

HIPAA Training Rules and Regulations

**University of Maryland
Department of Hearing and Speech Sciences**

**Portions of This Training Course Were Adapted From The
University of Michigan Health System
Online HIPAA Training Module**

Learning Outcomes

- **To understand basic HIPAA Rules and Regulations**
- **To understand how these rules and regulations are interpreted in a variety of health care settings**
- **To be able to apply these rules and regulations in everyday clinical situations**

Please Note

It is the policy of the University of Maryland to comply with HIPAA to the extent that it is applicable to the University.

Since the University's activities include both HIPAA covered and non-covered functions, the University has determined that it is a hybrid entity for HIPAA coverage purposes.

<http://hipaa.umd.edu/org.html>

The University has designated its *Health Care Component* as meeting the requirements for HIPAA compliance. The *Health Care Component* includes the University Health Center and other University units that may have access to health care information because of their activities in support of the University Health Center.

<http://www.hipaa.umd.edu/CoveredUnits.pdf>

“Other units that perform health care functions may voluntarily choose to comply with or participate in some or all HIPAA requirements, policies or procedures. Such voluntary compliance or participation shall not affect a unit’s status as a non-covered component.”

<http://hipaa.umd.edu/UniversityCompliancePolicy.pdf>

The Hearing and Speech Clinic voluntarily chooses to comply with HIPAA privacy practices.

You are being asked to participate in this HIPAA training, because the Clinic feels it is important for you to:

- ***Be knowledgeable about client rights as defined by HIPAA***
- ***Understand your responsibilities as a health care provider***
- ***Ensure that client information is handled confidentially at all times in this clinic***

What does HIPAA stand for?

HIPAA stands for...

Health **I**nsurance **P**ortability and
Accountability **A**ct

What *is* HIPAA?

- HIPAA is *a law related to the delivery of health care*. It offers protections that *improve portability and continuity of health insurance coverage*. *For example, it:*
 - Limits exclusions for preexisting medical conditions
 - Prohibits discrimination in health insurance enrollment based on health status-related factors
 - Provides rights that allow individuals to enroll for health coverage when they lose other health coverage, get married or add a new dependent
 - Guarantees availability of health insurance coverage for small employers

What *is* HIPAA?

- HIPAA also establishes *standards for the privacy of Protected Health Information [PHI]*.
- Congress called on the Department of Health and Human Services to issue *patient privacy protections* as part of HIPAA.
- These protections, **known as the Privacy Rule**, were signed into law in 2001 by President George W. Bush and took effect in 2003.

What exactly does the Privacy Rule do?

- The **Privacy Rule** portion of HIPAA gives citizens new rights to privacy by ***requiring all organizations that handle health care information – whether written, oral or computer-based – to reasonably safeguard that information.***
- The rule ***provides patients with access*** to their medical records and more ***control over how their personal health information is used and disclosed.***
- It establishes ***penalties for organizations that fail to comply*** with the law.

The five basic principles of the Privacy Rule are:

1. **Consumer Control**: Patients have rights to control the release of their medical information.
2. **Boundaries**: With few exceptions, a patient's health information should be used for health purposes only. Other uses must be kept to the minimum necessary for a specific purpose.
3. **Accountability**: There are specific federal penalties for violating the privacy regulations, ranging from \$100 fine per violation for disclosures made in error, up to \$250,000 and 10 years in prison for malicious use of records.
4. **Public Responsibility**: Standards are provided regarding how information should be released to protect public health, investigate fraud and abuse, and for quality assessment purposes.
5. **Security**: Health Care organizations must establish clear procedures to protect patients' privacy.

More about Consumer Control, Boundaries, and Security ...

