

Physician Module: Lesson 1

Introduction:

Confidentiality and trust have always been an integral part of the physician-patient relationship. Some physicians may feel that the new “Privacy Rule” is unnecessary because physicians already know how to keep **health information (1)** However, HIPAA formalizes expectations for all health professionals to follow regarding patient rights and for safeguarding identifiable health information. Previously, there has been no federal protection of health information, just a patchwork of various state laws.

From the Hippocratic Oath:

All that may come to my knowledge in the exercise of my profession or outside of my profession or in daily commerce with men, which ought not to be spread abroad, I will keep secret and will never reveal.

General Purposes and Provisions of the Rule:

What Is HIPAA?

The “Privacy Rule” is a provision of the Health Insurance Portability & Accountability Act of 1996 (HIPAA). The purposes of the regulation are to:

- Protect and enhance the rights of consumers to their health information and control the inappropriate use of the information
- Improve the quality of **health care (2)** in the U.S. by restoring trust in the U.S. health care system
- Improve the efficiency and effectiveness of health care delivery by creating a national framework for health privacy protection that builds on efforts by states, health systems, and individual organizations and individuals.

Increasing public concern about loss of privacy, the advent of interconnected electronic information systems, advances in genetic sciences, and the rapid growth of integrated health care delivery systems all contributed to the reasons why these provisions of HIPAA were enacted.

The five basic principles of the Rule include:

Consumer Control –

Patients have new rights to control the release of their medical information.

Boundaries –

A patient’s health information should be used primarily for health purposes; any other uses must be kept to the minimum necessary for a specific purpose (i.e., application for life insurance).

Accountability –

There are specific federal penalties for violating the privacy regulations.

These penalties range from a \$100 fine per violation for disclosures made in error, up to \$250,000 and 10 years in prison for malicious use of records.

Public Responsibility –

Specific information is provided about releasing health information for public health, research, fraud and abuse investigations, and quality improvement purposes.

Security –

Health care organizations must establish clear procedures to safeguard health information. Entities who must comply with the HIPAA standards are health care providers who conduct financial or other administrative functions electronically; all health plans; and all health care clearinghouses. These entities are known as “**covered entities (3)**.”

HIPAA protects **Protected Health Information**, which is **individually identifiable health information** that is maintained or transmitted in *any* form (electronic, paper, or spoken).

Identifiable health information includes:

- Any information that relates to the past, present, or future physical or mental health or condition of an individual
- The provision of healthcare to an individual
- Past, present, or future payment for health care services
- Anything that identifies the individual (or can be used to identify the individual).
- Medical and demographic information collected from an individual, and created or received by a health care provider, health plan, employer, or health care clearinghouse.
- Names
- Geographic Subdivisions
- E-mail Addresses
- Fax or Phone Numbers
- Medical Record or Social Security Numbers
- Full-face Photographic Images
- Finger Prints or Voice Prints
- Birth Dates
- Hospital Admission or Discharge Dates
- License Plate or VINs (Vehicle Identification Numbers)
- Health Plan Beneficiary Numbers

When do we have to comply with the HIPAA standards?

The compliance date is April 14, 2003

HIPAA Compliance Requirements:

- Designate a privacy officer to oversee all activities related to HIPAA implementation and compliance.
- Give the patient a Notice of Privacy Practices (NPP) to inform patients about how the organization uses and discloses protected health information, and how the organization protects the rights of consumers by safeguarding their information. **Merely posting a Notice or making the Notice available is not enough.**
- Make a “good faith effort” to obtain a signed acknowledgement from the patient that he or she has received the Notice of Privacy Practices.
- Establish policies and procedures for securing the patient’s written authorization to use or disclose a patient’s health information for purposes other than treatment, payment, and health care operations, except in certain specific situations (see lesson 4) or as permitted.
- Develop or revise policies and procedures for ensuring your patients’ rights to:
 - Receive a Notice of Privacy Practices (NPP)
 - Inspect and copy their own medical record
 - Make an amendment to their medical record
 - Request restrictions on the use of their health information
 - “Opt out” or decline to be included in facility directories or receive fundraising information
 - Receive an “accounting” or list of (certain) disclosures of their health information
 - Receive confidential communications
 - Complain about how your office has used or disclosed their health information.
- Determine what protected health information is the “**minimum necessary**” needed by an employee (other than treatment personnel) to do his/her job.
- Insert required HIPAA language into contracts with vendors or businesses who use PHI to assist you, such as billing companies or IT vendors.
- Follow the established IRB common rule and HIPAA regulations and procedures for using and disclosing individually identifiable patient information for research purposes.
- Establish procedures that ensure fundraising personnel learn only patients’ demographic information and dates of service, and that patients can “opt out” or decline to receive fundraising communications or materials.

- Information relating to diagnosis or treatment cannot be communicated or used for fundraising purposes.
- Be sure that no **marketing** (materials that encourage a patient to use a service or product) materials are sent to patients without first securing a patient's signed authorization (marketing does not include hospital newsletters or other communications regarding a hospital's or physician's own health-related services or products).
- Develop a procedure for logging and addressing privacy complaints from patients and staff.

According to Kate Borten, editor of the *HIPAA Training Handbook for the Medical Staff* (Opus Communications, 2001):

“The role of the physician has changed: what was once an unregulated responsibility to protect patient privacy is now a legal one. Physicians are privy to more confidential health information than perhaps anyone else in the organization....under HIPAA, the hope is that educated patients will be able to trust their providers and the organizations in which they work.”

To build trust, the Privacy Rule calls on covered entities to learn the rules and then live them.

