

Meeting the Challenges of HIPAA in Providing Clinical Services and Conducting Clinical Research

Carol Ann Raymond, *The University of Georgia*

Barbara S.W. Solomon, *Purdue University*

Issue I: SAFEGUARDS

OCR 164.530, Administrative Requirements (c)(1) stipulate that facilities must *reasonably safeguard Protected Health Information (PHI) from any intentional or unintentional use or disclosure that is in violation of patient privacy policies and applicable federal and state law*. This statute will require Administrative procedures, physical measures, and technical means to protect client's health information.

Administrative Safeguards

These will include the following:

For oral communications regarding PHI:

1. Do not disclose PHI when discussing the client with his/her caregivers in the waiting room;
2. Do not discuss the client outside of the Clinic;
3. Do not discuss the client with anyone other than supervisors, unless specified on Authorization form;
4. Do not allow telephone calls discussing the client to be overheard by others;
5. De-identify the client for any class discussions.

For telephone messages, it will be important to tell student that they may leave telephone messages and appointment reminders on the client's answer machine if there is no link to medical information. They may also identify the clinic name and appointment time. A major exception is if the client requested an alternate means of communication. For Sign - in sheets, one should use name and time only; for schedule boards one should use initials only.

For client records (paper), the following rules will apply: do not remove the client record from the clinic floor; store records in locked file cabinets in secure areas and lock records overnight. Clinics should use an overnight file after clinic hours. During all times, users should turn the record face down when using on desk/table, de-identify working files and secure test protocols in the file immediately after evaluation sessions. In general, one should not photocopy from the client record unless needed for TPO or as authorized.

For video or audio recordings of clinical interactions, the following rules will usually apply: Mark with client initials and date of service only, rather than names. View or listen to recordings only in the presence of the treatment team. Following use, one should erase tapes or return them to the supervisor.

For Fax communications, the following rules will usually apply: Limit use to purposes that expedite treatment, not for convenience. Be sure to use a cover sheet

with a confidentiality statement. Do not state any PHI on the cover sheet (e.g., client name, DOB, medical record number, etc.) When sending faxes, ensure correct telephone number before transmission; call and verify any number in question before sending. Further, verify that the correct fax number has been dialed. After this, re-file faxed information with the fax cover sheet in the client's record and document the transmission in the client record. When receiving faxes, remove the transmission from the tray immediately upon completion of transmittal. Count the pages to ensure all have been received. Then, place documents containing PHI in a sealed envelope in the appropriate person's mailbox. If a fax transmission fails to reach the recipient, check the internal logging system of the fax machine to obtain the recipient's fax number. Then Send a fax to the incorrect number and request that the faxed information be destroyed immediately. Call the intended facility and confirm the fax correct number. Finally, notify the privacy officer of an inadvertent disclosure.

Guidelines for PHI destruction

Shred all paper documents with PHI; if the data are in electronic form, overwrite or reformat disk

Physical Safeguards

For electronic files, it is important to restrict access to those who have a right to use PHI. Save client files with PHI only to password-protected desktops in computer labs on the clinic floor (may not be transported to other university lab locations, home, etc.) Instruct students to print documentation with PHI only in the computer lab on the clinic floor. Clinicians should de-identify all information on floppy disks and de-identify email content concerning clients. At computer workstations, students should be reminded to position screens so that others cannot see PHI. They should return to the main menu or log off if leaving the computer, or use password protected screen savers.

For mail, both intra-campus and US, correspondence should be placed in sealed envelopes (no open envelopes should be used, as is sometimes the case on campuses).

To ensure record security, administrators should log-in the return of facility keys at the end of the student's program or if employment is terminated. In issuing passwords, be sure to include a combination of letters and numbers. Students should be warned not to reveal them to anyone (and in some practices only to the Privacy Officer). Passwords should not be posted on or near workstations and should be changed regularly according to security procedures.

Visitors and clients should be accompanied by members of the workforce when in areas with PHI. The parent, guardian, legal representative, or family member may observe a session relating only to the parent's child or family member who is receiving services. During simultaneous sessions in observation rooms that allow viewing into more than one treatment area, these individuals may not observe unless accompanied by students, clinic supervisors, or members of the treatment or diagnostic team, and only one client may be observed during a given treatment or diagnostic session. The client, parent, guardian, or legal representative must sign the Authorization for Use and Disclosure of Health Information form to allow observations by individuals

who are not university students, clinic supervisors, or members of the treatment or diagnostic team (i.e., teachers, case managers, etc.).

Students may observe clinic sessions for clinical training purposes, but must follow procedures as stated in Clinic Observation Policies; they must keep observation information confidential. Information may not be discussed with others who are not part of the client's treatment or diagnostic team.

AAC Devices present unique privacy issues. Both the storage of logged materials and viewing of communication logs may allow access to personal information. Thus, we recommend using password protection, including guidance in informed consent and use of encryption levels.