Consumer Control

- **Access to Medical Records**
 - Patients should be able to see *and obtain copies of their medical records*.
 - Patients should be able to *request corrections if they see errors*.
- **Limits on Use of Personal Medical Information**
 - *The rule does not restrict the ability of doctors, nurses and other providers to share information needed to treat their patients.*
 - *Patients must give permission* for their health information to be used or shared for certain purposes, such as for *marketing*.
 - Patients can get a list of disclosures made of their health information.
- **Confidential Communications**
 - *Reasonable steps must be taken to ensure that communications with patients are confidential.*
- **Complaints**
 - If a patient feels that his or her rights have been denied or that health information isn't being protected, *a complaint can be filed with*
 - the *provider or health insurer*
 - the *U.S. Government*

Boundaries

- **Your information can be used and shared...**
 - for *treatment and care* coordination
 - *to pay* doctors and hospitals for health care services
 - with *family, relatives, friends or others you identify* who are involved with your health care or your health care bills
 - *to protect the public's health*, such as by reporting outbreaks of contagious diseases
 - *to make required reports to the police* [e.g., reporting gunshot wounds]
- **Without your authorization, your provider generally cannot...**
 - *give your information to an employer*
 - use or share information *for marketing or advertising* purposes
 - *share private notes about mental health counseling* sessions

Security

- **Providers and health insurers must ...**
 - ***Establish written policies and procedures*** to protect confidentiality of protected health information
 - ***Provide a Notice of Privacy Practices [NPP]*** that describes how they use and share protected health information, the patient's rights and responsibilities regarding this information, and who to contact for more information
 - ***Ask patients to acknowledge*** that they have received this notice and consent to the release of protected information as indicated in the NPP
....In most cases this must be in writing
 - ***Provide training to employees regarding these privacy practices***
 - ***Take appropriate and reasonable steps to keep a patient's health information secure*** – i.e., secure patient records so that they are not readily available to those who do not need them
 - ***Document other events*** such as breaches of policies and amendments to patient records

Who must follow this law?

[Who are the *Covered Entities*?]

- A Covered Entity is anyone who collects, stores, or transmits individually identifiable health information
 - Most doctors, nurses, pharmacies, hospitals, clinics, nursing homes, and many other ***health care providers including Speech-Language Pathologists, Audiologists, and hearing instrument dispensing offices and practices***
 - ***Health insurance companies***, HMOs, most employer group health plans
 - ***Certain government programs*** that pay for health care, ***such as Medicare and Medicaid***

Within the speech, language, and hearing professions, covered entities include:

- Private practice
- Schools
- Nursing homes
- Hospitals
- Other institutional settings

Professionals working for these covered entities or contracting with them [e.g., in a nursing home] are subject to HIPAA rules and regulations

Who enforces the law?

The ***U.S. Department of Health and Human Services, Office for Civil Rights*** is responsible for the implementation and enforcement of the HIPPA Privacy Rule.

For more information about the Privacy Rule, visit....

<http://www.hhs.gov/ocr/privacy/hipaa/understanding/index.html>

What is Protected Health Information [PHI]?

Protected Health Information is individually identifiable health information created, received, transmitted and/or maintained by a covered entity.

This includes information relating directly or indirectly to:

- The person's past, present or future physical or mental health
- The provision of care to the person
- The person's health care bills and payments
- The person's demographic information

PHI includes

- ***Information*** that doctors, nurses, and other health care providers put ***in a patient's medical records***
- ***Conversations*** the health care provider has ***about a patient's care or treatment*** with others, including other health care providers
- ***Information*** about the patient ***in his or her health insurer's computer system***
- ***Billing information*** about the patient at his or her clinic

PHI may be sent, communicated or stored in any form.....

- Paper
- Electronic [including faxes, emails, electronic files and databases]
- Oral [discussions; conversations]

PHI includes personal information such as....

- Names
- Addresses including - Zip Codes
- Dates [e.g., Birth Dates]
- Telephone & Fax Numbers
- E-mail Addresses
- Social Security Numbers
- Medical Records, including the reason for seeking health care, diagnosis, x-rays, lab work, etc.
- Health Plan Numbers
- Billing Records
- License Numbers
- Vehicle Identification Numbers
- Account Numbers
- Biometric Identifiers
- Full Face Photos
- Any Other Unique Identifying Number, Characteristic or Code

**What exactly does HIPAA say
about consent to share PHI?**

In general, covered entities may use PHI for ***treatment, payment and health care operations [TPO]*** without any special permission from patients.