Definitions:

- 1. Health Information** - Any information, whether oral or recorded in any form or medium, that is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.
- 2. Health Care** means care, services, or supplies related to the health of an individual. Health care includes, but is not limited to, the following: preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status, of an individual, or that affects the structure or function of the body; and sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription.
- 3. Covered Entity** means: a health plan, a health clearinghouse, or a health care provider who transmits any health information in electronic form in connection with a standard financial or administrative transaction listed in Section 1173(a)(1) of the Act and Section 160.103 of the Final Rule.

Physician Module: Lesson Two

Introduction:

The goal of lesson two is to describe the various rights and controls individuals have over their **PHI (Protected Health Information)**.

This lesson will also provide you with information on ways to safeguard patient information in your day-to-day work, such as:

- Using and protecting computer passwords
- Proper disposal of information
- Remaining aware of your surroundings when discussing patients.

Standards for Individually Identifiable Health Information:

The Standards for **Individually Identifiable Health Information (1)** (Privacy Rule) assures that patients have specific rights regarding the **use** and **disclosure** of their protected health information (PHI). These rights are covered below.

Patient Rights for Use & Disclosure of their PHI:

Under HIPAA, a **covered entity (2)** must provide a patient with a copy of its Notice of Privacy Practices. The Notice informs the patient of his or her rights with regard to his or her protected health information, gives adequate notice of the uses and disclosures of the individual's PHI a covered entity might make, and informs the patient of the covered entity's legal duties to protect PHI.

The Notice must be conspicuously posted in the location of the Covered Entity, and a notice must be given to each individual. **MERELY OFFERING A COPY OF A NOTICE IS NOT SUFFICIENT!!**

Under HIPAA, a health care provider must permit an individual to restrictions on the uses or disclosures of the individual's PHI. The provider is not required to agree to a restriction.

However, if the provider agrees to a restriction, the restriction must be documented and must be honored, unless the individual rescinds the restriction or there is an emergency situation.

Key Point to Remember: A patient has the right to ask for a restriction, the provider is not required to agree.

Under HIPAA, a health provider must permit and accommodate reasonable requests by individuals to receive communications of PHI by alternative means. A provider may require that the request be in writing.

This may entail:

- Sending the patient a letter instead of giving a telephone call, or

- Communicating the information to the individual at an alternative location, such as calling or sending a letter to the individual's work instead of his or her home address.
- It can also mean giving the information in person under more private conditions, such as in conference room with door shut, not in semi-private patient room.

If a patient requests that her PHI be disclosed to her at a specific address, the provider may require the patient to provide an alternate address or other means of contact including information about how payment, if any, will be handled.

A provider MAY NOT require the individual to explain why the alternative communication is needed. [See Module IV for more information on this issue.]

Key Point to Remember: Contact patient at the designated location and in the designated manner.

An individual has a right to inspect and obtain a copy of PHI about him or her contained in a designated record set. A designated record set is broader than a medical record.

The **designated record set** includes the medical record, billing records, or groups of records that are used, in whole or in part, by or for the covered entity to make decisions about the individual.

HIPAA sets the minimum for access rights. However, Ohio Law gives individuals a greater right of access to PHI. If a patient wishes to inspect or copy his or her medical record, direct them to Medical Information Management.

Key Points to Remember:

- Patients have the right to access their medical information.
- Direct the patient to Medical Information Management.

Patient Rights to Change Health Information:

Under HIPAA, an individual has a right to request that a health care provider amend the information or medical record pertaining to her.

A provider may deny an individual's request for amendment if the record:

- was not created by the provider
- to be amended is not part of the designated record set

- would not be available for inspection (under the reasons given for denial of access)
- is accurate and complete.

Key Points to Remember:

- Patient has right to amend medical information.
- Direct the patient to Medical Information Management.

Patient Rights to Receive Disclosures of Health Information:

An individual has a right to receive an accounting (list) of certain disclosures of PHI made by the provider for the lesser of either six (6) years prior to the request date or April 14, 2003.

(Note: A covered entity need not provide an accounting for disclosures that occurred prior to April 14, 2003).

Patient Rights to File a Complaint:

In the Notice of Privacy Practices, a covered entity must inform an individual about her right to file a complaint if she feels that the covered entity has violated her privacy rights or wishes to complain about the covered entity's privacy policies and procedures.

A covered entity may not retaliate against or intimidate an individual for making a complaint.

Key Points to Remember:

- Individuals may file complaints.
- Direct the patient to the Privacy Office at 293-4477

Physician's Role in Safeguarding PHI:

An integral part of the physician-patient relationship is the physician's commitment to safeguard the patient's health information. Technological advances have revolutionized health care, and access to patient information has been made much easier as records have become electronic.

However, safeguarding such information is also more difficult.

Our duty to protect health information extends to all forms of information.

Protecting Data in PDAs:

Use passwords to access personal digital assistants (PDAs) or other hand-held computer, and be sure to keep track of these devices even at home so that others cannot see patient information.

Delete patient information from PDAs as soon as possible.

Watch for “Hidden” Information Locations:

Be aware that some biomedical devices store patient information. These devices (i.e., anesthesia units, clinical analyzers, ECG machines, infusion pumps, MRIs, and vents) are covered by HIPAA if they display memory, connect to another system, or transfer or store data.

Protecting Other Data Sources:

- Secure documents that contain patients’ health information before creating spreadsheets, Access databases, or other documents.
- Follow the Health System’s e-mail policy and guidelines when corresponding with or about patients.
- Do not remove patient records from the hospital or office unless a secure mechanism has been developed for transport, and records can be secured in the other location.
- Ask someone to retrieve expected FAXes and printed patient information.
- Use approved FAX cover sheets at all times, and verify the FAX number of the recipient before transmitting patient information.
- Keep private offices that contain patient information locked when not in use.
- Remember that physicians who are not directly involved in an individual’s care should not access the medical records of colleagues, hospital or office staff members, spouses, or other family members, neighbors, or friends unless specifically authorized in writing by the individual.
- Gather and remove any lists of patients, printouts of test results, or other identifiable patient information from conference and meeting rooms used in patient staffings or grand rounds.
- Be sure someone takes all medical records back to the patient care unit or office.
- Remember to properly dispose of anything containing patient information.
- Shred the information or place it in a locked disposal bin. If your bin is full, call the telephone number on the bin for a replacement.
- Be sure that patient information carried on the physician’s person (such as handwritten notes on cards and printed lists of patient information) does not fall out or is not left on counters, the floor, etc.

