



HIPAA PRIVACY MANUAL

Guidance for Field Staff

Contents

Introduction	3
1. What is HIPAA?	4
2. Enforcement	5
3. Protected Health Information	5
4. Facility Policies	6
5. Protecting Confidentiality	6
6. Patient Records	7
7. Faxes and Email	8
8. Release of Information	8
9. Reporting a Breach of Privacy	9
10. First Assist Policy for Confidentiality Statements	10
11. Quick Review	11
Test Questions	13
Answer Sheet	15

Introduction

As a healthcare professional, you know that the client facilities served by First Assist have always upheld strict privacy and confidentiality policies regarding access to patient health information. It is First Assist policy that all employees must abide by all rules, regulations and policies of the facility to which they are assigned, including those relating to confidentiality of patient information and patient records. Many clients have recently revised their privacy policies to comply with new privacy rules adopted pursuant to the Health Insurance Portability and Accountability Act of 1996 ("HIPAA").

As healthcare providers covered under HIPAA, the facilities to which you might be assigned by First Assist must provide you with appropriate training and orientation so that you can incorporate their privacy policies and procedures into your job role. However, it is also important for First Assist clients to know that you have some general knowledge of the HIPAA privacy rules.

To that end, First Assist has developed this manual to help our field staff understand the requirements for confidentiality and privacy under HIPAA. It gives guidance about workplace practices that may affect privacy and confidentiality, includes examples to illustrate potential situations in which privacy and confidentiality may be breached and contains a short test for you to complete and return to First Assist.

The potential consequences of noncompliance with client privacy policies and HIPAA can be serious and include termination of an assignment, termination of your employment with First Assist, civil penalties for the client, restrictions on your license to practice and even criminal penalties. Patient privacy is now more than an ethical obligation, it is also a legal obligation. It is therefore very important that you understand the HIPAA privacy rules and are familiar with the privacy policies of the client to which you are assigned.

1 What is HIPAA?

HIPAA stands for the Health Insurance Portability and Accountability Act of 1996. It covers three areas:

- Portability – ensuring continuity of coverage when moving from one health plan to another
- Accountability – expanding the government’s fraud enforcement authority
- Privacy and Security – protecting patient privacy and the confidentiality of protected health information

Under the third component, new privacy rules have been established to protect an individual’s medical records and other personal health information. These rules are the focus of this Manual.

Privacy Rules

In brief, the HIPAA privacy rules:

- Give patients more control over their health information
- Set boundaries for the use and release of medical records
- Establish appropriate safeguards that health care providers must put in place to protect the confidentiality of protected health information
- Enable patients to find out how their information may be used, and about certain disclosures of their information that have been made
- Generally limit release of information to the minimum reasonably needed for the purpose of the disclosure
- Give patients the right to examine and obtain a copy of their own health records and request corrections

Under the HIPAA privacy rules, a “covered entity” may not use or disclose individually identifiable health information except:

- as authorized by the individual who is the subject of the information;
- for treatment, payment and health care operations; or
- as otherwise permitted by the regulations.

A “covered entity” includes hospitals and other health care providers, health plans and health care clearinghouses (such as billing services). Essentially, HIPAA covers those who provide, bill or pay for medical care or process health information.

Generally, therefore, patient authorization is required for the disclosure of health information for purposes other than treatment and payment. The kind of information that is protected is described below. However, not all health information is treated exactly the same way under HIPAA. For example, psychotherapy notes are subject to stronger privacy protection. Treatment notes created by a mental health professional cannot be disclosed without individual authorization, even for purposes of treatment or payment.

The privacy rules apply to everyone working at a health care provider facility – including First Assist staff assigned to a client facility - who uses, accesses or interacts with patient information or patients in any way.

2 Enforcement

The Office for Civil Rights, in the Department of Health and Human Services, enforces the HIPAA privacy rules.

Breach of patient privacy can lead to civil and criminal penalties. Civil penalties are fines of up to \$100 for each violation of a requirement per individual. For instance, if a hospital released patient records, it could be fined \$100 for each record, up to a maximum of \$25,000.

