient’s medical condition.
  - The fact that a patient has been seen in a particular department is PHI.
  - Even the fact that someone is a patient at UMID is PHI.

For Example

PHI
- Names
- Addresses
- Dates
- Medical Record or Health Plan Numbers
- Biometric Information
- Photos
- Any Other Unique Identifying Characteristics

What is the "Minimum Necessary" Standard?

Amount of PHI used, shared, accessed or requested:
- Must be limited to the minimum necessary EXCEPT when PHI is used for treatment purposes.

This means:
- Only access information you need to do your job.
- Only release the information you are allowed to release as part of your job.

For Example
- Social security numbers should not be printed on reports unless an exemption has been obtained from the Compliance Office.
- Once obtained display only the last 4 digits and no more.
It's OK to...

- Give PHI to a coworker or another UMSP unit.
  - As long as they say they need it to do their job.
- Let a family member make an appointment for a patient without an authorization.
  - They can give you information, just don't share any information about the patient in return.
- Talk to a patient's family members involved in the patient's care, about things they need to know for that care.
  - As long as the patient's been given the opportunity to agree or object. For more information see the UMSP Policy APG-01-020 - Disclosures to Family and Friends of Patients.
- Talk to a patient about their condition with family members in the room.
  - As long as you have permission from the patient. For more information see the UMSP Policy APG-01-020 - Disclosures to Family and Friends of Patients.

Identity Theft

- We must protect all sensitive information in our care, not just information about patients’ health.
- Take extra care when dealing with information that could be used to steal a patient or staff member’s identity.
- If you believe this type of information has been lost, stolen, or inappropriately accessed contact the Compliance Office immediately.
- Fast reporting is very important so that appropriate measures can be taken!

For more information on Identity Theft and what you can do if it happens to you or someone you know visit http://www.ftc.gov/bcp/edu/microsites/idtheft/.
Things You Can Do

Protect PHI

*Tab Text*

We all have to work together to protect PHI. The topics on the left of the slide are presented in the following slides.
When Speaking

• Keep your voice down.
• Do not discuss patient information in public places.
• If you have to discuss a patient where others might hear, take precautions and avoid discussing extremely sensitive information.
• When talking to patients in semi-private rooms, use good judgment.
While at Work

- Make sure PHI is not visible to other patients and visitors.
- Keep books and charts where other patients and visitors cannot casually read them.
- Throw paper trash containing PHI in the locked blue bins.
- Sometimes patient safety requires the use of patient identifiers in public areas. To determine if it's appropriate, ask the Compliance Office.
- Do not hand patients their records/charts to carry from one area to another.
When Using Your Computer

- Before you walk away from your computer, log out. Remember! You are responsible for any use or misuse while you are logged in.
- If you put PHI or other sensitive data on a portable device, you are responsible for making sure it’s secure. If you are unsure about how to encrypt or secure a portable device, contact Dental Informatics for assistance.
- Turn computer monitors so they aren’t visible from public areas.
- NEVER share your password with anyone else, or log them into your account, even "just for a moment." You will be held responsible for all activity conducted under your log in credentials.
- Change your passwords at regular intervals. Pick a password that coworkers or friends could not guess easily and would not appear in a dictionary in any language.
Releasing Protected Health Information

Before you release PHI you need to:
1. Know whether the release requires an authorization.
2. Verify who you’re talking to.
3. Follow your unit's procedures.

Remember! If you aren’t sure, send the requesting person to Central Records for assistance.

Click on each area for more information.
Releasing PHI: Authorization

Most releases do not require authorization since they are for:
- Treatment (continuity of care, referrals, consultations), or
- Payment (billing health insurance companies), or
- Directly to the patient
Other types of releases can be made without authorization, but the rules for them are often complicated.

Remember! Either ask your supervisor or refer people to Central Records for releases you are not sure about.
Releasing PHI: Verification

5 seconds

- The basic principle is to use your judgment -- if you're suspicious of a requester, either do not release information or insist on sending it to the address you have on file for the patient.

Remember! You can always refer people to Central Records.

If you have any questions about access to, use or release of Protected Health Information, ask your supervisor or contact the Compliance Officer at dds-compliance.umich.edu
Patient Confidentiality Agreement Signature Page

Please read the following statements and confirm your agreement with them by signing below. Give only this signature page to your supervisor.

I agree to uphold UMSD Policy APG-01-007.
I agree to maintain patient confidentiality.
I agree to report incidents of noncompliance and/or security breach.
I understand that noncompliance with UMSD Policy APG-01-007 may result in dismissal, termination of contract and/or loss of access to UMSD property or resources.

Name (print) ___________________________________________ Signature: ___________________________ Date __________________

________________________________________________________________________