

**HIPAA Training
Handbook for the
Healthcare Staff:**

*An Introduction to Confidentiality
And Privacy under HIPAA*

HIPAA Training Handbook

Contents

Intended audience:	5
Overview: Privacy and confidentiality	6
<i>Why are privacy and confidentiality important?</i>	6
<i>What is HIPAA?</i>	8
<i>Potential Consequences</i>	9
Protecting privacy	13
<i>Ways to protect patient privacy</i>	13
<i>Case scenario #1</i>	15
<i>Case scenario #2</i>	16
<i>Any questions?</i>	16
Confidential Information	18
<i>How is patient information used?</i>	19
<i>Who is authorized to see information?</i>	19
<i>Case scenario #3</i>	21
<i>Case scenario #4</i>	22
<i>Any questions?</i>	23
<i>Authorization</i>	24
<i>Helping patients understand their rights</i>	24
Typical ways to protect confidentiality	26
<i>Ways to protect patient confidentiality: Using records and other information</i>	26
<i>Case scenario #5</i>	27
<i>Case scenario #6</i>	27
<i>Case scenario #7</i>	28
<i>Any questions?</i>	28
Electronic confidentiality protections.....	29
<i>Methods for protecting electronic information</i>	29
Using e-mail on the job.....	29
Passwords.....	29
More steps for protecting electronic information	30
<i>Case scenario #8</i>	31
<i>Case scenario #9</i>	31
<i>Case scenario #10</i>	32

[Helpful hints to use when working with computers26](#)

Exceptions to the rules33

There are some exceptions to confidentiality.....33

Seven reasons for releasing confidential information.....34

Understanding your role.....35

Summary36

Summary of issues.....36

Reporting violations.....37

For the Healthcare Staff:

An Introduction to Confidentiality And Privacy under HIPAA

Intended audience:

- Clerical staff including medical records staff, patient accounting, and registration, back office staff, human resources, etc.
- Dietary services
- Nursing assistants
- Housekeeping/facilities staff
- Trainees/students and volunteers
- All other ancillary staff

Intended for general workforce orientation and training, this booklet will acquaint workers in the hospital, physician's office, patient registration area, lab, and other settings throughout the facility with the requirements for privacy and confidentiality under HIPAA as well as the potential consequences of noncompliance. Case scenarios will illustrate potential situations in which privacy and confidentiality may be breached.

Overview: Privacy and confidentiality

Why are privacy and confidentiality important?

No matter where you work in healthcare—the hospital, labs, radiology centers, nursing homes, doctors' offices, business units, IT or right in a patient's home—It's important to understand what privacy and confidentiality mean.

Patients have the right to control who will see their protected, identifiable health information. This means that communications with or about patients involving patient health information will be private and limited to those who need the information for treatment, payment, and healthcare operations. Such communications may involve verbal discussions, written communications, or electronic communications. Only those people with an authorized need to know will have access to the protected information.

Hospitals and healthcare organizations have always upheld strict privacy and confidentiality policies. Unless you're new to healthcare, this idea will be familiar to you. However, the U.S. government strengthened the laws protecting privacy and confidentiality in response to situations in which private medical information has ended up in the wrong hands.

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



In New York, a congresswoman who had battled depression found out her medical history was released 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. In another divorce case, a woman threatened to use information about her husband's health status that she obtained from his health records in custody hearings, forcing him to settle in order to avoid public discussion of his health.

As the number of cases of misuse of health information rises, Congress has taken action to ensure that hospitals and healthcare providers protect health information privacy and confidentiality.

With the enactment of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), a patient's right to have his or her health information kept private

and secure became more than just an ethical obligation of physicians and hospitals -- it became the law.

What is HIPAA?

HIPAA is a broad law dealing with a variety of issues. Its original goal was to make it easier for people to move from one health insurance plan to another as they change jobs or become unemployed. This also means they must be able to move their medical records and information easily, to get the care they need.



To make it easier for healthcare organizations to share medical information, the law requires that common transactions – such as submitting a claim on the patient’s behalf – be in standard format for all healthcare organizations and payers. But as patient information becomes easier to transmit, it also becomes easier for information leaks and abuses to happen. This is especially true as more and more information is shared electronically through e-mail and the Internet.