Criminal penalties for “wrongful” disclosure can include not only large fines, but also jail time. The criminal penalties increase with the seriousness of the offense. For example:

- Knowingly releasing patient information can result in a one-year jail sentence and \$50,000 fine
- Gaining access to health information under false pretenses can result in a five-year jail sentence and a \$100,000 fine
- Releasing patient information with harmful intent or selling the information can lead to a 10-year jail sentence and a \$250,000 fine

3 Protected Health Information

Under HIPAA, the health information that is covered is called protected health information or PHI. PHI is any information that identifies an individual and meets one of the following definitions:

- It is created or received by a health care provider, health plan, employer, or health care clearinghouse,
- It relates to the past, present, or future physical or mental health or condition of an individual, or
- It describes the past, present, or future payment for the provision of health care to an individual

Such information may be on paper, electronic or verbal. In other words, all forms of information are confidential and must be protected! This could include: medical records, charts, handwritten notes, notes on report sheets, patient schedule forms and phone calls.

Examples of information that might identify someone include:

- Name
- Address
- Employer
- Relatives' names
- Date of birth
- Telephone and fax numbers

- E-mail address
- Identifying numbers such as social security number, medical record number, account number etc.
- Any other information that could be used to identify the patient

This information can only be used for permissible purposes and access to it must be limited to only those individuals who need the information for a legitimate purpose.

4 Facility Policies

The facility to which you are assigned should have policies in place to protect PHI. The policies that you need to know will depend on your role and the facility must educate you about the policies that will apply to you. Such policies might include:

- Defining who has access to PHI
- Listing the types of authorized disclosures and the procedure for releasing information
- When information may be released and how that release is documented
- Computer access

It is important for all First Assist staff to be familiar with the policies of the facility at which they are working. Be sure to read them carefully. If you have questions, see your supervisor or consult the designated privacy official at the client facility to which you are assigned.

Note that even though reasonable safeguards have been set up by the facility to prevent disclosures of PHI, sometimes an incidental disclosure occurs. A healthcare worker who makes an incidental disclosure will not be in violation of the privacy rules, provided the disclosure cannot reasonably be prevented, is limited in nature and occurs as a by-product of otherwise permitted use or disclosure.

For example: a patient in a doctor's office accidentally overhears part of a telephone conversation while walking down the hall (although note that it is important to take reasonable steps to safeguard conversations that may be overheard!).

Other types of disclosure will go beyond incidental and will be a violation of the privacy rules. For example:

- A doctor reviews a patient record and leaves it in the staff lounge to continue reviewing later
- A receptionist can be overheard in the waiting room while he/she converses with patients on the phone

5 Protecting Confidentiality

HIPAA introduces a new concept known as the "minimum necessary standard."

This means that healthcare providers must make reasonable efforts to disclose or use only the minimum necessary amount of protected health information they need to do

their jobs. This is the standard that guides healthcare facilities as they develop policies to protect patient privacy.

Note that the minimum necessary standard does not apply to sharing information for treatment. Clinical staff may look at the patient's entire record and share information freely with other clinicians directly caring for that patient.

Hospitals and other healthcare facilities therefore have to balance the need to protect patients' privacy and how much information needs to be disclosed to deliver quality care.

Even when providing care, however, there may be information you know or could find out that you don't need to share or discover to do your job. Ask yourself, "Do I or others need to know this to do our jobs?"

For example, if a patient is placed in an isolation room, you may become aware of why he or she is there, or may suspect you know why. This is confidential information about a patient and you should not communicate it to anyone else.

The orientation you receive from the facility to which you are assigned will normally include examples of the kind of confidentiality safeguards that have been put in place by the facility. For example, facility policy might require you to:

- Close patient room doors when discussing treatments and administering procedures
- Close curtains and speak softly in semi-private rooms when discussing treatments and administering procedures
- Avoid discussions about patients in elevators and cafeteria lines
- Not leave messages regarding patient conditions or test results on answering machines or with anyone other than the patient
- Avoid paging patients using information that could reveal their health issues

6 Patient Records

Your assignment facility should educate you about its policies regarding safeguarding patient records in your possession, both paper and electronic.

