An Introduction to Confidentiality and Privacy Under HIPAA
# Contents

1. Intended Audience 3

2. Overview: What is HIPAA 4  
   a. What is HIPAA and What Does it Govern 4  
   b. Enforcement 5  
   c. Why are Privacy and Confidentiality Important 6

3. Protecting Privacy 7  
   a. The Privacy Regulation 7

4. Confidential Information 8  
   a. What makes Information Identifiable 8  
   b. Case Scenario #1 8  
   c. Case Scenario #2 9  
   d. Case Scenario #3 9

5. Authorization 10  
   a. Psychotherapy Notes 10

6. Ways to Protect Confidentiality 10  
   a. The Minimum Necessary Standard 10  
   b. Ways to Protect Patient Privacy 11  
   c. Maintaining Records 12

7. Protecting Electronic Information 12  
   a. Ways to Protect Electronic Data 12  
   b. Passwords 13  
   c. Case Scenario #4 13  
   d. Case Scenario #5 13  
   e. Faxes 13  
   f. Case Scenario #6 14  
   g. E-mail 14

8. Exceptions to the Rule 16  
   a. When Reporting is Required 16  
   b. Case Scenario #7 17

9. Summary 17  
   a. Reporting Abuses 17

10. Answers to the Final Exam 18
An Introduction to Confidentiality and Privacy under HIPAA

1. Intended Audience:

- Nurses
- Nurse practitioners
- LVNs
- MAs
- Therapists
- Technicians
- Pharmacy staff

Intended for staff orientation and training, this booklet acquaints staff members with the requirements for confidentiality and privacy under HIPAA as well as the potential consequences of noncompliance. The booklet covers workplace practices that may affect privacy and confidentiality. Case scenarios illustrate potential situations in which privacy and confidentiality may be breached.
2. Overview: What is HIPAA?

2a. What is HIPAA and What Does it Govern?

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a multifaceted piece of legislation covering three areas:

- Insurance portability
- Fraud enforcement (accountability)
- Administrative simplification (reduction in health care costs)

The first two components of HIPAA, portability and accountability, have been put into effect.

**Portability** ensures that individuals moving from one health plan to another will have continuity of coverage and will not be denied coverage under pre-existing-condition clauses.

**Accountability** significantly increases the federal government’s fraud enforcement authority in many difference areas.

The third component, **Administrative simplification**, is arguably the most significant part of the legislation and is the focus of this booklet.

Administrative simplification received little attention when the law was first enacted because its implementation date was later than the other two components’. But today, two of its rules, privacy and security, are generating much discussion and debate in the health care community. The debate stems from the administrative, technical, and policy changes that the rules require health care organizations to make to protect their patients’ privacy and confidentiality of protected health information (PHI).

HIPAA’s privacy and security regulations punish individuals or organizations that fail to keep patient information confidential. Until these regulations were enacted, there was no federal framework to protect patient information from being exploited for personal gain. Now, the Office for civil Rights, in the Department of Health and Human Services, has been charged with enforcing the HIPAA privacy rule.
HIPAA states that “covered entities” must comply with its regulations. Covered entities for HIPAA’s privacy and security regulations include must providers, clearinghouses, and health plans.

2b. Enforcement

Breaking HIPAA’s privacy or security rules can mean either a civil or a criminal sanction. Civil penalties are fines of up to $100 for each violation of a requirement per individual. For instance, if the hospital released 100 patient records, it could be fined $100 for each record, for a total of $10,000. $25,000 is the annual limit for violating each identical requirement.

Have you ever looked up a coworker’s medical record to learn his or her birthday? Or read a neighbor’s medical history out of curiosity? Under HIPAA this could earn your organization a civil penalty and a fine.

Criminal penalties for “wrongful disclosure” can include not only large fines, but also jail time. The criminal penalties increase as the seriousness of the offense increases. For example, selling patient information is more serious than accidentally letting it be released, so it brings stiffer penalties.

“Egregious violations” such as the sale of a celebrity’s medical record information to a tabloid newspaper or the sale of health information to marketing or pharmaceutical companies for personal profit, could result in criminal penalties.

These penalties can be as high as fines of $250,000 or prison sentences of up to 10 years:

- Knowingly releasing patient information can result in a one-year jail sentence and $50,000 fine.
- Gaining access to health information under false pretences can result in a five-year jail sentence and $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.