Be Aware of Your Surroundings:

- Use discretion in discussing patients with colleagues, patient care staff, and students.
- It is important that physicians consider the information passersby, including family members, or patients themselves, might overhear.
- Obviously, discussions **should not** take place in elevators, while waiting in line in the cafeteria or other food vendors or the ATM machine, the hospital lobby, or gift shop.
- When dictating patient information, close the office door.
- Use discretion when discussing medical information with patients and family members.
- Draw privacy curtains, keep voices low, and honor patient requests to hear the information in a conference room or other private location.
- It is important that physicians do not begin sharing medical information with patients in full earshot of a roomful of persons in waiting rooms, lobbies, and hallways.
- Although you may not be able to go to a private room, consider moving across the room to a corner or another hallway.

HIPAA Password Tips:

- Physicians should keep passwords secret.
- Passwords should not be shared with anyone else, including other physicians, secretaries, and nurses.
- Physicians should expect to change their passwords upon their initial login to the system or application and again at regular intervals.
- Most applications track the user's password history and will not allow a previously used password to be re-used. Furthermore, users will only be granted one account per login per application unless additional logins are need for hospital business.

The following words, characters and phrases **should not** be used as passwords on any OSU Health Systems application:

- Words or phrases pertaining to Ohio State University (Buckeyes, Go Bucks, OSU, OSUMC...)
- The user's first, middle, last or login name in any form (as it is, capitalized, reversed, doubled, etc.)
- Personal information easily obtained about the user (license plate, hobbies/interests, telephone numbers, social security numbers, automobile numbers, pets, spouse, address, etc.)

- The following words, characters and phrases **should not** be used as passwords on any OSU Health Systems application:
- A word contained in any dictionary, spelling list or other lists of words such as a book.
- A password shorter than six characters
- Letter sequences right off the keyboard like QWERTY, MNBVCXZ
- The hostname of a computer.

Why is Your User Login Important?

- Unauthorized users can jeopardize the security of information stored on or accessible from a computer.
- To prevent this, we must configure the computer to authenticate all users who attempt to access it.
- Notify Information Systems Security or the Help Desk if you suspect suspicious activity regarding your computer accounts.
- Your computer ID and password are your unique identifiers; they let the computer systems know who is actually using the computer and accessing data.
- You should never share your ID or password. Computer audit records will show you as the authorized user. You can be held responsible for the actions of the individual(s) that you have shared your password with.

All staff must:

- Know what data is considered confidential
- Understand confidentiality policies
- Comply with confidentiality policies
- Report suspected or known breaches of confidentiality to management or security administration immediately

Managers will:

- Immediately report staff changes (terminations and transfers) to Data Security
- Educate staff in their responsibilities regarding information security.

Computer Viruses:

A computer virus is a program with the intention of spreading itself by first infecting files or system areas of hard and floppy disks and then replicating itself. The user usually has no knowledge that a virus is effecting their computer. Viruses can spread through e-mail or from downloading files and programs from the Internet. When you execute a program that's infected by a virus, the virus will run and try to infect other programs or files, either on the same computer

or other computers connected over a network. The newly infected programs will try to infect yet more programs. When you share a copy of an infected file with other computer users, running the file may also infect their computers with the virus spreading rampantly.

To help reduce the spread of viruses:

- Don't open e-mails from unknown sources
- Always make sure your virus protection software is running
- Notify the Help Desk if you suspect your computer may be infected.

Conclusion:

HIPAA stipulates new and expanded patient rights to privacy and confidentiality of their health information.

- All patient record documentation should be clear, accurate, complete, and timely.
- The “safeguarding” provisions are common sense – but worth careful review, not just because these “tips” are now part of Federal law, but because it's also the right thing to do.

Definitions:

1. **Individually Identifiable Health Information** - Information that is a subset of health information, including demographic information collected from an individual, and: is created or received by a health care provider, health plan, employer, or health care clearinghouse; and is relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and that identifies the individual; or, with respect to which there is a reasonable basis to believe the information can be used to identify the individual.
2. **Covered Entity** - A health plan, a health care clearinghouse, a health care provider who transmits any health information in electronic form in connection with a standard financial or administrative transaction listed in Section 1173(a)(1) of the Act and Section 160.103 of the Final Rule.
3. **Designated record set** - A group of records maintained by or for a covered entity that is: the medical records and billing records about individuals maintained by or for a covered health care provider; the enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or used, in whole or in part, by or for the covered entity to make decisions about individuals.

Physician Module: Lesson 3

Introduction

The purpose of this module is to acquaint physicians with HIPAA's specific paperwork requirements, and to help physicians and their office staff evaluate and modify office operations to comply with the Privacy Rule.

What is the Notice of Privacy Practices?

The Notice of Privacy Practices (NPP) is a central focus of HIPAA administrative requirements. The purpose of the Notice is to inform persons about:

- how health providers may use and disclose individuals' protected health information
- their rights under the regulation
- the health provider's legal duties regarding protected health information.

Providing the Notice of Privacy Practices:

The NPP must be provided no later than the date of first service delivery after the HIPAA compliance date (April 14, 2003).

The health provider must:

- Make hard-copies of the Notice available in the office.
- Post the notice in a clear and prominent location in the office.
- If the Notice is revised, make the document available upon request.
- Notices may be provided by electronic mail.
- If the provider maintains a website, the Notice must also be posted on the site.