Here are some common sense examples of good practice:

- Do not leave records unattended in an area where others can see it
- When you are finished using paper patient information, return it to its appropriate location, i.e., the medical records department or a file at a nursing station
- When discarding paper patient information, make sure the information is shredded or locked in a secure bin to be destroyed later. Leaving paper patient information intact in a wastebasket could lead to a privacy breach. For example, records could spill out of the wastebasket or the paper information could blow out of a garbage truck into the street

If you have access to electronic medical records, further safeguards are required:

- Use screen savers to block patient information displayed on unattended computer monitors
- Log off the system before you walk away
- Point computer monitors so that visitors or people walking by cannot view information
- Do not keep your password written down. Never share passwords with anyone
- Change your password regularly according to the facility's policy

7 Faxes and Email

HIPAA does not prohibit faxing or emailing patient information specifically, but security mechanisms are necessary to protect the confidentiality of the information. Keep in mind that faxed patient information can easily fall into the wrong hands, which would be a violation of privacy. Before faxing any patient information, check to see if facility where you are working has a policy that limits its use.

If you do fax patient information, make sure you are faxing it to a dedicated fax machine in a secure location and make certain that the person the information is being faxed to actually receives the fax. If you know you will receive a fax that contains patient information, tell the person faxing the information to warn you ahead of time so that you can be present to receive it.

Do not let faxed patient information lie around a fax machine unattended. Immediately dispose of or file faxed information before others can see it.

Check with your supervisor to see whether the facility has a policy for sending and receiving e-mail. Be sure to familiarize yourself with this policy if you use e-mail in your job. This policy will likely cover both the procedure for transmitting PHI electronically and safeguards for the facility computer system (e.g. protection against viruses etc.).

Remember that work e-mail is not meant for personal use. Sharing or opening attached files from an unknown source can open the door to viruses and hackers. It's also important to remember that you can never be sure who will have access to your e-mail on the receiving end. So never send confidential information about a patient in an e-mail unless doing so is permitted under the facility's e-mail policy.

As with faxes, do not let printed e-mails lie around. Immediately dispose of printed e-mails after use or file them in the medical record, as appropriate.

8 Release of Information

The healthcare facility where you are working should have policies in place about the circumstances when PHI may be disclosed. Such policies will likely cover: disclosure for treatment purposes, disclosure for payment purposes, disclosure at the request of the patient or representative, disclosures required by law, disclosures for research, disclosures as part of a litigation process or disclosures of directory information. Make sure you are familiar with the policies that may apply to your job and, if you are ever uncertain about a disclosure, check with a supervisor.

For example: A patient you are caring for may have requested not to be listed in the hospital directory. A friend calls and asks to speak to the patient or for the patient's room number. You should check if the patient is listed. If not, you may not disclose that the patient is in the hospital. Instead say: "Thank you for asking, but we do not have any information on that person."

Note that giving information over the phone, in good faith, when you believe the disclosure is authorized, is OK. For example: A father calls and wishes to check the condition of his son. The patient has authorized that information may be provided to family members. You are not sure if this is the patient's father. However, you may give out the information over the phone. You are entitled to accept that the person calling is who they say they are.

There are exceptional cases in which providers are required to release information regardless of whether the patient agrees, and the law allows that.

The following list gives examples of circumstances in which an organization may release information:

- There are laws that require providers to report certain communicable diseases to state health agencies. The provider must report when patients have these diseases, even if the patient doesn't want the information reported
- The Food and Drug Administration requires providers to report certain information about medical devices that break or malfunction
- Some states require physicians and other caregivers who suspect child abuse or domestic violence to report it to the police
- Police have the right to request certain information about patients when conducting a criminal investigation
- Certain courts have the rights, in some cases, to order providers to release patient information
- Providers must report cases of suspicious deaths or certain injuries, such as gunshot wounds
- Providers report information about patients' deaths to coroners and funeral directors

Patients are usually informed when their health information is reported to police or others outside the facility, but they do not have the right to control their information in these cases.