Your facility is committed to protecting patient privacy and confidentiality. When you fail to protect patient information and patient records by not following your organization’s privacy policy. It can have an impact on your ability to do your job, your status with your organization, and your license to practice. You should carefully review your organization’s privacy policy and understand its requirements.
2c. Why are Privacy and Confidentiality Important?

Patients’ expectations of privacy and confidentiality are important to any hospital, physician practice, lab, nursing home, pharmacy, or other provider 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, HIPAA calls on covered entities to learn the rules for privacy and confidentiality and then live by them. Communications with or about patients involving patient health information should be private and limited to those who need the information for treatment, payment and health care operations. Health care operations are activities such as conducting medical record reviews, training health care professionals, and evaluation staff performance that don’t qualify as treatment or payment but are related to those functions and necessary for the organization operations. Only this with an authorized need to know will have access to the protected information. Hospitals and health care organizations have always upheld strict privacy and confidentiality policies. Unless you’re new to health care, this will be familiar to you.

But there are changes. The U.S. government has strengthened the laws protecting privacy and confidentiality in response to instance of private medical information getting into the wrong hands.

In North Carolina, an employer fired a good employee shortly after learning that the employee has tested positive for a genetic illness that could lead to lost work time and increase insurance costs.

In New York, a congresswoman who had battled depression found out her medical history was release to newspaper reporters.

Not surprisingly cases of misuse of health information have also caused lawsuits. A California woman sued a pharmacy that released her medical information to her husband, who used it to damage her reputation in a divorce. And in another divorce case, a woman threatened to use information about her husband’s health status that she obtained form his health record in custody hearing, forcing him to settle in order to avoid public discussion of his health.

A number of cases of misuse of health information rise, Congress has taken action to make hospitals and health care providers do more to protect health information privacy and confidentiality.
And with enactment of HIPAA, protecting patients right to privacy and confidentiality became more than just an ethical obligation of physicians and health care organization. It became the law.

3. Protecting Privacy

3a. The Privacy Regulation

The privacy component of HIPAA protects individually identifiable health information that is transmitted or maintained in any form by covered entities. The regulations were published in the Federal Register on December 28, 2000.

Individually identifiable information is any information including demographic information, that identifies an individual and meets any of the following criteria:

- Is created or received by a health care provider, health plan, employer, or health care clearing house
- Relates to the past, present, or future physical or mental health or condition of an individual
- Describes the past, present, or future payment for the provision of health care to an individual

It’s important to note that HIPAA’s privacy regulation is not limited to health information maintained or transmitted electronically, but covers information written on paper or spoken.

Which of the following situation describe proper techniques for protecting a patient’s privacy and confidentiality?

1. A doctor brings a patient into an unused room to discuss the patient’s medical condition.

2. A doctor who is reviewing a patient’s record leaves the folder in the doctor’s lounge to review later.

3. A doctor e-mails a physician friend about a patient’s condition. He explains the condition but omits any identifying information regarding the patient.

Answer: #1 and #3
4. Confidential Information

4a. What makes Information Identifiable?

Any information that might identify someone is called individually identifiable information under HIPAA. Elements that make information individually identifiable include the following:

- Names
- Addresses
- Employers
- Relatives’ names
- Date of birth
- Telephone and fax numbers
- E-mail addresses
- Social Security numbers
- Medical record numbers
- Member or account numbers
- Certificate numbers
- Voice prints
- Fingerprints
- Photos
- Codes
- Any other characteristics, such as occupation, which may identify the individual

Essentially, individually identifiable information is anything that can be used to identify a patient. Releasing any of this information for other than permissible purposes is a violation of the HIPAA privacy regulation.

4b. Case Scenario #1

Consider the example of a mail patient in the waiting room. He’s the only male in the room. His physician is discussing his condition—testicular cancer—with a nurse, and everyone in the waiting room can hear the conversation.

Question: What could have been done differently to protect this patient’s privacy?
Answer: The caregivers should have tried to find a private room or area where details could not be overheard. Even when the patient’s name is not specifically used in conversation, remember that details about his or her case or condition can be identifying factors in certain circumstances.