Before computerized records, it would have been difficult to remove many records and make use of the information. Today, with e-mail and electronic storage of information, in just a few minutes at a computer, thousands of records can be sent anywhere

Imagine you wanted to identify patients who had an expensive medical condition in order to discriminate against them. Using paper records, if you could get them, the task would take countless hours. But with a computer and standardized records, it's simple to sort out patients who have expensive illnesses and potentially use that information to hurt their chances at getting jobs or insurance. Standardizing and computerizing patient health information has important benefits, but it also brings risks.

As a result, an important part of HIPAA focuses on patient privacy and confidentiality. Under HIPAA, it is illegal to release health information in appropriate parties or to fail to adequately protect health information from release.

Potential Consequences

The U.S. Department of Health and Human Services (HSS) will enforce HIPAA. Breaking HIPAA's privacy or security rules can mean either a civil or criminal penalty.



Civil penalties are fines of up to \$100 for each violation of the laws per person, up to a limit of \$25,000 for each identical requirement or prohibition. For instance, if a hospital released 100 patient records illegally, it could be fined \$100 for each record, for

a total of \$10,000. If multiple violations are found, these fines could increase significantly.



Civil 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. In other words, selling patient information is more serious than accidentally letting it be released, so it brings stiffer penalties. These penalties can be as high as \$250,000 fine or a prison sentence of 10 years. For example:

- Knowingly releasing patient information in violation of HIPAA 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.

Your facility is committed to protecting patient privacy and confidentiality. When you fail to protect patient information and records by not following your organization's policies, it reflects on your ability to perform your job. To learn more

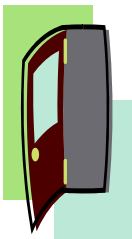
about the consequences of violating patient privacy and confidentiality, review your organizations' privacy policy.

Protecting privacy

Ways to protect patient privacy

Whether they are in the hospital, physician's office, lab, or other setting, patients receiving medical care expect privacy. They expect to be physically separated from strangers and employees when they consult or interact with their doctors and nurses, and they expect that their private health information will not be shared with people who don't have a need to know.

This organization is committed to giving patients privacy. As you work here, you will see many ways patient privacy is protected.



Patient care or discussion about patient care is kept private by closing room doors or drawing privacy curtains and conducting discussions so that others may not overhear them. Patient medical records are not left where others can see or gain access to them. Laboratory, radiology, and other ancillary test results are kept private.

Privacy is essential to the healthcare provider's mission, and it's important to patients – many of whom will be uncomfortable in strange surroundings. As you perform your job, you need to protect patient privacy.

When carrying out your job assignments and meeting deadlines, remember that you don't want to interfere with

patient privacy or jeopardize the confidentiality of patient information in the process.

Much of this is common sense. Knock on a door and ask to enter before entering a room. Keep patient records locked away and out of public areas. If you find records unattended, return them to the nursing supervisor.

If you need to page a patient, the page should not include information that can allow others to identify the patient's condition or reason for being there. Check your organization policy to understand how to handle this.

If visitors ask you for information about a patient, direct them to the information desk for assistance rather than giving out patient names or locations yourself. If you have access to the facility's directory, you should check it to ensure the patient has agreed to be listed before you disclose any information.

Patients expect privacy when they are receiving healthcare. It's up to everyone to see that their expectations are met by both respecting their privacy and not repeating any information that may detract from a patient's privacy.

Case scenario #1

You are called to work in a patient's room to perform a routine job assignment. You knock on the door and are invited in. You see that a nurse is in the room, discussing the patient's condition or medication

Q What should you do? Should you ask if it's OK to perform your job? Or should you come back later?

A If the Task is critical to patient care, ask if you can interrupt. Otherwise explain that you are there to perform a routine job and will return in 15 or 20 minutes. That protects the patients' privacy by allowing them to conduct their discussions without being overheard.

While some patients may say that it's OK for you to remain in the room during a consultation, remember that patients might not feel comfortable sharing complete information about symptoms while you are in the room. Some patients might not feel comfortable asking you to leave. Some nurses might even forget that you shouldn't be in the room while they are discussing treatment with a patient.

That's why good privacy practices require that you tell them you will return later to complete your work so that you don't interfere with the patient's care.

Case scenario #2

You are working in the emergency department when you see that a neighbor has just arrived for treatment after a car crash and you hear someone saying that he will be taken to surgery soon. Your neighbor's wife works in another part of the hospital.