The facility where you are working should have procedures in place to ensure it complies with the law and makes reports when necessary. Unless reporting this information is part of your job, you should not report it yourself. Check with your supervisor when you have questions about whether a report is necessary.

9 Reporting a Breach of Privacy

All of the client facilities to which you may be assigned should have designated a "Privacy Officer" who is normally the person designated to handle complaints.

If you think there has been a privacy breach, or that privacy violations may be occurring regularly in the organization where you are working, you must immediately notify First Assist and the facility Privacy Officer or other designated person at the facility. If you don't know who to contact at the facility, you should ask a First Assist representative for assistance, ask your supervisor or consult the organization's privacy policy.

Examples of the type of occurrences that you should report include:

- Sharing passwords
- Passwords left out in plain sight
- Someone is seen looking up patient information without a work reason to do so
- Patient records are left lying out exposed
- Someone removes patient records from the facility without authorization

You may also file a complaint with the Office for Civil Rights (OCR) in the U.S. Department of Health and Human Services if you suspect the facility is not complying with HIPAA. Patients and members of the public may do this too.

A complaint must be filed in writing (either on paper or electronically) within 180 days of the date the complainant knew about the violation of privacy.

The OCR has the authority to audit an organization's privacy practices for HIPAA compliance, and will likely do so by reviewing the organization's policies and procedures and interviewing staff.

10 First Assist Policy for Confidentiality Statements

First Assist requires every employee to sign a confidentiality statement, which may be provided to any client on request. The confidentiality statement is part of your employee agreement. In addition, you may be required by First Assist or the client to participate in additional training about HIPAA.

You may also be asked by the client facility to which you are assigned to sign an additional confidentiality and/or non-disclosure agreement confirming that you will abide by all rules, regulations and policies of the client regarding confidentiality and patient privacy under HIPAA.

It is important to remember that failure to maintain patient privacy may lead to termination of an assignment and termination of your employment by the Company, as well as further repercussions as designated by the applicable credentialing board and available at law. Also, your confidentiality obligations continue after the termination of your employment, regardless of the reason for termination.

11 Quick Review

Q. A technician updates a chart, leaves the chart on the nursing station desk and walks away. Is this a breach of the privacy rules?

A. Yes. The chart should be filed appropriately, not left out in plain view.

Q. A nurse calls a restaurant where a physician is having dinner and asks the hostess to have the doctor call the hospital about the pain medication for Mr. Jones. Is this an appropriate message?

A. No. The message contains patient identifying information. The correct message would have been to ask the doctor to call the hospital as soon as possible and ask for the nurse.

Q. Whiteboards are used to display patient name, diagnosis and room number. The boards are placed where the public cannot see them. You notice that the name of a well-known local celebrity is on the board. May you inform the local newspaper that he is in the hospital?

A. No. To do so would be a HIPAA violation.

Q. A doctor puts printed lab results that he/she no longer needs into the shredder. Is this the correct action to take?

A. Yes.

Q. It has been regular practice to leave the records system open and logged on at the nurses' station computer at the end of a shift. This saves time during shift changes for staff who need to retrieve records. Is this allowed under HIPAA?

A. No. It may be a timesaver, but this practice is not allowed. It is equivalent to sharing a password. Log off the system when you leave the station.

Q. A man tells you that he is here from JCAHO to perform an accreditation review. He wants your password to log on to the electronic medical record system. What should you do?

A. Ask the man to show you his JCAHO identification and find out who his contact is at the facility. The contact can take him to the appropriate area and give him the information he needs. If the man cannot tell you who his contact is, call your supervisor or the privacy officer.

Q. A patient calls your department and requests that their test results be faxed to a specialist. The patient gives you the fax number. The results are ready, but it's after hours. Should you fax the information?

A. Check if the facility has a policy on who may fax clinical reports. In any event, it is not good practice to send the fax to an unattended machine unless you know it is in a

locked room or has a locked cover. You have no way to ensure that someone besides the physician or his staff will not see the fax.

Q. A member of the Clergy calls to ask what room Joe Smith is in. How do you respond?

A. Check the patient's directory status. If the patient is in the directory and has not placed any restrictions on releasing this kind of information, you may inform the caller of the room number.