Required Elements for the Notice of Privacy Practices:

- The NPP must be written in plain language.
- The header must say:
“This notice describes how medical information about you may be used and disclosed and how you can get access to this information. Please review it carefully.”

The Notice must contain:

- Descriptions of the types of uses and disclosures that the health provider is permitted to make for treatment, payment, and health care operations.

- Descriptions of each purpose for which the provider discloses PHI without obtaining the patient’s written authorization (e.g., as required by law, for health oversight and public health activities).
- statements about specific uses or disclosures related to activities such as fundraising and appointment reminders; statements about the individual’s rights under HIPAA.
- statements about the health provider’s duty to maintain the privacy of protected health information and to abide by the terms of the Notice currently in effect.
- instructions about how the patient may register a complaint if the patient believes his/her privacy rights have been violated.
- a contact person with phone number.
- effective date of the Notice.

The Acknowledgement of the Notice of Privacy Practices:

Except in an emergency treatment situation, providers must make a “good faith effort” to obtain a written acknowledgement of the individual’s receipt of the Notice of Privacy Practices.

If the provider is unable to obtain a written acknowledgement, document the reason why the acknowledgement was not obtained in the patient’s record.

The health provider must attempt to present the Notice at the first service delivery after the compliance date, including service delivered electronically.

If the encounter occurs over the telephone, the provider should mail the document to the individual the next day, including a tear-off sheet for the patient to mail back. If the patient does not reply, the provider has satisfied the “good faith effort” requirement.

HIPAA does not mandate a specific form to use for the Acknowledgement. A provider may have the individual initial a cover sheet, sign a separate form, or use a log that contains multiple signatures of persons who have acknowledged receipt of the Notice.

HIPAA Authorization:

The HIPAA Privacy Rule does not require providers to obtain the patient’s consent to use and disclose protected health information for treatment, payment, and health care operations.

However, most other uses and disclosures require the patient’s written authorization.

Examples of situations that require the patient’s written authorization:

- to disclose information to an employer for an employment decision or to a life insurance company to determine the person’s eligibility
- to use or disclose psychotherapy notes
- To release protected health information for marketing (obstetrician wants to sell patient list to a diaper company)
- to use PHI for research.

Elements of the HIPAA Authorization:

A HIPAA authorization includes:

- a description of the specific information to be used or disclosed.
- the name and/or title of the person(s) authorized to use or disclose the information (Dr. X, or “administrative staff;”).
- the name and/or title of the person(s) who will receive the information (another doctor, facility, company).
- description of the purpose(s) of the use or disclosure.
- an expiration date or expiration event related to the use(s) or disclosure(s) of the information (e.g., “at the end of the research study”).)
- signature of the individual and date signed.

The provider must include statements that address:

- The individual’s right to revoke the authorization in writing.
- The provider may not condition treatment or payment on the provision of an authorization except that related to research-related treatment or use of PHI for research, or the provision of health care that is solely for the purpose of creating PHI for disclosure to a third party.
- The consequences to the individual of a refusal to sign the authorization when the provider is permitted to condition treatment on the provision of the authorization.
- The potential for information disclosed to be re-disclosed by the recipient and no longer protected by the Privacy Rule.

Go to www.ama-assn.org/ama/pub/category/6900.html to view the AMA’s model HIPAA Authorization.

The Minimum Necessary Standard:

Under HIPAA, physicians are permitted to share a patient's entire medical record with other health professionals for treatment purposes; all other uses and disclosures must adhere to the "minimum necessary" standard - **the physician must limit the amount of protected health information shared to that needed to fulfill a specific purpose.** For example, an entire medical record is not needed to establish eligibility for life insurance, or for disclosures to public officials.

Physicians should work with office managers to determine which employees need access to what types and amounts of patient health information to carry out their duties.

Policies, procedures, and criteria should be developed to assure that only the minimum necessary health information is used or disclosed by the physician or his/her office staff members.

If someone asks for patient information, it's imperative that the physician or his/her staff know why the information is needed, and limit the disclosure to only the information needed to answer the question.

Office Practice Considerations – The Waiting Area

What can patients hear in your waiting room?

Receptionists should devise ways to talk with patients by telephone so that health information will not be overheard by waiting room patients. (For example, do not say a patient's name, address, etc. aloud and then discuss test results or treatment plans). Take care so that patients are not asked medical questions while they are standing at the reception desk.

What can patients see at the front desk?

Sign-in sheets should contain ONLY the patient's name and time of arrival. (Sign-in sheets should never reveal the reason for visit or a diagnosis, or a doctor's name that would "give away" the patient's diagnosis if in a multi-specialty clinic). Patient records and loose sheets of information should be kept out-of-sight of persons standing at the counter. Keep computer screens that might show patient information away from full view of persons standing at the counter.

Office Practice Consideration – Exam Room:

What can patients see and hear in exam-room hallways?

- If charts or clipboards containing patient records are kept in door pockets, turn them inward so that names are not in view of passersby.

- **Patient information (appointments, follow-up notes, lab printouts, etc.) should not be posted on bulletin boards in hallways where patients will be walking.**
- **Physicians should always go to an office and shut the door when dictating notes and reports after a patient's visit.**
- Don't discuss patient-specific information among staff members when patients and family members are proceeding through hallways.
- **If computers are placed on carts outside exam rooms, be sure that patient information is not left "up" on the screen for anyone to read. Be sure to secure the patient's record after the patient has departed.**

Office Practice Considerations – File Rooms & Record Areas:

Are patient records kept in a secure area?

- **If records are not kept in a locked medical records office, pull-down covers should be provided for open-records systems, or records should be placed in locked file cabinets.**
- Records should not be kept in unsecured areas overnight (desktops, counters, open bins, mailboxes, etc.)
- Records should be gathered before daily close of business and secured in approved areas.

