

SELF-STUDY PACKET FOR

HIPAA

(Health Insurance Portability & Accountability Act)
Compliance Training



Protecting Patient Privacy

What Everyone Should Know About HIPAA
(Health Insurance Portability and Accountability Act)

Sponsored by

| Duke University Health System | Duke University School of Medicine |
| Duke Private Diagnostic Clinic |

Copyright 2002 Duke University

How to Use this Self-Study Packet

The purpose of this self-study packet is to teach you about HIPAA and how it affects you in the workplace. Please review the materials contained in this packet. Then complete the case studies on pages 13 - 16 to test your knowledge of the material covered. Also, be sure to fill out the course evaluation and acknowledgment form and return these forms to the DUHS Compliance Office, DUMC Box 3162, to receive credit for completing the course.

Learning Objectives

In this course you will learn:

- The basics about HIPAA in the workplace
- What is “Protected Health Information”
- How HIPAA affects the workforce
- What can happen if someone breaks the HIPAA laws, and
- How to get help if you have a question about HIPAA.

What is HIPAA?

HIPAA stands for the Health Insurance Portability and Accountability Act. “**Portability**” protects our health coverage when we have job changes. “**Accountability**” requires health care institutions like ours to protect patient information. This part of the HIPAA law requires health care providers to follow certain rules to protect patient health information.

What is Protected Health Information?

When we speak of patient information, we're talking about what HIPAA calls, "Protected Health Information." Protected health information is any health information that could identify a particular person. The person could be living or deceased. The information could be about the past, present or future health of a person. The information could be written on paper, displayed or stored in computer, or it could be spoken. Examples include patient charts, reports, x-rays, billing systems, nursing notes, conversations about patients....even some kinds of trash.

What Makes Information Identifiable?



Identifiable Information

- ◆ Name
- ◆ Address
- ◆ Phone or fax number
- ◆ E-mail address
- ◆ Social security, medical record, certificate numbers
- ◆ Photos
- ◆ Voice, finger, retinal prints
- ◆ Date of Birth
- ◆ Employer
- ◆ Insurance account numbers

Certainly a name or an address could identify a person. A phone number, or social security number could also easily identify a person. Information that could be used with other information to learn someone's identity includes birth date, employer, and insurance or other account numbers. This is the kind of information we must all protect.

HIPAA Gives Patient's Rights

HIPAA came about because of the public's concern about how health care information is used. So HIPAA gives patients more control over their own health information. It provides patients with certain rights to protect their information, which include:

- Patients can get a statement about how we use their health information.
- Patients can ask for and, in most cases, get copies of their records.
- Patients can ask to have any mistakes in their records corrected.

To learn more about Patient Rights under HIPAA, go to hipaa.dukehealth.org

HIPAA Privacy Rules

HIPAA requires health care providers to follow certain rules to protect the privacy of protected health information. HIPAA also limits the use and the disclosure of patient information.

We “use” health information in our facility. We “disclose” or release health information when we give it to another entity to use.

“Use” = In the Institution “Disclosure” = Outside the Institution

Patients typically give approval for use or disclosure of their information by signing a written form. However, some disclosures are required by law, such as reporting gun shot wounds, and do not require patient permission.

Minimum Necessary

“Use” = In the Institution

HIPAA requires us to limit internal use of protected health information to the minimum necessary. Routine access will be limited by job functions. Non-routine access will be limited by policies and procedures. Because of this, you may soon find that you have less access to information than before HIPAA. Your access to patient information will be limited to only the information you need to do your job.

If it's not part of your job, it's not part of your business! If not involved in their care, NO ONE is allowed to look up any information on strangers, friends, family members, or even themselves!

“Disclosure” = Outside the Institution

When protected health information is given to other institutions, it should be limited to the minimum necessary. Only the information needed by the outside user should be given, unless the information is needed for treatment. And, when we ask others for information, we ask only for what we need and no more.

How does HIPAA affect you?

HIPAA affects EVERYONE. Whether you work directly with patients or not, you may find yourself in situations involving patient information.