A covered entity may voluntarily choose, but is not required, to obtain the individual's consent for it to use and disclose information about him or her for treatment, payment, and health care operations.

A covered entity that chooses to have a consent process has complete discretion under the Privacy Rule to design a process that works best for its business and consumers.

<http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/usanddisclosuresfortpo.html>

Treatment, Payment and Health Care Operations [TPO] are defined as:

Treatment: includes various activities related to patient care

Payment: includes various activities related to paying for or getting paid for health care services

Health Care Operations: generally refers to day-to-day activities of a covered entity, such as planning, management, training, improving quality, providing services, and education

Examples of when the individual's authorization is not required...

- A primary care provider may send a copy of an individual's medical record to a specialist who needs the information to treat the individual.
- A physician may send an individual's health plan coverage information to a laboratory who needs the information to bill for services it provided to the physician with respect to the individual.
- A hospital emergency department may give a patient's payment information to an ambulance service provider that transported the patient to the hospital in order for the ambulance provider to bill for its treatment

<http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/usanddisclosuresfortpo.html>

Does my health care provider need my written permission to share or discuss my health information with family and friends involved in my care or payment for my care?

HIPAA does not require that you give your health care provider written permission. However, your provider may prefer or require that you give written permission.

Always let your provider know if you object!

There ARE times when written permission IS required:

- To use or share PHI for certain marketing and fund-raising activities.

For example: An audiologist cannot give a hearing aid company a list of patients with hearing loss without an authorization.

- To use or share PHI for research

For example: A researcher cannot enroll a patient in a study without an authorization that includes what the PHI will be used for, who can use it, and for how long.

The “Minimum Necessary” Rule

- Generally, the amount of PHI used, shared, accessed or requested ***must be limited to only what is needed.***

For example: When a company bills for a blood test, it does not need the patient’s complete medical record.

- Employees should have only such PHI as their job responsibilities require.

For example: Someone who delivers food trays to patients may need PHI about the patient’s diet but does not need to know why the patient is in the hospital.

- ***In some cases, the “minimum necessary” rule does not apply, such as when PHI is shared among health care providers for treatment.***

Incidental Disclosures

In the course of routine communication, PHI may sometimes be inadvertently disclosed to someone who is not authorized to receive that information. HIPAA regulations call this an **incidental disclosure**.

For example, visitors may hear a patient's name as it is called out in a waiting room or overhear a clinical discussion as they are walking down a hallway on the unit.

Incidental disclosures are allowed if reasonable steps are taken to limit them!

Incidental Disclosures

Reasonable safeguards to secure and protect PHI may include:

- *Speaking in soft tones when discussing PHI*
- *Not discussing PHI in public hallways or in elevators*
- *Using [but not sharing] computer passwords*
- *Locking cabinets that store PHI*

NOTE: Research is **not** considered TPO. For information about HIPAA as it relates to research at the University of Maryland, see:

<http://www.umresearch.umd.edu/IRB/hipaa.html>

In addition to sharing PHI for TPO.....

“The Privacy Rule permits use and disclosure of protected health information, ***without an individual’s authorization or permission, for 12 national priority purposes.*** These disclosures are permitted, although not required, by the Rule in recognition of the important uses made of Health Information outside of the health care context.”

These include:

- For public health purposes, such as to report births and deaths
- To report abuse or neglect
- For law enforcement
- For organ donation organizations
- To share PHI with medical examiners and funeral directors
- To avoid threats to health and safety
- For certain research activities if there is documentation that a waiver of participants’ authorization to use/ disclosure their protected health information for research purposes has been approved by the IRB

<http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/index.html>

What about record keeping?

Record Keeping

Covered entities ***must keep a written record, or an "accounting," of certain disclosures.*** This accounting must be kept for 6 years from the date of the disclosure.

