

HIPAA—What You Need to Know

HIPAA Privacy Rules

On April 14, 2003, the new **Privacy Rules** of the Federal Health Insurance Portability and Accountability Act of 1996 (“**HIPAA**”) go into effect. These rules ensure that any authorized person who is granted access to patient records and information protects holds such data in the **strictest confidence** and uses it only for the limited purpose for which they have been allowed to access it. The new **HIPAA Privacy Rules** apply to doctors, nurses, administrators, bill processors and anyone else who has access to the patient’s **PHI** (“**Protected Health Information**”), they extend to all PHI in any form, whether oral, recorded, written, electronic or in any other medium, and they apply to however that PHI is transmitted, orally, by mail or fax, or over the Internet or telephone. More importantly, the new law imposes strict penalties for anyone who improperly discloses or uses PHI or otherwise violates the Privacy Rules.

New Patient Rights

Under HIPAA patients have a right to:

- Receive a copy of the Notice of Privacy Rules and Practices of the healthcare provider. This informs the patient how their confidential information of PHI is handled.
- Receive a full accounting of all disclosures of their PHI outside of routine payment, treatment and health care operations.
- File complaints if confidentiality is breached or PHI is not handled appropriately.
- Request that PHI, such as bills or lab reports, be received at a location other than their home address.
- Request special handling of their PHI, i.e., certain information can never be shared with any outside party or organization.
- Read and obtain copies of their PHI at any time (with the exception of psychotherapy notes, information for a court of law and if the release of information would harm someone).
- Amend their PHI if they find they had an error.

What You Must Do to Protect Patient Rights to PHI

Some Guiding Principles:

1. PHI should be held in the strictest confidence and not disclosed to any unauthorized person unless the patient has authorized the disclosure or it is used by authorized persons in the care of the patient. PHI should also be used only for authorized purposes.
2. You must at all times comply with the Privacy Policies and Procedures or the HIPAA Privacy Rules of the Contracting Provider (hospital or other healthcare provider where you are assigned). Ask for a copy when you report for your assignment if they do not automatically hand you one.
3. If you are unsure of a situation, refer to the Facility Privacy Officer (“FPO”) or his/her designee.
4. When speaking with authorized persons communicate the “**Minimum Necessary**” PHI to do your job in a soft voice to minimize being heard.
5. When accessing patient data, using patient charts or using computers make certain that someone is not looking over your shoulder.
6. Follow the Contracting Provider’s Policies regarding the use of computers and never let anyone learn or use your password.
7. Never hand any document containing PHI to anyone if you do not know if they are authorized to see it. Make certain that documents containing PHI are placed in a safe area as designated by the Contracting Provider.



8. Access only the PHI that you have been expressly authorized to access and use. Do not assume that you have access to all of the PHI of the patient. You only have the right to access the **Minimum Necessary** to perform your job.
9. The Contracting Provider should have specific rules for the handling of PHI by authorized persons when it is used for “**Treatment, Payment and Operation**” or TPO.
10. Do not remove PHI from areas designated by the Contracting Provider.
11. Make certain you have signed the **Confidentiality Agreement**. If you have not, contact your consultant immediately.

Since the HIPAA Privacy Rules have become an integral part of healthcare delivery you should expect to hear references to the key HIPAA terms: “HIPAA”, “HIPAA Privacy Rules”, “Hospital Privacy Policy”, “Facility Privacy Officer”, “Notice of Privacy Practices”, “Protected Health Information”, “PHI”, “Minimum Necessary”, “Treatment, Payment and Operations”, and “TPO” wherever you are assigned. Now you know what they mean and how important they are.

Sample Common Situations

Phone Message to Patients

Ask the patient in advance if you can leave messages or confirm appointments. Only leave the date and time of your call on voice mail. Never leave any PHI in a message or share PHI with a third party.

Conversations

Speak softly and if possible, find a private place. You must not be overheard when speaking of PHI. Make sure to ask yourself: To whom am I speaking? If you do not know that the person with whom you are speaking has authority to learn anything about the patient, including their name and treating physicians, or to discuss the patient’s condition, refer them to the nurse’s station. “I’m sorry sir, but someone at the nurse’s station will be able to help you. If for some reason someone is not there, let me know, and I will hunt them down for you.”

Using the Phone, Fax & Email

Make certain that you dialed the correct number or sent your message to the correct address.

Unauthorized Files

If someone hands you a document and you are not sure that you should have it, rather than looking through it, take it to the nurse’s station and seek guidance. You do not want to see a file that should not be in your hands and you do not want to be observed doing it.