Q **Should you notify the neighbor's wife that her husband has arrived in the emergency department?**

A No. The correct course of action is for you to tell the nursing staff that you know the patient and his wife, and let them know that if they need to locate her, you can help by providing information.

When patients are in the hospital they have the right to decide who should know they are there. Your neighbor has a right to privacy. Your neighbor may not want to notify his family of his accident. If he is conscious, the emergency department staff will allow him to decide who should be notified of his presence at the hospital.

If he is unconscious, the doctors and nurses will use their professional judgment about whether to notify his wife and will decide whether you, as a friend, should be involved in any way. Leaving the decision to the emergency department staff is essential.



Any questions?

For more discussion about your organization's privacy policies, refer to your employee handbook or organization policies. And, if a privacy issue arises and you are unsure what to do, consult your supervisor or your privacy official.

Which situation describes proper techniques for protecting a patient's privacy and confidentiality?

1. A dietitian brings a patient into an unused room to discuss the patient's medical condition.
2. A volunteer who is filing leaves a patient record on a table while taking a break

Answer: #1

Confidential Information



What is confidential information?

When patients give information to their providers, they expect that only people involved in their healthcare will see it.

Confidential information includes patient identity, address, age, Social Security number, and any other personal information that patients are asked to provide.

In addition, confidential information includes the reason a person is sick or in the hospital, the treatments and medications he or she may receive and other observations about his or her condition or past health conditions.

How is patient information used?

The hospital collects this information so that it can take care of patients and perform other related functions. However, the facility and its workforce can use it only in limited ways.

Obviously, doctors, nurses, therapists, dietitians, and other caregivers use information about patients to determine what services they should receive. In addition the billing department uses confidential information to bill patients or their insurance companies for the services they receive. Other physicians and quality control directors review confidential information to make sure patients are getting good care.

Other uses are, generally speaking, not allowed. It's helpful to ask yourself before looking at any patient information: Do I need this in order to do my job and provide good patient care? What is the least amount of information I need to do my job? This requirement to use or share only the "minimum" necessary is mandated by the HIPAA privacy rule.

Who is authorized to see information?

All members of the workforce at a hospital contribute to the quality of care. But that doesn't mean everyone needs to see health information about patients.

Many employees have no access to patient information either in the computer or on paper. That's because they don't need to know the information. That's an important phrase to remember: *Need to know*.

If you do not need to know confidential patient information to do your job, you will not be given access to it. That means that you should not look at medical records, either in the computer or on paper.

But there still be occasions when you will have access to confidential information. For example, if a patient is placed in an isolation room, you may learn why he or she is there, or you may suspect you know why. This is confidential information about a patient, and you should not share it with anyone else.



Another example of confidential information is the information about a patient's condition that you see written on whiteboards around the hospital. The information contained on these boards is used for giving care to patients. In general, it is recorded in places where

the public will not see it. But you may work in areas where this information is visible.

This information is confidential. That means you should not use it or share it with anyone, including coworkers, other patients, patient visitors, or anyone else who may ask you about it.

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 that information confidential, and you must not pass it on.

Case scenario #3

The newspaper has reported that someone famous has come to the hospital, and you're curious to know if this is true.

Q **Should you ask around or look for records about this person?**

A Obviously the answer is no. You are not allowed to satisfy your curiosity. If you look at patient records for any non-business reason, it is cause for dismissal and possible legal consequences. Remember that this rule applies not just to people without access to medical records, but to anyone.

If doctors or nurses look at confidential information about patients for non-treatment purposes, they can be fired or lose their privileges to work at the hospital. If doctor or

nurses share information about patients outside the hospital with people who do not have a right to know that information, they can be fired or lose their privileges to work at the hospital. Further, there may be legal consequences and their licenses may be in jeopardy.

It's important to realize that protecting confidential information is a responsibility that the entire workforce shares, including volunteers, regardless of whether they directly care for patients.

Case scenario #4

A friend is concerned because his girlfriend is in the hospital. He asks you to find out anything you can.



Should you try to find information for your friend?



Again, of course, the answer is no. You should direct your friend to the information desk, where he can learn the patient's location and general con-dition, if the patient has agreed to have her information in the directory.