4c. Case Scenario #2

Mr. Olsen, a patient in the facility ahs had an adverse reaction to his medications. The nurse tries several times to reach the patient’s physician for instructions, with no success. Finally, she reaches the club where the physician is attending a social event. She asks the receptionist to tell the physician that Mr. Olsen has had an adverse reaction to his medications, and she urgently needs a call back.

Question: What should the nurse have done differently?

Answer: Leaving a message that provides any identifying details about the patient or his condition is a breach of confidentiality. If the person receiving the message knows Mr. Olsen, then information about his presence at the facility and his condition could lead to speculation about the patient. Whether in person, on the phone, or via voicemail or answering machine, never leave a message with a third party that contains health information about the patient. The nurse should have simply requested an immediate call back from the physician about an urgent patient matter.

4d. Case Scenario #3

Susan is a nurse in the ER of a city hospital, and she has just heard through the grapevine that a fellow nurse is pregnant. The other staff members would like to give this nurse a baby shower, but nobody knows when the baby is due or whether it is a boy or girl. Susan has access to the records and could easily find the answers to both the questions.

Question: Should Susan try to get information about the pregnancy and share it with the staff?
Answer: Absolutely not. This is clearly an unauthorized use of medical information. Remember that you should never look at the records of patients you are not helping to care for.

5. Authorization

5a. Psychotherapy Notes

Not all protected health information is treated the same under the privacy rule. Psychotherapy notes have much stronger protections because the personal notes of the treating psychotherapist can be damaging if they fall into the wrong hands. HIPAA requires individual authorization for the release of psychotherapy notes – even for treatment, payment and health care operations.

The final privacy rule defines psychotherapy notes in this way:

“Notes recorded (in the medium) by a healthcare provider who is mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint or family counseling session and that are separate from the rest of the individual’s medical record.

Psychotherapy notes excludes medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical test, and any summary of the following items: diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date.”

6. Ways to protect Confidentiality

6a. The Minimum Necessary Standard

Health care workers must make a reasonable effort to disclose or use only the minimum necessary amount of protected health information they need to do their jobs.

Making minimum necessary determinations is a balancing act. Providers must weigh the need to protect patients’ privacy against their reasonable ability to limit the information that is disclosed and deliver quality care.
Before looking at patient information staff should ask themselves, “Do I need to know this to do my job?”

However, there is no minimum necessary requirement when it comes to treatment. Clinical staffs are allowed to look at their patient’s entire record and share information freely with other clinicians directly caring for the patient.

There will also be occasions when you will have access to confidential information that you don’t need for your work.

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; do not communicate it to anyone else.

You may also see patient information on whiteboards throughout the facility. They are usually posted where the public cannot see them. In the course of providing patient care, you may work in areas where they are visible.

You must keep this information confidential. Do not disclose it to anyone, including coworkers, other patients, patient visitors, or anyone else who may ask.

In the course of doing your job, you may also find that patients speak to you about their condition. Although there’s nothing wrong with this, you must remember that they trust you to keep what they tell you confidential. Do not pass it on.

**6b. Ways to Protect Patient Privacy**

Here are some common sense ways nurses and other clinical staff members can protect patient privacy:

- 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.
- Do not leave messages regarding patient condition or test results on answering machines or with anyone other than the patient.
- Avoid paging patients using information that could reveal their health issues.
Preserving the right to privacy is essential to the organization’s mission, and it’s important to patients, many of whom will be uncomfortable in their strange surroundings.

6c. **Maintaining Records**

When patient information is in your possession, you are responsible for safeguarding it. Do not leave it unattended in an area where others can see it. This is especially important in public buildings, provider locations, and areas with heavy pedestrian traffic.

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 you are finished looking at electronic patient information, log off the system. Do not leave the information visible on an unattended computer monitor.

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 in a wastebasket could lead to a privacy breach. The wastebasket could get knocked over. The paper information could fall of a recycle truck and blow down the street.

Computer equipment must undergo special processing to remove all traces of patient information before being thrown away.

7. **Protecting electronic information**

7a. **Ways to Protect Electronic Data**

If you have access to electronic medical records, here are some ways to protect patient privacy:

- 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.
7b. **Passwords**

Do not keep your password written down. Never share passwords with anyone. Avoid guessable names for your passwords, such as your last name or the name of you child. Change your password regularly according to your facility’s policy.