For example: You happen to see a friend in a waiting room. You want to express your concern about whatever brings him to the clinic. Or, suppose you're cleaning a conference room, or you've walked in for the next meeting, and you find papers with patient information left on the table.

What do you do in these situations?

How Patient Information is Exchanged -

To know what to do in the situations above, you need to understand how patient information is exchanged:

- Spoken Information
- Information on Paper
- Information in Computers

Protecting Spoken Information

As you start to enjoy your lunch, you can hear two doctors at the next table talking about a patient. While you're not familiar with the terms they're using, you do pick up a few facts about who the patient might be. What do you do?

If you overhear co-workers talking in a public place, remind them that confidentiality is important. Public areas can be handy places to talk about work. But when it comes to patient health information, public places are not a good choice. Even if no names are used, identifiers such as age or marital status can reveal the patient's identity. Other people may be within earshot – people who just might know the patient being discussed. Find a private space if your job requires that you talk about patients.



Even if you don't work directly with patients, you might one day walk by a waiting room and see someone you know. He's not looking well, and he seems to be by himself. You want to express your concern and see if you can be of help. What do you do?

Respecting privacy doesn't mean you should ignore someone you know, but don't ask for personal health information. A patient might tell you about his illness, but you can't ask. And you can't repeat the information you hear. Unless you're involved in the patient's care, you don't have the right to ask for information or even to tell other people who our patients are.

Let's say you've entered a patient's room to explain an upcoming procedure. The patient has several visitors in the room who may or may not be family. What do you do?

Before entering a patient's room, you should first knock and ask if you may enter. If other people are in the room, ask the patient if it is okay to discuss their care with visitors present. Let the patient decide if other people can hear about the procedure.

Many of us are stopped in the hallway by patients and visitors to get directions. Under HIPAA law, what do you do?

If you can give directions without asking for personal information, you're being kind and respectful of the patient's right to privacy. If it's not clear where the patient is going, or if someone asks you about a patient, direct them to the information desk.

Protecting Spoken Information

Around patient rooms ...

- *Knock first and ask to enter*
- *Close doors or curtains when talking about treatments or doing procedures*
- *Speak softly in semi-private rooms*

In public areas ...

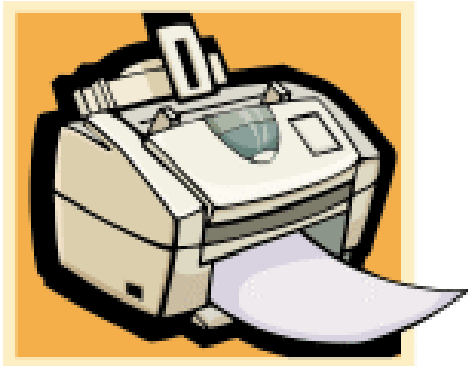
- *Don't talk about patients*
- *Direct visitors to the information desk*
- *Don't leave messages on answering machines about patient conditions*

Protecting Papers

Another way patient information is exchanged is on paper, such as patient charts, order forms, faxes, email print outs, O.R. schedules, clinic appointment schedules, etc.

Suppose you enter a conference room and find papers with patient information left on the table. What do you do?

Papers that have protected health information should be returned to the person who left them. If you can't find the owner of the papers, give them to your supervisor for shredding.



Suppose you work in an area where several people share a fax machine that is located in a public area. While you are in that area, you see a fax arrives with protected health information on it but no one comes to get it. Later that day, you notice the fax is still there. What do you do?

Tell your supervisor about the fax. If you share a fax or printer with others, it's your duty to pick up your papers right away. Don't leave any patient information or reports out in the open. Fax machines and printers are best located in a private area, away from public view.

Protecting Papers

- ◆ Find the owner of "lost" papers
- ◆ Shred information no longer needed
- ◆ Don't leave papers unattended
- ◆ Keep information away from public view

Information on Computers

A third way patient information can be exchanged is on a computer. Even if you don't work directly with patients, you may work with patient information on a computer.