Patients and Their Families Know Their Rights

If patients believe their privacy rights have been violated, they can contact the Contracting Provider’s designated HIPAA or Privacy Officer.

Reporting Violations

If you see anyone violating the Contracting Provider’s Privacy Policies and Procedures, sharing confidential PHI with an unauthorized person, or misusing or destroying PHI, report it immediately to the designated person for the Contracting Provider and to your Foundation Medical Staffing representative.



HIPAA Confidentiality Agreement

Employee Name & Classification

By signing below, I agree that, as a healthcare professional and as required by HIPAA, I will hold in strictest confidence any and all Personal Health Information (“PHI”) related to patients and their care that I may learn or have access to as part of my job duties. This applies to every Foundation Medical Staffing healthcare client, or Contracting Provider, where I may be assigned. I also understand that as my employer, Foundation Medical Staffing must have procedures in place for making certain that the company and all of its employees who may have access to PHI because of their job assignments understand the importance of protecting PHI and agree to protect its confidentiality as required by law and that I must sign this agreement under those procedures.

A. My Obligation Concerning PHI

1. Use and Disclosure of PHI

I agree to keep all PHI disclosed to me confidential, and not to use or disclose such PHI except as necessary to provide temporary staffing services to Contracting Providers. I agree that I will use such PHI only on the premises of the Contracting Provider unless expressly permitted in writing by the Contracting Provider to remove PHI from the premises.

2. Compliance with Privacy policies and Procedures

I agree to comply with the Privacy Policies and Procedures of any Contracting Provider at which I provide temporary staffing services.

3. Notification

I will notify Foundation Medical Staffing and Contracting Provider of any instances of which I become aware in which the confidentiality of PHI has been breached or the Privacy policies and Procedures of a Contracting Provider have been violated.

4. Questions

I will refer any questions I have about the handling of PHI to the Contracting Provider’s designated person or the charge nurse.

B. Effective Date

This agreement shall remain in effect for so long as I am employed by Foundation Medical Staffing to provide temporary services to Contracting Provider’s.

C. Effect of Breach

I understand that if I breach any provision of this agreement, I may be subject to discipline, including termination

Employee Signature

Date

Received by

Date



HIPAA & PATIENT CONFIDENTIALITY CERTIFICATION QUIZ

EMPLOYEE NAME: _____ SCORED BY: _____

1. Which one of the following statements is true regarding the HIPAA privacy rules?
 - A. They are new restrictions on using and disclosing Protected Health Information
 - B. They are the first comprehensive federal protection guidelines on privacy
 - C. They give patients greater access to and protection of PHI
 - D. All of the above
2. Protected Health Information includes all health information except PHI in oral form.
 - A. YES
 - B. NO
3. You should get prior approval before leaving a message to confirm an appointment on a patient's answering machine.
 - A. YES
 - B. NO
4. After getting approval to leave messages on a patient's answering machine, leaving the patient's lab results on the answering machine would be considered acceptable.
 - A. YES
 - B. NO
5. The transporter asks what the patient is here for. Your response should be:
 - A. She needs to go via wheelchair to ultrasound; any other information would be a violation of the patient's privacy
 - B. She's here for a pregnancy ultrasound
 - C. Jenny Smith is Joe from the lab's girlfriend and needs an ultrasound to find out when the baby is due
6. You see your neighbor walking down the hall at the hospital where you are working. The neighbor recognizes you and says hello. Is it okay to ask her/him, "What are you here for?"
 - A. YES
 - B. NO
7. What would be a reasonable action to take to protect patient privacy if you are talking with a patient about their care in a semi-private room, and the other bed in the room is occupied?
 - A. Close the curtain between the patients, stand/sit close to the patient and keep the volume of your voice low.
 - B. Get the other patient out of bed, take them from the room, return and talk to patient
 - C. Write out all the information and give it to the patient to read
 - D. Inform the other patient that you are about to discuss confidential information in the next bed and ask her/him not to listen to you conversation
8. Your co-worker asks you for your pass code to the computerized patient database because they forgot theirs. Is it okay to give them your code?
 - A. YES
 - B. NO
9. Your father-in-law just had lab work done and the results will not be available to him until his doctor's appointment in two days. Is it okay to access the lab results and give the results to him if they are not normal?
 - A. YES
 - B. NO
10. Failure to comply with HIPAA and Confidentiality Policies can result in disciplinary action including termination.
 - A. YES
 - B. NO