Disclosures that **require** a written record include those:

- For public health activities and reporting
- About victims of abuse, neglect or domestic violence
- In response to a court order
- To a medical examiner, funeral director or for cadaveric organ donation.

If requested, these written records must be provided to the patient.

Record Keeping

Covered entities ***do not need to document*** disclosures made:

- To carry out treatment, payment or health care operations [TPO]
- Pursuant to the patient's authorization
- To the individual or the individual's personal representative
- To persons [e.g. family] involved in the individual's care
- For national security or intelligence purposes
- To correctional institutions or law enforcement officials about an inmate or other individual in legal custody
- As de-identified information
- Incidentally

What about other laws that protect privacy?

- We already follow many other laws, rules and guidelines to protect privacy
- Generally, the Privacy Rule supersedes contrary state law, but there are times when State law controls.
- In cases where state law provides more protection, state law should be followed. For general information about HIPAA vs. state law, check the following sites:

<http://www.apa.org/monitor/jan03/hipaa.html>

http://privacy.med.miami.edu/glossary/xd_state_preemption.htm

Signing Confidentiality Agreements

- Non-employed vendors providing a service where they need to have access to PHI might be required to sign a confidentiality agreement [e.g., a business associate agreement] promising to keep PHI confidential.

For example: a company developing database software must see actual PHI, so they would need a written agreement.

- Employees, volunteers, trainees, and other individuals whose work is controlled may not be required to sign such a confidentiality agreement. This varies by employer.

Penalties for Violating the Privacy Rule

Civil penalties:

- range from \$100 to \$50,000 or more per violation, depending on factors such as whether the covered entity knew or should have known of the failure to comply or whether the covered entity's failure to comply was due to willful neglect.
- Penalties may not exceed a calendar year cap (\$1,500,000) for multiple violations of the same requirement.

Criminal penalties for those who deliberately misuse protected health information are:

- For knowing misuse of PHI – up to 1 year imprisonment, or \$50,000 fine, or both
- For obtaining PHI under false pretenses – up to 5 years imprisonment, or \$100,000 fine, or both
- For using PHI for commercial advantage, personal gain, or malicious harm – up to 10 years imprisonment, or \$250,000 fine, or both.

Need more information?

For more information about the Privacy Rule, please visit these websites:

www.hhs.gov/ocr/hipaa

<http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/index.html>

Frequently Asked Questions

- Q: Is PHI the same as the medical record?
- A: No. HIPAA protects more than the official medical record. A great deal of other information is also considered PHI, such as billing and demographic data. Even the information that a person is a patient here is Protected Health Information.

- Q: What if I'm accidentally overheard discussing a patient's PHI record?

- A: It is not a violation as long as you were taking reasonable precautions and were discussing the protected health information for a legitimate purpose. The HIPAA privacy rule is not meant to prevent care providers from communicating with each other and their patients during the course of treatment. These "incidental disclosures" are allowed under HIPAA.

- Q: If I overhear patient care information in the elevator or in the hallway, how should I handle it?

- A: If it seems appropriate, remind the speakers of the policy in private. If the conversation clearly violates policies or regulations, you might need to report it to the appropriate individual at your place of work.

- Q: I work in the hospital and don't need to access PHI for my job, but every now and then a patient's family member asks me about a patient. What should I do?

- A: Explain that you do not have access to that information, and refer the individual to the patient's health care provider.

- Q: I know that patients have a right to their PHI. What about parents and guardians of incompetent patients?
- A: If someone other than the patient has the legal right to make health care decisions for the patient, that person is the patient's personal representative and has the right to access the patient's PHI.

However, if you have good reason to believe that informing the personal representative could result in harm to the patient or others, then you do not have to disclose the PHI.

- Q: What should I do if a government agency or law enforcement person requests information about a patient?

- A: If working with law enforcement is not part of your responsibility, contact your supervisor. If it is your responsibility, provide only the minimum amount necessary to support the investigation after verification of the authority of the individual or organization making the request.

Remember! Always consult your supervisor if you're not sure what to do.

