

SELF STUDY

THE HIPAA PRIVACY RULE

The requirements of the HIPAA Privacy Rule include informing you of OhioHealth's privacy practices and our commitment to protecting the privacy of the health information of our patients. The purpose of this information is to help you understand our privacy practices. It is also important that you understand your responsibility to help us ensure that we are doing everything possible to protect patient health information from unauthorized uses and disclosures.

WHAT IS HIPAA?

- The Health Insurance Portability and Accountability Act (HIPAA) was signed into law in 1996. At that time, most attention was paid to the provisions of HIPAA that deal with allowing us to keep our health insurance if we lose or change our jobs.
- The Administrative Simplification provisions of HIPAA are the ones we are concerned about here and they are the ones that have a significant impact on all health care providers. The three major components of the Administrative Simplification Provision are: the 1) Transaction Rule, 2) Security Rule, and 3) Privacy Rule.

THE ADMINISTRATIVE PROVISIONS OF HIPAA

1) The Transactions Rule (effective 10/16/03)

The goal of the Transactions Rule is to simplify and standardize how certain electronic transactions (such as billing) are conducted. With so much more health information being transmitted electronically, it is more vulnerable to wrongful use or disclosure. Therefore, there is a need for additional regulations to keep health information private and secure. In addition, by doing this, the health care industry is more efficient, uses technology more effectively and hopefully reduce costs.

2) The Security Rule (effective 4/21/05)

The Security Rule includes many requirements to ensure that health information is protected from accidental or intentional alteration, loss or destruction. The requirements of the

Security Rule apply to electronic health information, for example, on desktop or laptop computers, networks, CD-ROMS, and email transmitted over the Internet.

3) The Privacy Rule (effective 4/14/03)

The purpose of the Privacy Rule is to protect health information from being used or disclosed inappropriately. Before the Privacy Rule, it was up to individual States to protect a patient's privacy – some States did a good job, others did not. With the Privacy Rule, all health care consumers throughout the United States have a similar level of privacy protection. With the privacy rights required by the Privacy Rule, health care consumers have more control over how their health information is used and disclosed.

The remainder of this training will be about the privacy rule and your role in complying with this regulation and protecting OhioHealth patient's privacy rights.

THE PRIVACY RULES

- All “covered entities” are required to comply with the requirements of the Privacy Rule. A “covered entity” is any health care provider, health plan or health care clearinghouse that transmits health information electronically (for instance, submitting claims to Medicare).
- In order to meet the requirements of the Privacy Rule, all OhioHealth employees, volunteers, contract staff, students, and physicians-must understand his or her responsibilities with respect to patient health information.

WHY WE COMPLY WITH THE PRIVACY RULE

- The Privacy Rule is a Federal law. It is not an option to disobey this law. If we do not comply with its requirements we risk civil or criminal penalties.
- In addition, protecting patient privacy and ensuring that a patient's health information is safeguarded is the right thing to do. As health care consumers ourselves, it is assuring that all health care entities are required by the government to protect our health information.
- We require that all members of our workforce comply with our privacy practices. Failure to do so can result in appropriate disciplinary action.

PERSONAL HEALTH INFORMATION (PHI)

- The information that is protected by the Privacy Rule is called personal health information (PHI).
- The specific information that is protected is any information related to a patient's health condition (past, present and future) that could identify the patient. This is information that could identify the patient that is maintained in medical records, in computers, in conversations we have with each other, in reports, in billing records – everywhere throughout the agency.
- It is our job to protect our patient's health information from being used or disclosed in ways that are not allowed and that violate their privacy.

MORE ABOUT THE PRIVACY RULE

- The Privacy Rule explains ways that a patient's health information is allowed or required to be used or disclosed.
- To ensure that the requirements of the Privacy Rule do not hamper the provision of health care, a patient's health information is allowed to be used or disclosed for treatment, operations and payment (TOP).
 - 1) Treatment has to do with direct care, case management, care coordination, consultation with other health care providers, referrals and all that pertains to the provision of health care to the patient.
 - 2) Operations are the day-to-day activities needed to run the agency. This includes such things as performance improvement activities, risk management, fund raising, training, auditing, and strategic planning.
 - 3) Payment has to do with all matters related to obtaining or providing reimbursement for health care services provided to the patients.

HOW WILL OHIOHEALTH COMPLY WITH THE PRIVACY RULE

There are many things we do to comply with the requirements of the Privacy Rule.

- 1) The Notice of Privacy Practices

- Our Notice of Privacy Practices is the foundation of our privacy practices. It provides examples of how we use and disclose PHI for treatment, payment and operations and when we are required to disclose PHI to the government and law enforcement officials.
- It also informs patients of their privacy rights and what they must do to exercise them. The process for lodging a complaint regarding privacy violations is also described.
- We provide a copy of the Notice of Privacy Practices to all patients before we provide care to them (as do all OhioHealth entities). We are required to obtain a written acknowledgement from every patient that they have received a copy of our Notice of Privacy Practices. If we are unable to obtain the patient's written acknowledgement, we must document our efforts to do so and explain why we were not able to obtain it.