- Keep computer screens pointed away from the public.
- Never walk away from a computer screen with patient information on it.
- Be sure to log off when you leave your computer.

Remember, your user name is used to track what you view in the computer system. Only you should use your user name and password. Anyone who needs to get to computer records should use his or her own user name and password.

Another way to protect patient information on a computer is to follow the rules about passwords. Never share your password or let someone else use your password to log into the computer system. Your password should be unique and secret.

Your password is yours alone!

- Don't share it with anyone.
- Never write it down.
- Create a strong password.
 - ◆ Use 6 characters with letters and numbers.
 - ◆ Do not use your name or other terms that can be easily guessed.

**To learn more about Password Security, go to
hipaa.dukehealth.org**

Protecting Information on Computer

- ◆ Keep computer screens pointed away from the public
- ◆ Never leave patient information in public areas unattended
- ◆ Log-off workstations when leaving the area
- ◆ Report computer errors
- ◆ Follow rules to protect your password
- ◆ Report computer viruses
- ◆ Protect handhelds and laptops

What Can Happen if You Break the Law?

Now that you know what you should be doing to protect patient information, let's look at what can happen if you don't.

There are levels of disciplinary action that can be taken. For example, a careless act, such as discussing patient information in a public area, could lead to counseling, but looking at a neighbor's medical record on purpose could lead to a final written warning. Using information for personal gain could lead to termination.

Discipline for DUHS Employees – 1st Offense

- » **For Carelessness - Counseling**
- » **For Intentional Misuse – Final Written Warning**
- » **For Personal Gain - Termination**

Repeat Offenses May Result in More Severe Discipline

There are also legal penalties for breaking the law. Penalties can be made against both an individual and the organization.

Legal Penalties:

- **Wrongful disclosures**
 - » Up to \$50,000 per violation + up to 1 year in prison
- **Gaining access to information by false pretenses**
 - » Up to \$100,000 per violation + up to 5 years in prison
- **Intent to sell, transfer, or use**
 - » Up to \$250,000 per violation + up to 10 years in prison

Don't take chances with your job or with the law.

How to Get Help

Knowing about HIPAA includes knowing where to go for help. As much as you need to follow the new rules, you must also take action if the rules are broken. Our patients expect it and deserve it.

We have Privacy and Security Officers and Directors for each facility in our organization.

You can report any problems directly to them or to your supervisor.

As part of your job, you should report when you think the privacy or security rules have been broken. **No one will be punished for reporting problems or asking for help.**

PRIVACY AND SECURITY OFFICERS & DIRECTORS

	Privacy	Security
Duke University Health System	Britt Crewse 668-2573	David Kirby 286-6567
Duke University Hospital	Barbara Woolley 684-2615	Terry Mears 286-6336
Durham Regional Hospital	Kathy Thomas 668-2119	Sandy Triplett 470-4182
Raleigh Community Hospital	Cindy Nordlund 954-3123	Kim Abbott 954-3718
Duke University Affiliated Physicians	Lisa Sutphin 416-8108	Julie McCauley 416-8107
Private Diagnostic Clinics	Guy Decarlucchi 668-5190	Tammy Clay 668-5161
Patient Revenue Management Organization	Roman Perun 620-5103	Roman Perun 620-5103
School of Medicine/School of Nursing	Juli Tenney 668-0679	John Williams 684-1883
Duke Health Community Care	Laverne Mullin 620-3853	Laverne Mullin 620-3853
Davis Ambulatory Surgical Center	Sally Walters 470-1008	Sally Walters 470-1008

If you don't want to make a report in person, you may call the toll-free Compliance Integrity Line.

**Compliance Integrity Line:
1-800-826-8109**

Don't delay!

And if possible, take action to prevent problems from happening. For example, in the clinic, a list of patients can be moved to an area away from public view. Or, charts stored in a public area can be moved to a more private area.

It's not always clear whether HIPAA applies or what the best way to handle a situation is. HIPAA was never meant to hinder patient care, but if questions come up or you don't know what to do, be sure to get an answer from someone who knows.