- Q: When the law requires me to make a disclosure, such as reporting HIV infection, do I need to tell the patient that I disclosed the information?

- A: You need to tell the patient only if they ask for an accounting of disclosures, and the disclosure was made without an authorization.

If there is good reason to believe that informing the patient could result in harm to that individual, then you may not be required to tell him or her. In some cases, government agencies can also require that the patient not be informed.

- Q: Do I need to record the fact that I've made these disclosures?

- A: For the most part, yes. You need to document most disclosures made without authorizations except disclosures made for TPO purposes. Your employer should have procedures for documenting disclosures and for determining which disclosures do not require documentation.

- Q: As part of my job, I have access to a patient's PHI. How do I know which family and friends can be told this information?

- A: Always ask the patient who can receive this information and document the patient's response in the medical record.

- Q: When I am speaking to a patient, and friends or family members are in the treatment room, do I assume the patient has given me permission to speak of the PHI in front of these persons or do I need to ask them to leave?

- A: It is proper to speak, unless the patient objects. If you are uncertain, you can ask the patient if it okay to discuss their PHI in front of the person.

- Q: If the patient is not conscious, to whom can we disclose the PHI?

- A: You will have to decide this on a case-by-case basis. If you know the patient's preferences, as in "you can tell my spouse, but not my sister," then document the request and follow it. Otherwise, use your professional judgment. Always use the Minimum Necessary standard: disclose only information that is directly relevant to the person's involvement with the patient's health care.

Once a patient has regained consciousness, he or she will determine when and how we can share protected information.

- Q: Can someone else still pick up a patient's prescriptions, x-rays, or medical supplies?

- A: Yes, if in the care provider's professional judgment it is okay to give the prescription, x-rays or medical supplies to that individual.

- Q: If a patient asks for his or her PHI, do I need any special identification from the patient?

- A: If the patient is asking for his or her own information, you will need to verify his or her identity.

- Q: What if someone from a government agency comes up and asks me for information?

- A: First determine if this is part of your job responsibility to provide such information and verify who the person is asking for such information. Then contact your supervisor.

- Q: What if I get approached by an individual who just says he's a friend of a patient?

- A: Check to see if this individual has been approved by the patient for disclosure of PHI. If so, ask for one or more pieces of identification, including a picture ID.

- Q: What if I get a phone call looking for information, and the caller says it's the patient? What should I do?

- A: If the request is made by phone, and the requester identifies him- or herself as the patient, you can ask him or her to provide personal information for verification, such as his or her birth date, or Social Security number.

- Q: What about requests to leave information on voice mail or an answering machine?

- A: If you are asked to phone or leave confidential information via voice mail, for example, you should verify with the patient or other approved individual that it is okay to leave messages this way. Make sure you confirm the number. Some employers may have more restrictive policies, so check with your supervisor and/or department head.

- Q: How much information is it OK to leave?
- A: Always leave the minimum possible amount of information. And remember to make sure ahead of time that it's okay to leave a message on voicemail *OR* with any individuals [e.g., caretaker or daughter] who are likely to answer the phone.

- Q: What if I'm not supposed to leave a message?

- A: If you are asked not to leave voice messages, do not do so. This is especially important with patients who may not want to share PHI with family members, roommates, or co-workers.

- Q: What if a patient requests that I communicate with him or her via e-mail?

- A: If your employer has specific policies regarding e-mail requests, follow them. Otherwise, here are some things you can do...

1. Inform the patient to not use email for time sensitive matters, as you may be out of the office or busy taking care of other patients.
2. Make sure that patients understand that e-mail is not secure.
3. Verify the patient's identity. Ask patients if they have an e-mail address when you see them face-to-face. You may want to have them fill out a form authorizing e-mail contact.
4. Do not initiate e-mail with patients without first getting their permission, and only use the e-mail address they provided, unless they notify you of a change.

-cont'd. on next slide...