2) Privacy Officer

- OhioHealth designates a Privacy Officer who is responsible for matters related to privacy in organization.
- The Privacy Officer is responsible for ensuring that policies and procedures related to our privacy practices are followed.
- The Privacy Officer receives and follows up on any complaints related to privacy violations.
- If you have questions or concerns about patient privacy or any violations that you witness, please contact the Privacy Officer immediately. The OhioHealth Corporate Privacy Officer can be reached at the Ethics and Compliance Office at 566-5350

3) Policies and Procedures

We have policies and procedures that describe our privacy practices and how we comply with the Privacy Rule. The privacy policies and procedures are available for reference whenever you have a question or want more information about any of our privacy practices.

4) Business Associate Agreements

We ask our students, vendors and contractors, to sign agreements that require them to respect our privacy policies and procedures and protect our patients PHI.

Patient Rights under HIPAA

- The purpose of the Privacy rule is to give individuals more control over how their health information is used and disclosed. Patients are informed of their rights and

how to exercise them in our Notice of Privacy Practices. The Privacy Rule provides patients with specific rights with regard to their health information. We need to be aware of the patient privacy rights and what a patient needs to do to exercise them.

- If a patient asks you a question about their rights and you are not sure of the answer, contact a supervisor or the Privacy Officer to get the correct answer.
- The following is a list of the patient privacy rights as explained in the Notice of Privacy Practices.

1. RIGHT TO RECEIVE A COPY OF THE NOTICE OF PRIVACY PRACTICES

- All patients have the right to be informed about how their health information is used and disclosed. The Notice of Privacy Practices provides this information and all patients will receive a copy of it. It will also be posted at all OhioHealth patient service locations. The Privacy Rule requires that the patients acknowledge in writing that he or she has received it.
- The Notice of Privacy Practices includes how we may use and share PHI including for:
 - TOP (treatment, operation, payment)
 - Fundraising
 - Reminder Notices
 - Notifying of products and services
 - Workers compensation issues
 - Employer related reporting
- The Notice of Privacy Practices also outlines how a patient may opt out of certain disclosures, such as facility directories (such as used at our front desk), and notifies the patient that other disclosures require separate authorizations.

2. RIGHT TO REQUEST ACCESS TO HEALTH INFORMATION

- A patient may request access to his or her health information in order to inspect or copy it. There are very specific procedures that must be followed to review and grant or deny requests for access.
- If your job involves entering information in the patient's clinical record, remember that your documentation may be read by the

patient. As always, it is important to ensure clear, concise and accurate documentation.

3. RIGHT TO REQUEST AMENDMENT OF HEALTH INFORMATION

A patient may believe his or her medical records contain errors. If so, he or she may request to have the information corrected. There is a specific procedure that must be followed to review and grant or deny requests for amendment.

4. RIGHT TO REQUEST AN ACCOUNTING OF DISCLOSURES

- Patients may request an accounting of the disclosures of their health information. The accounting does not have to include disclosures made for treatment, operations, or payment (TOP) or disclosures the patient has authorized.
- Again, there are specific procedures that must be followed that are detailed in our policies and procedures.

5. RIGHT TO REQUEST RESTRICTIONS ON THE USES AND DISCLOSURES OF PHI

- The patient may request a specific limit on how their PHI is used or disclosed even though the Privacy Rule allows it. There is a formal process for requesting restrictions that must be followed and it is described in our policies and procedures.
- The agency may or may not agree to the patient's request, but, if we do, we must make sure that the agreed to restriction is followed.

6. RIGHT TO REQUEST CONFIDENTIAL COMMUNICATIONS

Patients may request that they receive communication from us in a manner or at a location that they designate. For example, a patient may prefer that their health information is discussed only when no one else is present. If a patient requests confidential communications, all staff that provide direct care must be aware of the request and honor it.

7. RIGHT TO LODGE A COMPLAINT

- The process for lodging complaints about our privacy practices is described in our Notice of Privacy Practices. Patients or their representatives have the right to lodge complaints about our privacy practices. The process for lodging complaints is outlined in our Notice of Privacy Practices.

- Staff and volunteers may (and should) make complaints to the Privacy Officer (without fear of retaliation) if they become aware of any potential privacy violations. It is everyone's responsibility to protect patient privacy and make sure we are meeting the requirements of the law.

THE MINIMUM NECESSARY STANDARD

Another piece of the Privacy Rule says we do not use, disclose or request more PHI than is absolutely necessary. We must limit the amount of PHI used by staff, volunteers, or others involved in a patient's care to the minimum amount necessary to perform his or her duties effectively.