- ◆ **Ask your supervisor or the Privacy or Security Officer, Director or Manager in your work area.**
- ◆ **When in doubt, ASK!**
- ◆ **No one will be punished for reporting or asking for help.**

Remember These Key Points!

- ◆ Patients have a ***right to privacy***.
- ◆ If you are not involved in ***treatment, payment or facility operations***, patient information is NOT your business.
- ◆ ***You are responsible*** for information you see or hear.
- ◆ You ***may lose your job*** and be charged with a ***felony*** if you break the HIPAA Rules.
- ◆ ***Ask for help.***

HIPAA QUIZ

Circle the correct answer.

1. Dr. Jones, head of surgery, asks to see Kristi Smith's chart. Dr. Jones is not Kristi's physician but Kristi is his wife's best friend and he wants to see how she is doing. What do you do?
 - a. Give Dr. Jones the chart
 - b. Ask Dr. Jones for the appropriate authorization to review Kristi's chart.
 - c. Tell Dr. Jones that he cannot see the chart since he is not the patient's physician.
 - d. Tell Dr. Jones you are too busy to get the chart.

2. You enter a conference room for a meeting and notice that several reports with patient information are on the table. What do you do?
 - a. Throw the reports in the trash.
 - b. Leave the reports where you found them.
 - c. Notify housekeeping to come clean the room
 - d. If you can determine who left the reports, return the reports to them. Otherwise, give the reports to your supervisor for shredding.

3. Coach K is a patient at the facility where you work. Your friends want you to check his medical record to be sure he is doing okay after his recent surgery. Your job gives you access to everyone's patient records. What should you do?
 - a. Look at his medical record but don't share any of the information with your friends.
 - b. Look at the chart and share with your friends only information that is public knowledge.
 - c. Explain to your friends that no one in health care should look at patient records unless it is a job requirement.
 - d. Make copies of the medical record for your friends.

4. In the situation above, Jane, a nurse who is not involved in Coach K's care, looks at Coach K's medical record to see how he is doing. This is the first time Jane has inappropriately accessed someone's record. What could be the consequences for Jane?
 - a. Nothing will happen to Jane.
 - b. Jane will receive counseling for accidentally looking at Coach K's medical record.
 - c. Jane will receive a final written warning and could face fines for intentionally accessing Coach K's medical record
 - d. Jane will be terminated because she is a bad employee.

5. You notice that someone has left a computer terminal used to enter orders while still logged on to the system. You leave it as is, thinking the person will return shortly. Later, a patient looks at what has been entered on the screen. Who is responsible for this breach of privacy?
 - a. You. You should have protected the information from being disclosed.
 - b. The person who left the terminal while still logged on.
 - c. The hospital is responsible
 - d. All of the above.

6. Dr. Avery and Nurse West are discussing a patient's care outside the patient's room. The patient's neighbor, who has come to visit the patient, hears the discussion between the doctor and the nurse. Have the doctor and nurse violated hospital policy?
 - a. No. The patient should not have been eavesdropping.
 - b. No. Hospital policy allows health care providers to discuss patient care anywhere they need to.
 - c. Yes. Discussions regarding patient care should only be held in private rooms where anyone not involved in the patient's care can overhear.
 - d. Maybe. It depends on whether the health care providers could find a place that provides greater privacy.

7. You see a member of your church being brought in by EMS to the emergency department after a car crash. She appears to be unconscious. The charge nurse is calling the surgeon on call to arrange for surgery. What should you do?
 - a. Call the patient's spouse to let him know his wife is about to be taken to surgery.
 - b. Notify the church pastor to start the prayer chain.
 - c. Let the charge nurse know that you know the patient and can assist in locating her husband.
 - d. Go back to your job.

8. You overhear a fellow employee telling someone over the phone about one of the patient's in your area. You believe the other person on the phone is the employee's sister. What do you do?
 - a. Confront the employee and remind him of the rules regarding privacy and confidentiality.
 - b. Report your suspicions to your supervisor or the privacy director of your facility.
 - c. Tell the patient about what you overheard.
 - d. a and b.