Section II – RESEARCH

Covered entities include health plans and health care providers that transmit health information electronically in connection with HIPAA transactions. Researchers are not themselves covered entities (unless they are also health care providers and engage in any of the covered electronic transactions). If researchers are employees of a covered entity, they may have to comply with that entity's HIPAA privacy policies and procedures. For researchers who currently obtain protected health information (PHI) from a covered entity, and for those investigators who in the future may wish to obtain PHI as part of their research or to pre-screen potential research subjects, the requirements imposed by HIPAA will change how you conduct your research.

The release of health information that has been properly and completely de-identified is not regulated by HIPAA. However, the investigator may be subject to IRB review. The basic rule is that "research" is not part of "treatment," "payment" or "health care operations," and therefore the researcher must obtain a written authorization that complies with the requirements of the HIPAA Privacy Regulations.

Requirements of a valid authorization include the following. A valid authorization must be written in "plain language" and must contain certain "core elements," including:

- The name of the individual whose information will be used or disclosed.
- A meaningful and specific description of the information to be disclosed.
- The name or specific identification of the person or class of persons who are to receive the information.
- A description of the purpose of the disclosure.
- An expiration date or expiration event.
- The date and signature of the individual or the individual's "personal representative," (such as the parent of a minor, or the individual's attorney-in-fact or guardian).

In addition to the "core elements," the authorization must contain statements concerning the individual's right to revoke the authorization in writing, the exceptions to the right to revoke the authorization and a description of how the individual may revoke the authorization. It should also disclose the ability (or inability) of the covered entity to make the treatment, payment, enrollment or eligibility for benefits conditional on the authorization, as well as the potential for the information to be redisclosed by the

recipient to others and to lose federal privacy protections concerning use and disclosure of the information. The participant must be given a copy of his/her authorization.

What is de-identified information?

De-identified information is not "protected health information" as defined in the HIPAA Privacy Regulation. Information is considered de-identified if all of the following identifying information is removed: Social Security number, health plan beneficiary numbers and other identifying information; account numbers; certificate of license numbers; vehicle identifiers and serial numbers that include license plate numbers; device identifiers and serial numbers; Web Universal Resource Locators (URLs); Internet Protocol (IP) address numbers, full face photographic images and other comparable images. Other more common identifying information includes:

- Name
- Medical record numbers
- Geographic subdivision smaller than a state including street address, city, county, precinct, zip code
- Any and all dates (except the year), including birth date, encounter date, and date of death
- Telephone numbers
- Fax numbers
- Electronic mail addresses
- Any other unique identifying number, characteristic or codes
- Finger prints and voice prints

A key point about research is that, in general, covered components cannot use or disclose PHI for Research unless they have obtained an individual's signed Authorization. For research, the Privacy Rule permits covered components to use and disclose PHI for research conducted with individual authorization or without individual authorization under limited circumstances.

Prior Authorizations

The Privacy Rule permits a covered entity to continue to use and disclose information based on an authorization from the patient received prior to the compliance date of April 14, 2003, even if the authorization does not meet the requirements of the Privacy Rule.

A covered entity may also continue to use or disclose protected health information created or received for a specific research study authorized before the compliance date, if, prior to the compliance date, the covered entity obtained informed consent of the individual to participate in the research study or a waiver of informed consent by an IRB for the study in accordance with the Common Rule or the FDA's human subject protection regulations. If a prior study involves accrual of new subjects after April 14, 2003, the researcher will need to obtain a written authorization from the new subjects, or will need to seek a new application to the IRB for a waiver, if it is not possible to obtain authorization, or if the IRB has waived informed consent.

Use of PHI without Authorization

Individuals may apply to an IRB or Privacy Board to use PHI without authorization. They should complete a University Application for waiver of authorization or modification of authorization under the HIPAA Privacy Rule. The requirements of the waiver are:

- Minimal Risk to the privacy of individuals
- Research not practical without waiver
- Research not practical without access to the specific PHI

Covered entities may also permit researchers to review PHI in medical records during reviews preparatory to research. Requirements specify that no PHI will be removed from the covered entity during the review and that the PHI that the researcher seeks to use or access is necessary for the research purposes. In some instances, the purpose of the research prevents the removal of all the information required by HIPAA. In such cases, information within certain guidelines can be released to researchers through the use of a Data Use Agreement to access a limited data set. To qualify as a limited data set all "facial identifiers" must be removed.

Section III - HIPAA PRIVACY AND SECURITY AUDITS

The Privacy regulations state that covered components may not use or disclose PHI unless permitted by the regulation and procedures designed to protect this information. HIPAA requires the University to ensure the safety of individually identifiable health information and to ensure proper security as a part of that requirement. The standards protect the information in paper format, computer format or discussed orally. Assessment of all covered components is based on the HIPAA Privacy Rule. Once the assessment is complete, action plans address the identified areas of improvement. Privacy assessments should occur annually. The ITaP Security group, in cooperation with the HIPAA Privacy Compliance Office, assesses the security of electronic systems and storage of protected health information (as mandated in HIPAA and the Gramm-Leach Bliley Act (GLBA). Security assessments also occur annually.