HOW WE SAFEGUARD PERSONAL HEALTH INFORMATION (PHI)

- PHI is one of our most valuable assets – without it we could not function or provide care to our patients. We must do everything we can to protect it from loss or destruction. If we use or disclose PHI in ways that are not allowed by the Privacy Rule, we not only violate a patient's privacy, but we are also subject to fines and penalties.
- It is everyone's responsibility to ensure that every form of PHI – written, electronic and oral – is safeguarded.

Can you name areas where written PHI might be found?

Did you name?

- File cabinets
- Medical Records room
- Reports
- Travel charts
- Desks
- Whiteboards
- Trash/recycle bins
- Near shredders, fax machines, printers and copiers
- In staff mailboxes

Can you think of some ways that written PHI can be safeguarded?

Did you name?

- Lock travel charts/ laptops in your trunk when not using them.
- Promptly place PHI in the recycle box when it is no longer needed
- Don't leave PHI unattended on your desk or in your work area
- Lock file cabinets containing PHI when not in use
- Remove PHI from photocopiers, fax machines, and printers

Electronic PHI is particularly vulnerable to misuse, loss, destruction or accidental disclosure.

You can find electronic PHI:

- In desktop computers
- In laptops and PDAs
- Transmitted in faxes
- On CD-ROMS and diskettes
- On computer networks or intranets
- In transmissions over the internet

Can you think of some ways to safeguard PHI that is maintained electronically?

Did you say?

- Locate fax machines in secure areas
- Always use a fax coversheet that includes a confidentiality statement and instructions for misdirected faxes.
- Do not leave computer screens with PHI visible to the public
- Shut down your computer when you will not be using it
- Never share your computer password with others
- Do not include PHI in email transmissions
- Make sure the PHI on your laptop or PDA is password protected

Where is oral PHI?

- In conversations we have about patients
- When we talk on telephones or cell phones
- Phone messages at the office or left on answering machines

Can you think of ways to safeguard oral PHI?

- Do not talk about patients in public places or places that might be overheard by patients and families
- Do not talk about patients to anyone not involved in the patient's care
- Do not use phones in patient's homes to call or report on other patients

THE PRIVACY GOLDEN RULE

Do unto the PHI of others, as you would have them do unto yours.

By now you should be able to recognize PHI, respond by protecting PHI and request assistance if you don't know the correct response or feel a privacy violation has occurred. In conclusion, the Privacy Rule not only protects the privacy of the health information of our patients, but it also protects our own health information when we are in the position of needing care.

HIPAA PRIVACY POST-TEST

Student's Name: _____ Date: _____

1. The Transactions Rule, Security Rule and Privacy Rule are:
 - a. New components of the Medicare Conditions of Participation
 - b. Part of the Administrative Simplification provisions of the HIPPA legislation
 - c. Intended to ensure quality health care is provided to all patients
 - d. Concerned with reducing the health care benefits provided to patients
2. The HIPAA Privacy Rule:
 - a. Provides patients with more control over how their health information is used and disclosed
 - b. Provides a minimum level of privacy protection for all health care consumers
 - c. Requires that health care agencies develop systems and processes to ensure that patient's health information is safeguarded from wrongful use or disclosure
 - d. All of the above
3. Protected health information is:
 - a. Any information related to a patient's past, present or future physical or mental condition
 - b. Health information about an individual in any form
 - c. Health information that identifies the individual
 - d. All of the above
4. Name three forms of PHI protected by the Privacy Rule

5. My job with respect to protected health information requires me to:
 - a. Do everything I can to safeguard it from unauthorized uses and disclosures
 - b. Make sure I keep it hidden from other health care providers
 - c. Cover it up whenever I am working with it
 - d. Never let a patient know what I know about his or her health condition
6. The minimum necessary standard requires that:
 - a. I use the least amount of health information necessary to do my job effectively
 - b. Patients provide only the minimum amount of information, regarding their health status needed to treat them

- c. There are minimum standards for protecting patient privacy
- d. None of the above

7. Notice of Privacy Practices

- a. Gives details on how our organization uses and discloses the patient's health information
- b. Must be carried with me at all times in case someone has a question about our privacy practices
- c. Will probably change every few months

8. Where can I reach the person designated as Privacy Official for OhioHealth?

9. Patients are informed of their privacy rights and how to exercise them:

- a. Each time they have contact with anyone from the agency
- b. In the agency's Notice of Privacy Practices
- c. When they are upset with the care being provided to them
- d. All of the above

10. The agency's privacy policies and procedures:

- a. Reflect the information provided in the Notice of Privacy Practices
- b. Detail how the agency complies with the requirement of the Privacy Rule
- c. Are available to all staff members to refer to as needed
- d. All of the above

"I understand the policies as they relate to maintaining the privacy of our patients' individually identifiable health information as it applies to me and my job and I understand I am expected to comply with them.

I know it is my right and responsibility to seek guidance about privacy issues when I am uncertain about which actions to take and to report situations to management when I have reason to believe there is a violation of the policies."

Signature: _____

Date: _____