9. James Rose, a patient in your care, has had an bad reaction to his medications. You try to reach Dr. Jones, his physician, for instructions. You find out that the doctor is at his health club. You call there and get the receptionist. What should you do?
- Tell the receptionist to tell Dr. Jones that Mr. Rose has had an adverse reaction and to call you back immediately.
 - Have the receptionist page Dr. Jones to the phone.
 - Tell the receptionist to tell Dr. Jones to call you back immediately.
 - b or c.
10. You are logging into your computer first thing Monday morning. You enter your password but get a message that your log-in failed. You try again and it doesn't work. You are positive that you are using the correct password. What do you do?
- Notify the Help Desk or your computer support of your problem so that they can research the problem.
 - Since you can't work on your computer, take this opportunity to clear out your inbox.
 - Ask your coworker, Susie, to let you use her logon ID and password.
 - Find a computer that someone else is already logged into and work from that computer.

HIPAA CASE STUDIES ANSWERS

Grade yourself.

1. **b** – Always get permission from the patient or patient’s representative before disclosing patient health information to anyone who doesn’t have a need to know that information.
2. **d** – Your actions will protect the information
3. **c** – Those working in health care should only look at information needed to perform their jobs unless patients give them permission to review their medical records.
4. **c** – For accessing Coach K’s medical record on purpose when it is not required by her job, Jane will receive a final written warning and could be subject to possible fines if Coach K seeks legal remedy for the inappropriate access.
5. **d** – Maintaining privacy is everyone’s job.
6. **d** - Dr. Avery and Nurse West should make every reasonable effort to find a private place to discuss the patient’s case.
7. **c** – Your friend has a right to privacy and may not want to notify her family of the accident. If she is able to, she will decide who should be notified.
8. **d** - If you feel comfortable discussing the matter with the employee, you should remind the employee of the privacy policies. You should also let your supervisor or the privacy director at your facility know so that appropriate steps can be taken to minimize the privacy breach.
9. **d** - If Dr. Jones can come to the phone, you can speak with him directly about the matter. Otherwise, you should simply request that the doctor be given a message to call back immediately regarding an urgent matter.
10. **a** – Contact the Help Desk or your computer support area so that they can determine why your password is not working. If they find that a possible security breach has occurred, they will reset your password immediately and notify your facility’s Security Director so that he/she can check whether your user name and password have been used to gain inappropriate access to patient information

**I acknowledge that I have completed the HIPAA
Compliance Self-Study Packet.**

Name: _____

Employee ID # _____

Social Security Number _____

Department _____

Organization _____

Please forward this sheet to:

SOM Compliance Office, 684-9700

**HIPAA FOCUS REVIEW EVALUATION FORM
SELF-STUDY**

"Protecting Patient Privacy – What Every Employee Should Know About HIPAA"

We would like your comments regarding the content & ease of understanding of the material presented. After reviewing the material, please respond to each question below.

A. How well did the training meet the following objectives?

	1	2	3	4	5
	Not at all	Slightly	Moderately	Mostly	Completely
Identify the two goals of HIPAA law					
Define "protected health information"					
Identify situations in which HIPAA affects employees					
State the consequences for breaking HIPAA laws					
State how to get help in reporting problems or answering questions					

B. Please rate this training experience on presentation and content:

	1=Poor	2=Below Average	3=Average	4=Above Average	5=Outstanding
Presentation (accuracy, tone, graphics)					
Content (organization, clarity, examples)					
Quiz (format, clarity of questions)					

C. What was the most important thing you learned?

D. What topics remain unclear?

E. Will you change your behavior in the workplace as a result of participating in this training? If yes, how?

F. Please list other patient information, privacy and security topics you would like to learn more about.

G. How satisfied were you with the following items:

	1=Not at all	2=Slightly	3=Moderately	4=Mostly	5=Completely
Convenience of self-study					
Scope of content presented					
Presentation style					

H. Length of this enduring material: **Too short** **Adequate** **Too long**

I. Please list any other suggestions you have for improving future training materials.