A Sample Privacy and Security Audit

"The IT Security and Policy group will be working with your department to conduct a HIPAA risk assessment. HIPAA, which is the Health Insurance Portability and Accountability Act of 1996, is a comprehensive law affecting institutions and departments that deal with protected health information. It requires the University to ensure the safety of individually identifiable health information, and to ensure proper security as a part of that requirement. As part of this assessment, you may receive questionnaires, or be asked to participate in meetings to help identify HIPAA compliance issues or security risks. We appreciate your assistance - it is the key to a successful and complete assessment.

Those staff members who are asked to participate in risk assessment meetings will help to determine assets (such as data and systems), risks to those assets, such as disclosure or destruction, and to help identify processes and policies that are needed, or that are already in place. If you are asked to participate in one of these meetings, you

can best help by preparing for it with a mental list of what assets and risks that you know of, and coming to the meeting prepared to brainstorm and work with others from your group or organization.

Security Scans

As part of the HIPAA risk assessment, IT Security and Policy will be conducting a security scan of the computer systems on your network. This scan is a non-intrusive scan and simply looks for information that your computer provides to the outside world through its Internet connection. To do this, it queries the computers and determines what services and information they offer to the world, then determines how those services are configured and if they need to have security patches or preventative measures applied. This scan does not check the contents of your hard drive or what software you are running on your desktop! It will, however, help us find out what is needed to make your system more secure and help IT Security and Policy assess the network as a whole.”

Section IV – A SAMPLE EMPLOYEE/STUDENT CONFIDENTIALITY AND SECURITY AGREEMENT

“As an employee, student-employee/student clinician, I acknowledge that I may have access to highly sensitive and confidential personal, medical, student, or workplace information. I may receive this information directly from individuals or indirectly from third parties who may provide this to me for work related purposes. I further agree that I will maintain the confidentiality of personal medical information and information contained in patient/student records. Information I receive of a confidential or personal nature will be used or disclosed to others only when it is legally permissible to fulfill the essential requirements of my job/ clinical practicum assignment, and then on a strict need-to-know basis.

As a condition of my employment/participation in clinical practicum, I agree that I will NOT do any of the following:

- Remove any records, reports or copies of documents containing confidential or personal information from their storage location except as needed for the performance of my duties;
- Release my user identification code(s) or password(s) to anyone, or allow anyone to access or alter information under my identity.
- Access, use or disclose confidential information for any personal purpose or out of curiosity, or allow others to do so by giving them my access codes, passwords or use of my equipment for any purposes not essential to my work or theirs.
- Take patient information from the premises in paper or electronic form unless all identifying information has been deleted or appropriately coded.

I further agree that I WILL:

- Only use confidential and personal medical or student information as needed to perform my job and will only disclose this information to those authorized to receive it;
- Report unauthorized disclosures of personal medical or student information to my supervisor;

Meeting the Challenges of HIPAA

- Comply with email, telephone and fax procedures designed to protect the confidentiality of information being transmitted;
- Abide by all procedures and policies established to protect the privacy and confidentiality of personal medical or student information;
- Abide by all procedures and policies established to manage the use of the software, network, reporting, and use of components that comprise the Human Resource data management system;
- Keep personal information about staff, faculty, students or any member of the University community including information in databases and hard copy files secure and ensure that it is not readily accessible to others.

I am expected to be familiar with/and abide by policies and procedures applicable to me concerning the privacy and security of personal, medical or student information.

I am responsible for logging out of information systems and will not leave unattended a display device to which I have logged on;

My user identification code and password are the equivalent of my signature and that I am accountable for all entries and actions recorded under them;

My obligation to maintain the confidentiality of personal medical information and information contained in patient/student records under this agreement will continue after termination of my employment/clinical practicum and my privileges are subject to periodic review, revision and renewal;

Violations of this agreement will be subject to sanctions up to and including termination of employment/loss of clinical privileges.

By signing this, I agree that I have read, understand and will comply with this agreement.

Signature: _____

Date: _____

Printed Name: _____

Department: _____

References and Resources

ASHA HIPAA information:

http://www.asha.org/about/legislation-advocacy/federal/hipaa/hipaa_index.htm

Audiology

<http://www.audiology.org>

<http://www.hearing.org/hipaa/>

<http://www.hcAnalytics.com>

Federal HIPAA sites:

<http://www.aspe.hhs.gov/admnsimp>

<http://www.hipaa.org>

Medicaid and Medicare

<http://www.cms.hhs.gov/hipaa/>

Meeting the Challenges of HIPAA

Phoenix Health Systems <http://www.hipaaadvisory.com>

Privacy Rule (Office for Civil Rights)

<http://www.hhs.gov/ocr/hipaa/>

OCR Guidance (explains significant aspects of the Privacy Rule):

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

Security Rule

<http://www.cms.hhs.gov/hipaa/hipaa2/default.asp>

For additional information regarding HIPAA Guidelines and Forms for Research, please visit:

<http://www.irb.purdue.edu/hipaaguidelines.shtml>

<http://privacyruleandresearch.nih.gov>