Office Practice Considerations – Office Technology

Using FAX machines and printers:

Modern technology has greatly enhanced our ability to communicate among professionals.

However, human error can quickly turn faxing and printing computer documents into HIPAA violations. For example, one hospital faxed a patient's record to the local newspaper instead of the medical record's department because the newspaper's fax number was one digit different from the department's number. The newspaper wrote an article about the hospital's carelessness.

Here are some pointers for using fax machines and printers in physician offices:

- Keep faxes and printers away from public areas.
- Designate someone to retrieve patient information quickly from printer and fax bins.
- Be sure to use a fax cover sheet that alerts receivers that confidential health information is enclosed, and what to do if a misdirected fax is received.
- Limit faxing of patient information to situations in which mailing is not feasible.

- Confirm the accuracy of fax numbers; program frequently used fax numbers into your office fax machine.
- Be sure that your fax machine prints a confirmation of outgoing transmissions.
- Train employees to secure faxed and printed material from computers as soon as possible.
- Be sure that patient information doesn't get mixed-in with business information.

Office Practice Consideration – Communicating With Patients:

Appointment Reminders:

The Privacy Rule does not require specific language to use when reminding patients by telephone about appointments. However, it's important that we use the minimum necessary information to accomplish the task. It is prudent to get the patient's permission before leaving messages with family members or on answering machines/voicemail. A patient may not want her husband or child to know about a particular medical appointment, or someone may want messages to be left only at work or on a pager.

One script might be: "This is Dr. Jones' office with a message for Ms. Smith. Please call XXX-XXXX." Or, "This is Doctor's office with a message...." Health providers need to determine what is appropriate language. Mentioning specific appointments may be risky for some practices, and not others.

Test Results; Notices:

Use letters or fold-up postcards with seals to communicate test results to patients or to remind them about scheduling annual exams such as Pap smears and mammograms.

Office Practice Considerations – Use of E-Mail:

E-mail is a popular mode of communication. The Medical Center's policy on Electronic Resources (Policy #07-03) provides the following guidelines:

- Messages with confidential content must be transmitted to an individual directly (clinician to clinician) for purposes related to patient care...and are not to be broadcast to a distribution list.
- Patient-specific messages that reference highly sensitive information, e.g., information related to mental health or HIV diagnoses must not contain the

patient's name. Patient identification must be limited to the medical record number.

- Clinical e-mail messages must be promptly deleted after they are read. E-mail messages should not be saved or archived on a PC for any length of time.
- Patient-specific e-mail communications between clinicians should be documented in the patient's record just as other means of clinician-to-clinician communication would be.
- Communication of patient-specific information outside the OSUMC network using e-mail should be avoided and should never occur without appropriate patient's consent.
- E-mail and Internet accounts are assigned to individuals and each individual is responsible for the proper use of their accounts, including proper password protection.

The American Medical Informatics Association (AMIA) has published an excellent White Paper titled "Guidelines for the Clinical Use of Electronic Mail with Patients." The paper can be accessed at the following website:

http://www.amia.org/pubs/other/email_guidelines.html

The paper is dated 1998, and is currently being updated for 2002.

The Department of Health and Human Services Regulatory Reform Initiative has developed a top privacy concerns quiz. Click on the link below to view the quiz as a PowerPoint presentation.

http://www.regreform.hhs.gov/HIPAAQUIZ_0204171/index.htm

HIPAA is a combination of administrative requirements and rules for everyday interactions between health care providers and patients. The rules can be divided into one or more of the following categories:

- Patient rights
- Access to health information and medical records
- Disclosures of PHI to others
- Proper disposition and disposal of records

HIPAA is not intended to impede patient care, but the Rule does remind us that privacy and confidentiality are essential components of that care.

Physician Module: Lesson Four

HIPAA, Covered Entities may use or disclose an individual's protected health information (PHI) if certain requirements are met. There are four basic scenarios:

1. The covered entity obtained written permission or authorization from the individual;
2. The use or disclosure is for treatment, payment or operations activity of the entity
3. Situations in which the entity does not have to provide the individual an opportunity to agree or object to the use or disclosure; and
4. Situations in which the individual must be given an opportunity to agree or object to the use or disclosure.

Each scenario has its own rules and restrictions. The goal of this module is to inform you about provisions in the Rule that will require professional judgment in determining when to use or disclose protected health information in certain circumstances.

Marketing:

Under HIPAA, marketing is defined as making a communication about a product or service that encourages recipients of the communication to purchase or use the product or service.

A health provider may not use or disclose protected health information for marketing without an authorization, except if the communication is made in the form of:

- A face-to-face communication between the health provider and the individual; or
- A promotional gift of nominal value is given by the provider.

If an authorization is obtained, the authorization must state whether remuneration from a third party is involved, whether directly or indirectly.

The following situations are NOT considered marketing:

- Describing a health-related product or service that is offered by the health care provider.
- Communications regarding treatment options, case management, care coordination, alternative therapies, health care providers or settings of care for the individual.

Fundraising:

A health provider may use, or disclose to a business associate, or to an institutionally-related foundation, limited protected health information for the purpose of raising funds for its own benefit:

- An individual's demographic information (e.g, name, address, phone number, birth date, occupation, employer, spouse's name)
- Dates of health care service provided to the individual
- Medical Center Development personnel may not access any other information about the individual without the patient's written authorization. The Notice of Privacy Practices (NPP) also contains information about fundraising, including the patient's ability to "opt-out" of receiving fundraising materials or communications by written request.

Physicians may **not** share any information with Medical Center Development personnel about a patient's diagnosis, medical history, or even the fact that the physician treats the patient unless written authorization has been obtained from the patient.

Contact Medical Center Development at 293-2510 for further information about how physicians may work with Medical Center Development to continue to facilitate fundraising efforts.