5. If you receive any request via e-mail, don't assume the sender is the person he or she claims to be, especially if the request is unexpected. If you have not previously verified an e-mail address with the patient, contact either the patient to verify the sender's identity and e-mail address, or contact the person making the request by another method for verification of the e-mail address. If in doubt, talk to your supervisor. In general, be careful about sending PHI in response to e-mails because of the difficulty in identifying senders accurately.
6. Minimize the amount of information disclosed in an e-mail.

- Q: What if patients disclose their PHI in an e-mail?

- A: If patients disclose their own PHI in an e-mail to you, you can discuss it. However, you should try to avoid disclosing ***additional*** PHI in return.

- Q: What do I do if I receive a request for PHI by fax?

- A: Most often, faxed requests for PHI will come from other health care providers or payers, like billing agencies or insurance companies, although patients may occasionally ask to have information faxed to them.

If a patient, health provider, or payer requests that you fax PHI, get a specific fax number from them and double-check the number before sending.

- Q: Is there any way I can make the process more secure?

- A: It's a good idea to program commonly used fax numbers to diminish potential dialing errors. If possible, ask the person to whom you've sent a fax to confirm it was received.

- Q: What if someone from a government agency sends me a fax asking me for information?

- A: Ask for the request to be on official agency letterhead, and call back the indicated number to verify the request is legitimate.

- Q: What if I find a fax went to a wrong number?

- A: In the event you find that a fax went to a wrong number, try to retrieve the communications containing the PHI that were faxed to the wrong number, or ensure that they have been destroyed in a secure fashion.

- Q: What if I receive a request for PHI on my pager?

- A: When communicating via alpha pagers, you should send only the minimum amount of information necessary, and delete received messages once you no longer need them.

- Q: I have temporary staff people who will only be here a short time. They need computer access to do their work. Can I give them my password or log them in as me?
- A: No. If you allow someone to use your access, you will be held responsible for what they do. You are better off giving them their own accounts while they are working with you.

- Q: What are some things I can do to protect PHI on my computer or PDA?

- A:
- install a hard-to-break password, using a variety of letters and numbers
- Engrave the PDA or computer with a serial number to help deter theft.
- Make sure your computer is running up-to-date virus software
- Consider using a screen saver that locks your computer when you're away from your desk

- Q: What else can I do for security?

- A: Don't allow others, such as family members, to use your equipment. They might accidentally access confidential information.

- Q: I'm going to dispose of my laptop. Are there special precautions I should take?

- A: Use a secure erase program to remove PHI from all personally owned PDAs, laptops, and computers before selling or otherwise disposing of them.

- Q: What's the safest way to dispose of PHI in the office?

- A: Paper records containing PHI should be shredded or disposed of in designated confidential recycling receptacles and not in the regular trash.

Ask a supervisor or your privacy officer for assistance with secure disposal of non-paper records containing PHI, like disks, radiographs, and other types of storage media. Never put them in the regular trash.

In general, follow your employer's secure disposal procedures for using secure disposal bins or shredding documents.

- Q: What will happen if the PHI regulations have been violated?
- A: You and/or your employer may face civil or criminal penalties and be substantially fined. Further, employees who knowingly misuse protected health information may be subject to prosecution, fines and/or imprisonment up to ten years, in addition to any disciplinary actions that your employer might take.

*The following questions and answers are
specific to the University of Maryland
Hearing and Speech Clinic*

- Q: I sometimes run into my client at parties and other social events. Is it okay to talk about therapy with her in these situations?

- A: You shouldn't just assume that her participation in therapy is "common knowledge," *even if* her communication difficulties are apparent. Keep the conversation social in nature and follow her lead. If she brings up therapy, you can assume that others know, and that she is comfortable discussing it in public. The same goes if you have friends in common. Never discuss your client's therapy, even if mutual friends know that she sees you.

- Q: The clinic has a rule that reports must not be photocopied from a patient's file. But what if the previous clinician sends a report to me via email? Would that violate the "photocopy" rule?
- A: Electronic transmission of reports via email is permissible, if and only if the report has been "de-identified." That is, all information that can be used to identify this individual must be removed from the report before it is sent. In fact, the previous clinician should remove all PHI from old reports that are stored on his or her personal computer and/or data storage devices.