Q. You are a nurse in the emergency room. A child is brought in with suspicious bruises and other injuries. You suspect that the child is being abused, but her mother insists she is not and begs you not to report the incident. What should you do?

A. Check with your supervisor or the facility's privacy official to find out if state laws apply. That person can, if needed, check with legal counsel. If the state requires it, the case must be reported to the police. Making the report will most likely not be your responsibility – again, check with your supervisor.

Test Questions

1. **Which of the following is not addressed by HIPAA?**
 - a. Insurance portability
 - b. Hospital accreditation
 - c. Fraud enforcement
 - d. Administrative simplification

2. **Which organization has been charged with enforcing HIPAA's privacy regulation?**
 - a. The Joint Commission on Accreditation of Healthcare Organizations
 - b. The Office for Civil Rights
 - c. The Centers for Medicare and Medicaid Services
 - d. The Federal Bureau of Investigation

3. **What kind of personally identifiable health information is protected by HIPAA's privacy rule?**
 - a. Written
 - b. Electronic
 - c. Spoken
 - d. All of the above

4. **Authorization is required to release psychotherapy notes for any reason including treatment.**
True or False?

5. **Confidentiality protections cover not just a patient's health-related information, such as his or her diagnosis, but also other identifying information such as Social Security number and telephone number.**
True or False?

6. **The minimum necessary rule applies to all uses and disclosures including those for treatment.**
True or False?

7. **What does HIPAA say about faxing patient information?**
 - a. It can be done only among providers.
 - b. All patient information must be de-identified.
 - c. It is not allowed.
 - d. None of the above

8. **Which of the following are common features designed to protect confidentiality of health information contained in patient medical records?**
 - a. Locks on medical records room
 - b. Passwords to access computerized records
 - c. Rules that prohibit employees from looking at records unless they have a need to know
 - d. All of the above

9. **In which case is it acceptable for a hospital to release information without a patient's permission?**
- a. When the patient is under 16 years old
 - b. When the person requesting the information is a spouse, parent, or sibling
 - c. When a provider suspects child abuse and state laws require providers to report suspected abuse
 - d. None of the above
10. **When is the patient's authorization to release information required?**
- a. In most cases when patient information is going to be shared with anyone for reasons other than treatment, payment, or health care operations
 - b. Upon admission to a hospital
 - c. When patient information is to be shared among two or more clinicians
 - d. When patient information is used for billing a private insurer
11. **You are working at the hospital when you hear that a neighbor has just arrived in the ER for treatment after an accident. What should you do?**
- a. Contact the neighbor's spouse to alert him or her about the accident
 - b. Tell the charge nurse in the ER that you know how to reach the patient's spouse and offer the information if it's needed.
12. **If you suspect someone is violating the facility's privacy policy, what should you do?**
- a. Nothing
 - b. Watch the individual involved until you have gathered evidence against him or her
 - c. Report your suspicions to the facility's privacy or complaint officer, as required by facility policy
13. **You talk softly on the phone to a doctor in order to provide health information as required by your role. Visitors and patients walking past may overhear the conversation. This is an example of incidental disclosure.**
True or False?
14. **Casual conversation between nurses in the elevator about a patient is a HIPAA violation.**
True or False?

HIPAA MANUAL TEST

ANSWER SHEET

- | | | | |
|----|-------|-----|-------|
| 1. | _____ | 8. | _____ |
| 2. | _____ | 9. | _____ |
| 3. | _____ | 10. | _____ |
| 4. | _____ | 11. | _____ |
| 5. | _____ | 12. | _____ |
| 6. | _____ | 13. | _____ |
| 7. | _____ | 14. | _____ |

I have received a copy of the First Assist HIPAA Privacy Manual. To verify that I have read the material in the Manual, and that I understand it, I have personally completed the test at the end of the Manual and recorded my answers above. I agree to maintain the confidentiality of patient information in accordance with the guidelines contained in the Manual and the policies and procedures of each hospital or other facility where I am assigned.

Employee Signature

Date

Print Name

First Assist, Inc Staff

Score