Uses and Disclosures: Patients Must Have the Chance to Agree or Object

Under HIPAA, there are situations in which a health provider may use or disclose PHI if the individual was informed in advance, and has been given the opportunity to agree to, prohibit, or restrict the use of the health information.

No written authorization from the individual is required. The health provider may inform the individual of the specific use or disclosure orally, and the individual may agree or object orally as well.

If the individual does not object (and the applicable conditions or restrictions are met), the provider may:

- List an individual in a facility directory
- Directory includes: patient's name, location in the facility, general condition and religious affiliation.
- Only people who ask for the patient by name may obtain this information. Exception: clergy may ask for a list of all patients who have stated a specific religious preference (Methodist minister asks for all Methodists).

If patient is unable to agree or object, follow any known prior expressed preference of the patient and exercise professional judgment to determine whether disclosure is in the best interest of the individual.

If the individual does not object (and the applicable conditions or restrictions are met), the provider may:

- Use or disclose information to an individual involved in the patient's care
- Use or disclose information to notify, identify or locate a family member, personal representative, or other person responsible for the patient's care to inform her of the location, general condition, or death of the patient.

Examples of Uses & Disclosures:

- Provider may notify a patient's adult child that his father has suffered a stroke and tell the son that his father is in the hospital's intensive care unit.
- Patient brings spouse into the doctor's office when treatment is being discussed; it is reasonable to infer that the patient wants the spouse to know about her treatment.
- Friend has brought the patient to the emergency room for treatment: it may be reasonable to tell the friend that the patient has suffered a heart attack and provide further updates on prognosis and progress.
- Patient is riding home with a friend after visiting the ED and now is on crutches to go home: friend will likely need to know information about patient's immediate care needs, including mobility limitations getting into and out of the car, etc.

Rules and Restrictions for Uses and Disclosures:

- If the patient is present and able to agree: If patient agrees, or does not object, or it is reasonable to infer from circumstances that the individual does not object, disclose information directly relevant to the person's involvement with patient's care or payment.
- If individual is not present or able to agree or emergency situation: determine whether disclosure is in the best interest of the individual, and disclose only information directly relevant to the current situation.

Disaster Relief Areas & Disclosures:

- A “covered entity” may make disclosures to assist in disaster relief efforts. The disclosure must be to a public or private entity authorized by law or by its charter to assist in disaster relief efforts.
- Disclosure is for the purposes of coordinating with other organizations to identify, locate and notify the family member or personal representative about the location, general condition, or death of the patient.

Example: Manhattan hospital emergency rooms on September 11, 2001; hurricanes, floods, etc.

Uses and Disclosures: Patients Must Have the Chance to Agree or Object:**Key Points to Remember:**

If the patient is available, confirm with patient first.

If not, exercise your professional judgment, acting in the best interest of the patient.

Uses and Disclosures: The Chance to Agree or Object is Not Necessary:

Under HIPAA, a health provider may make certain disclosures without obtaining any permission from an individual. These uses and disclosures are ones that either are required or permitted under federal, state or local law.

However, because the individual does not generally have an opportunity to control or restrict these disclosures, the individual has the right to be informed about these disclosures through an “accounting” or official log.

These situations include uses and disclosures for public health activities, including, but not limited to:

- surveillance; investigations; tracking FDA-regulated products; reporting adverse events; reporting vital events; workplace health surveillance
- reports of child abuse or neglect
- notification of a person who may have been exposed to a communicable disease
- disclosures about adult victims of abuse, neglect, or domestic violence, subject to certain restrictions and requirements

Restrictions and requirements regarding public health disclosures:

- If law requires the public health disclosure, disclose only what the law requires.

- If the disclosure is **not** mandatory, use professional judgment to determine whether the report is necessary to prevent serious harm to an individual or other victim or there is an immediate need to act by law enforcement.
- The individual may choose to agree to the disclosure.

The individual must be told about the disclosure unless:

- doing so would place the individual at risk of serious harm
- the disclosure would be to the personal representative who is reasonably believed to be responsible for the abuse, neglect or other injury and informing him/her would not be in the best interest of the individual.

Situations other than public health activities in which the chance to agree or object is not necessary are:

- Uses and disclosures for health oversight activities (audits, inspections, investigations, licensure or disciplinary actions).
- Disclosures for judicial and administrative proceedings.

The following limited information may be provided in response to a law enforcement official's request for specific information in order to locate a suspect, fugitive, material witness, or missing person:

- Name and address
- Date and place of birth
- Social security number
- ABO blood type and Rh factor
- Type of injury
- Date and time of treatment
- Date and time of death, if applicable
- Description of distinguishing characteristics, such as height, weight, gender, race, hair and eye color, facial hair, scars, tattoo
- **NO: DNA information, dental records, typing, samples or analysis of body fluids or tissue**

Additional situations where limited information may be provided:

- Disclosures to law enforcement officials to alert them of a suspicious death that may have resulted from criminal conduct.

- Disclosures about a decedent's medical information to a funeral director or medical examiner as authorized by law.
- Disclosures to an organ procurement organization for cadaveric organ, eye or tissue donation
- Uses and disclosures to avert a serious threat to health or safety
- Uses and disclosures for specialized government functions (national security and intelligence activities; protective services)
- Disclosures to correctional institutions and other law enforcement custodial situations
- Disclosures for Worker's Compensation
- Uses and disclosures for research purposes with a waiver of individual authorization obtained from an IRB or Privacy Board.

The Role of Personal Representatives:

If under applicable law, a person has authority to act on behalf of an individual who is an adult or emancipated minor to make decisions related to health care, a health provider must treat such person as a personal representative with respect to protected health information relevant to such personal representation. **Example:** A son has durable power of attorney for health care for his father, and his father is currently incapacitated. The son may receive information that is relevant to his role as personal representative of his father.