- Q: The university has a shared drive where students and faculty can save information that might be of interest to everyone. Is it okay to store my clients' reports on this drive?

- A: No. Because so many individuals have access to this drive, your clients' confidentiality would be severely compromised. In addition, the files on this drive are not deleted on a regular basis, and information about a client can potentially be accessible for months or even years!

- Q: Is there a way to easily delete all personal information from a Word document?
- A: Yes. First, delete all identifying information from the “header” [e.g., name, address, date of birth, etc.]. Then, use the “search and replace” function of Word to search for the individual’s name and replace it with initials or with “John” or “Jane Doe.” If there is any other information that could be used to identify the individual [e.g., titles like, “President of State University”], you should delete that too!

- Q: I'm a research assistant for a professor in our department. One of my therapy clients would be very appropriate for our current study. Is it okay to give my client's contact information [i.e., name and email address] to the professor, so that she can recruit my client for her study?

- A: It depends.
- If you are a licensed therapist and this is a private client, then the answer is NO. You should tell your client about the research study, and let him or her contact the professor if interested in being a participant.

Continued on next slide

Continued from previous slide....

- If you are a graduate clinician or licensed SLP, and you are seeing the client through the university clinic, the answer depends on how your consent-for-services form is worded.....
- If the form states that client records can be shared with professors in the department, and it is clear that these professors might contact the client regarding interest in a research study, then you can give the researcher this lead.
- However, if the form does not clearly state that professors might contact clients for research purposes, you should tell your client about the research study, and let him or her contact the professor if interested in being a participant.

- Q: A current client referred her friend to our audiology clinic. When the friend came for his evaluation, he asked how his hearing compares with that of his friend [he was thinking of getting similar hearing aids]. Can I tell him?

- A: No. While it is possible that your client wouldn't mind sharing that information with her friend, she must explicitly be given the option to consent. Furthermore, this option is typically given when a friend or relative is directly involved in patient care or payment.

- Q: What is the best way to dispose of my working drafts of Therapy Plans, Progress Reports, and Diagnostic Reports?

- A: The best way to dispose of these and similar types of paperwork [e.g., session logs and notes with PHI] is to shred them.
- **NEVER** just put them in the trash – intact!

- Q: Occasionally, I've found abandoned Daily Therapy Logs on the work table in the student room or in the garbage. Most of these logs have the client's full name printed on the top....and some have performance summaries and critiques! Does this violate the client's privacy?

- A: Definitely! When logs are no longer needed, they should be shredded!
- An alternative would be to print ONLY the client's first name and last initial....or just his/her initials.

- Q: I communicate with some of my clients and/or their parents via email. Should I print these emails out and file them in the client's folder?

- A: It's always a good idea to include these correspondences in the client's file. Questions DO sometimes arise later in the semester or in subsequent semesters, and it is important to have this documentation.
- In addition to filing the email, you can also write a contact note in the front of the file, indicating that you communicated with the client, parent, etc. via email and that the email has been filed.

- Q: What about phone calls? Should I document these in the client's file?
- Yes. Document phone calls with a contact note that briefly summarizes the conversation. Always include the name of the individual you spoke with and his or her relationship to the client.

- Q: I've been in the observation room during a diagnostic, and we have had to put the speaker on "field" so that all members of the team can hear. But, other individuals are typically in the observation room watching therapy sessions. Is this a violation of HIPAA?
- This would probably be considered "incidental disclosure," which is permissible under HIPAA regulations, provided reasonable safeguards are taken. For example, keep the volume level to a minimum and only use "field" when it is absolutely necessary.
- During the conference that follows the diagnostic, it is best to use headphones, because these discussions can be very private and sensitive.

For specific questions about the University's Privacy Policy, contact:

Privacy Officer

Warren Kelley

Assistant Vice President; Student Affairs

2108 Mitchell Building

Telephone: (301) 314-8436

Email: HIPAA-Privacy@umd.edu