7c. **Case Scenario #4**

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 that needs to retrieve records.

**Question:** Is this an allowable practice under HIPAA?

**Answer:** No. It may be a timesaver, but this practice is not allowed. It is equivalent to sharing a password. When many employees gain access to the system under the same password, there is no way to audit who sees records. Generally, you shouldn’t leave the system open when you leave the station.

7d. **Case Scenario #5**

A man tells you that he is here to work on the computers. He wants your password to log on to the electronic medical record system.

**Question:** What do you do?

**Answer:** The best response is to ask the man who at the organization contacted him. The contact can take him to the appropriate area and give him the information he needs. If the repairman cannot tell you who his contact is, call your supervisor or the privacy official.

7e. **Faxes**

HIPAA does not address faxing patient information specifically, but protects it under the privacy rule. 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 with your supervisor to see if your facility 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.

7f. Case Scenario #6

You are just coming off a double shift at the hospital, and a physician has asked you to fax her patient’s lab test results to her office fax. The results are ready, but it’s after hours in her office and none of her office staff are available to receive the fax.

Question: What do you do?

Answer: Don’t send the fax to an unattended machine unless you have been assured that 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. Talk with the incoming shift about handling the fax during office hours, and leave a message with the physician’s office asking them to call for a fax of the results that were requested.

7g. E-mail

HIPAA does not ban the use of e-mail for sending patient information, but security mechanisms are necessary to protect the confidentiality of the information.

Check with your supervisor to see whether your facility has a policy for sending and receiving e-mails. Be sure to familiarize yourself with this policy if you use e-mail in your job. This policy will protect both confidentiality of information and the computers from viruses that can harm them.

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 it is permitted under your hospital’s e-mail policy.

When you send e-mails, always double-check the address line just before sending the message to be sure that your e-mail doesn’t go the wrong person or list by mistake.

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.

**Helpful Hints to Use When Working with Computers**

- Review your organization’s policies on using computers.
- Do not use work e-mail for personal messages.
- Never share or open attached files from an unknown source.
- Never send confidential patient information in an e-mail unless your facility has a policy that allows it and mechanisms in place to protect the information.
- Always double-check the address line of an e-mail before you send it.
- Never share your password or log on to the system under someone else’s password.
- Always keep computer screens pointed away from the public.
- Never remove computer equipment, disks, or software from the facility unless you have permission.
8. Exceptions to the rule

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

The following list gives the 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 provider to release patient information.
- Providers must report cases of suspicious deaths or certain injuries, such as gunshot wounds.
- Providers report information about patient’s deaths to coroners and funeral directors.

8a. When Reporting is Required

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

The organization 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.

If you are interested in more information about what your state requires, you might find it useful to contact the department of public health, attorney general, or your organization’s privacy official.
8b. Case Scenario #7

You are a technician 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 no to report the incident.

**Question:** What should you do?

**Answer:** It’s important to know your own state laws in this case. Check with your supervisor or your organization’s privacy official, and that person can, if needed, checks with legal counsel or the attorney general. If you state requires it, you should report cases of suspected abuse to the police. You should ensure, however, that the information goes only to the authorities necessary under the law. This exceptional need to report does not provide an open door to share the patient’s information with others.

9. Summary

HIPAA requires organizations to have detailed policies and procedures in place that dictate how employees can use patient information, when they can disclose it, and how they should dispose of it. Be sure to read these carefully. If you have questions, see your supervisor or consult your organization’s privacy official.

9a. Reporting Abuses

If a patient, a member of the public, or an employee suspect your organization is not complying with HIPAA, he or she may file a complaint with the Office of Civil Rights (OCR) in the U.S. Department of Health and Human Services.

A complaint must be filed in writing (either on paper or electronically) within 180 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 your organization’s policies and procedures and interviewing staff.
All organizations must also designate an individual who handles complaints. This person may or may not be the organization’s privacy official.

You should feel free to contact this person if you think there are privacy violations occurring regularly in your organization. Ask your supervisor, or consult your organization’s privacy policy, to find out who handles complaints in your organization.
10. Answers to the Final Exam

1. b
2. c
3. b
4. b
5. d
6. true
7. d
8. d
9. c
10. a
11. b
12. true
13. c
14. true
15. false