Health information of minors (persons under 18 years of age):

A health care provider must treat a parent, guardian, or other person acting in loco parentis as the minor's personal representative, *except* in the following circumstances:

- The minor consents to the health care service; no other consent for the service is required by law, **and** the minor has not requested that such person be treated as the personal representative.
- The minor may lawfully obtain the health care service **without the consent** of a parent, guardian, or other person acting in loco parentis in the following situations in Ohio:
 - diagnosis and treatment of a venereal disease
 - diagnosis or treatment of substance abuse
 - examination or treatment for any problem resulting from sexual abuse or sexual offense
 - a 17-year old may consent for blood donation
 - testing for HIV
 - abortion (with Court approval)

- diagnosis or treatment of a mental health disease
- birth control (under Title X program –very limited conditions)

A parent, guardian, or other person acting in loco parentis assents to an agreement of confidentiality between a health care provider and the minor.

Questions about the status of minor persons and their health care services should be directed to Legal Services (Page 2001).

Deceased individual:

If an executor, administrator, or other person has authority under applicable law to act on behalf of a deceased individual or on behalf of the individual’s estate, treat him/her as a personal representative with respect to PHI relevant to such representation, and release the appropriate information.

Role of Personal Representative: Abuse, Neglect, Etc.:

A health provider may elect **not** to treat a person (such as a spouse or parent) as the patient’s personal representative, unless state or other law or regulation requires otherwise, if the provider has a reasonable belief that:

- The patient has been or may be subjected to domestic violence, abuse, or neglect by such person; or
- Treating such person as the personal representative could endanger the patient; and the health provider decides that it is not in the best interest of the patient to permit such person to be the personal representative.
- In this case, the provider would not disclose protected health information to this individual or individuals.

Key Points to Remember:

- If appropriate, provide the personal representative with information relevant to the representation.
- Keep in mind the best interest of the patient

Requests to Receive PHI in Alternate Ways or Locations:

Health care providers must permit individuals to request and must accommodate reasonable requests to receive communications about their health information by alternative means or at alternative locations.

Examples:

- A patient may ask that discussions about his/her health status be conducted in a room with the door shut.
- A patient may be concerned that her mother will answer the phone when the gynecology clinic calls with results of an STD test, so she asks the clinic to mail the results in a sealed envelope instead of calling.
- A patient asks a doctor not to use postcards to remind her about appointments.
- A patient asks that her doctor's office leave appointment reminder messages only on her cell phone, not her home or work phone.

A health provider may require the individual to make a request in writing. The provider may condition the accommodation on an alternate address or contact method, and information as to how payment will be handled. **However, a health provider may not require the patient to explain why the patient wants alternative means or locations for communications about PHI.** **Example:** An individual cannot simply state that the provider may not contact the patient at home about billing issues, without providing an alternative contact address. Individuals may not use this provision to avoid payment for services.

Key Points to Remember:

- Reasonable accommodations, when practicable.
- The provider must not ask for an explanation for the requests.

The HIPAA standards give physicians a good deal of latitude to make decisions about the patient's best interest regarding confidential communications.

- Health care providers must keep track of certain disclosures of PHI, and remember that patients have a right to know what is being done with their health information.
- Unless authorized in writing by the patient, Medical Center Development personnel may know only demographic information and dates of service, not diagnosis, medical history, health information about the family, or even that a patient is seeing a particular specialist.

Meg Johnson
 HIPAA Privacy Manager
 The Ohio State University Health Systems
 614-293-4477

Physician Module: Quiz One

1. **(True / False) There is no restriction on what information a covered entity may use or disclose to raise funds or solicit donations for development**
2. **(True / False) HIPAA is not important and does not apply to me.**
3. **Where can I obtain more information about HIPAA at OSU Health System?**
 - a. By calling the Health System's Privacy Office @293-4477
 - b. By sending an email to "Privacy Office" on GroupWise
 - c. By accessing the HIPAA Resource Page on Webster under Business/Staff Resources
 - d. All of the above
4. **(True / False) Protected Health Information (PHI) does NOT include the patient's phone number or e-mail address.**
5. **What kind of effort must a covered entity make to receive a signed acknowledgment from an individual indicating that he or she has received a Notice of Privacy Practices?**
 - a. Good Faith Effort
 - b. Half-Hearted Effort
 - c. Heroic Effort
 - d. No Effort
6. **(True / False) The HIPAA Privacy Rule only applies to information that is stored electronically.**
7. **(True / False) HIPAA replaces existing federal protections on health information.**
8. **One of the purposes of the HIPAA Privacy Rule is to:**
 - a. Put bad health care providers in jail.
 - b. Protect & enhance the rights of consumers to their health information and control the inappropriate use of the information.
 - c. Create barriers to effective patient care
 - d. Assist with the implementation of "The Lawyers Full Employment Act"
9. **Under the HIPAA Privacy Rule, one of the principles of the Rule is Security. Security of Health Information involves:**
 - a. Never disclosing information to anyone, ever.
 - b. Developing policies and procedures to ensure appropriate access to and safeguard health information.

- c. Permitting unfettered access to full PHI (Protected Health Information) to anyone who asks.

10. (True / False) Covered Entities must add confidentiality language in their contracts between themselves and an individual or company that provide services for the covered entity.

Physician Module: Quiz Two

1. (Yes/No) Carla Crabby, a patient of Dr. Q, recently reviewed her medical information and found what she believes to be an error. She wishes to amend her information. Dr. Q is offended and not only summarily denies the amendment, but also bans Ms. Crabby from her practice. Under HIPAA, is this appropriate?
2. What is the purpose of the Notice of Privacy Practices?
 - a. To inform patients of their rights and the covered entity's obligations to protect information under HIPAA.
 - b. To deplete the forests of the world.
 - c. To create an administrative nightmare.
 - d. To undermine the patient/doctor relationship.
3. (True/False) If a patient asks that his information not be disclosed for use in quality studies, the provider must agree not to use the information for that purpose.
4. At OSUMC, if a patient wishes to file a privacy-related HIPAA complaint or concern, where should the patient be directed?
 - a. To the circular file
 - b. To the moon
 - c. To the privacy office or to the Secretary for the U.S. Department of Health and Human Services
 - d. We don't need to tell individuals where they can complain to.
5. **When should passwords for computer systems be shared?**

- a. When I am extremely busy and need someone to access information for me.
 - b. When a co-worker needs information in a system that I have access to.
 - c. Never
- 6. Where should extra or unneeded copies of patient information be disposed of?**
- a. A recycle bin
 - b. A regular trash bin
 - c. In a patient shredder or locked patient bin
- 7. (True/False) In order to make individuals aware of their rights and the covered entity's obligations with respect to protected health information, it is sufficient to have the Notice of Privacy Practices posted in the office.**
- 8. (True/False) A provider may deny access to a patient's medical record.**
- 9. (True/False) Before agreeing to contact or provide information to a patient at an alternate address by a specified method, the provider is entitled to know why a patient does not wish for such communications to be sent to a patient's home.**
- 10. Dr. M is an extremely busy physician. Situation 1: Dr. M is so busy, she must zip from patient to patient, and her residents have to literally sprint to keep up with her. The residents are afraid that if they don't catch her in the hallway to discuss patients, they may never have an opportunity to do so otherwise. Situation 2: Dr. M is so busy that she also takes her inpatient charts home with her to work on. She doesn't bother contacting Medical Information Management-after all, it's her chart. Is this okay?**

- a. Situation 1 Yes, Situation 2 Yes
- b. Situation 1 No, Situation 2 No
- c. Situation 1 Yes, Situation 2 No
- d. Situation 1 No, Situation 2 Yes

Physician Module – Quiz Three

- 1. Of the choices below, what is the best method to send test results?**
 - a. By regular postcard
 - b. By letter or folded, sealed postcard
 - c. By voice mail
 - d. By e-mail
- 2. When faxing patient information, which of the following are essential to protect patient information?**
 - a. Use a fax cover sheet
 - b. Verify that the number you are faxing to is the correct number
 - c. Make sure that the information is retrieved from the fax machine properly
 - d. All of the above
- 3. Minimum necessary standard does not apply to:**
 - a. Uses and disclosures for payment purposes
 - b. Uses and disclosures for health care operations**
 - c. Uses and disclosures for treatment purposes**
 - d. Uses and disclosures for research purposes**
- 4. (True/False) The physician's name should be included on the appointment sign-in sheet.**
- 5. (True/False) HIPAA requires a covered entity to obtain consent for the use and disclosure of patient information for treatment, payment, and health care operations and may refuse to treat an individual because of failure to consent.**
- 6. (True/False) Patients should not be asked about medical problems or medical histories at the reception desk, in waiting rooms or in common areas.**
- 7. When must a provider give a patient a Notice of Privacy Practices?**
 - a. Never

- b. At the first service delivery after the compliance date (April 14, 2003), including telephone calls for treatment to the office.
 - c. Within three months after a patient is seen.
 - d. Each and every patient must be sent or given a Notice of Privacy Practices on April 14, 2003.
- 8. (True/False) An individual may revoke an authorization.**
- 9. When contacting a patient for an appointment reminder, it is best to:**
- a. Leave the reason for the visit on the patient's answering machine.
 - b. Get the patient's permission before leaving messages with family members or on voicemail.
 - c. Not contact the patient.
- 10. What information should not be included on an office sign-in sheet?**
- a. Name
 - b. Time of Appointment
 - c. Reason for visit/complaint

Physician Module – Quiz Four

- 1. (True/False) If HIPAA does not require that the covered entity give the individual an opportunity to agree or object, the disclosure need not be noted, recorded and included in an accounting of disclosures.**
- 2. When making a disclosure of PHI, what is the key concept to consider?**
- a. Best interest of the patient
 - b. Most expedient path
 - c. Most restrictive option
- 3. A signed authorization is required from the patient before disclosure for which of the following:**
- e. Marketing
 - f. Treatment
 - g. Inclusion in the Facility Directory
 - h. Report of child abuse to state agency as required by law
- 4. (True/False) An individual has no right to know about a report of adult abuse, neglect or domestic violence a health care provider made about him or her.**

5. **(True/False) An adult daughter brings her elderly father to an appointment, and comes into the treatment room with her father. She explains that she helps her father out with his medication and she comes to appointments to make sure of what each new medication or adjustment will be. In this situation, a provider must either obtain a signed authorization from the father before any discussion, or ask the daughter to leave the room to prevent a disclosure of health information to the daughter.**
6. **(True/False) A 25-year old male who was involved in an automobile accident is admitted to the hospital. He is unconscious. The covered entity is not permitted to contact his family or personal representative to inform them of his location or condition.**
7. **If a patient is unable to agree or object to his or her inclusion in the facility directory, the health care provider must:**
 - a. Assume the patient would want to be included in the directory.
 - b. Follow any known prior expressed preference of the patient and exercise professional judgment to determine whether inclusion is in the best interest of the individual.
 - c. Not list the patient in the directory.
8. **Requests for information about individuals in our facility should be directed to:**
 - a. The front desk and the facility directory
 - b. The patient care floor nurse
 - c. The attending physician
 - d. Anyone with access to e-results
9. **If a patient requests that the health provider only contact him by calling his cellular phone, the provider MAY NOT:**
 - a. Require the individual to explain the reason for the request
 - b. Require the individual to place his request in writing
 - c. Require the individual provide an alternate contact address for billing or payment
10. **PHI (protected health information) used or disclosed for all but the following must meet the "minimum necessary" standard":**
 - a. Payment
 - b. Fundraising
 - c. Research
 - d. Treatment