Remember that you are not to seek out confidential patient information other than when required by your job. When it is made available to you, you are not to repeat it to anyone. Protecting patient confidentiality isn't just a hospital priority, it's the law.



Any questions?

Remember if you decide to violate these policies, you can be dismissed and prosecuted. Violating patient confidentiality is a crime.

For more information about how the hospital will respond to violations of this policy, consult your hospital's privacy policy.

Confidential Information Quiz

Circle the correct answer.

- 1. A patient's confidential information includes his or her**
 - a. Social Security number
 - b. Address
 - c. Age
 - d. Name
 - e. All of the above

- 2. Which of the following phrases should you keep in mind when determining whether you should have access to patient information?**
 - a. Disregard all patient information
 - b. Any information out in the open is public record
 - c. Need to know
 - d. All of the above

Answer: 1.e and 2.c



Authorization

In order to use or share health information for certain business-related purposes, such as releasing information to financial institutions that offer loans or selling mailing lists to marketing companies, organizations need to receive authorizations from patients. With an authorization – which must be in writing – the patient voluntarily agrees to let your organization use the information only for a particular request or need. Providers may not refuse to treat patients who won't sign authorization forms.

Authorization is also required to disclose psychotherapy notes, but it's not needed to disclose information about an organ donor, about a deceased patient, or for fundraising as long as the information is limited to individual demographics and dates of services and your organization or fund-raising arm is performing the fundraising.

Patients have the right to revoke their authorization at any time. They may also ask providers to restrict how their medical information is used to carry out treatment, payment, and healthcare operations, but providers are not required to agree to the restrictions.

NOTICE

Helping patients understand their rights

It's important that patients understand how they can protect their own health information and

how providers protect their information. That's why the HIPAA rule also requires healthcare providers to post notices telling patients how their information will usually be used.

This notice of privacy practices tells patients about the provider's privacy policies and practices and ways the provider will use their information. It also tells patients about their rights, including the right to access their own records and request amendments to them. HIPAA requires providers to make "good faith efforts" to obtain patients' written acknowledgement that they received a copy of the notice of privacy practices.

You will also see these information notices posted in places where patients can see them. If patients have questions about how the organization uses information you can direct them to these posted notices, or to the organization's privacy official for answers.

Testing your understanding

3. The notice of privacy practices explains the ways the organization will use patient information and tells patients about their rights regarding the information. True or false?
4. A patient can be denied treatment if he or she hasn't signed an authorization form. True or false?

Answer: #1 True, #2 False

Typical ways to protect confidentiality

Ways to protect patient confidentiality: Using records and other information

Your organization uses many tools to protect confidentiality.

- Records are kept locked and only people with a need to see information about patients have access to them.
- Employees who use computerized patient records to not leave their computers logged in to the patient information system while they are not at their workstations. Computer screens containing patient information are turned away from the view of the public or people passing by.
- Posted or written patient information maintained in work areas such as nurses' stations is kept covered from the public.
- Discussions about patient care are kept private to reduce the likelihood that those who do not need to know will overhear.
- Electronic records are kept secure, and the facility monitors who gains access to records to ensure that they are being used appropriately.

- Paper records are always shredded or placed in closed receptacles for delivery to a company that destroys records for the facility. They must never be left in the garbage.

All of these are basic ways the organization protects confidentiality. But truly protecting confidentiality depends upon you. You must not share information that you overhear or see in the course of your work. Doing so is a violation of the law.

Case scenario #5

You are walking by a trash can and notice that a pile of photocopied records has been laid on top of the trash.

Q How should you handle this? Should you put the records in the shredder or secure disposal container?

A The best response is to gather the records and take them to your supervisor. He or she will want to report this to the facility's privacy official so that the facility can try to find out why the records were disposed of improperly.

Case scenario #6

While you are entering a room containing records during off-hours, you find that the door is unlocked.

Q Should you lock the door? How should you respond?

A The best response is, again, is to contact your supervisor or the security department staff and notify

them of the unlocked door. They will want to follow up with the privacy official to find out why it was left unlocked.

Case scenario #7

You are approached by an individual who tells you that he is here to work on the computers and wants you to open a door for him or point the way to a workstation.



How do you respond to this request?



The best response is to ask this person who his or her contact is at the facility. Often, this is the information services director or the facilities manager. That individual can take the repairperson to the appropriate work area. If the repairperson cannot tell you who his point of contact is, contact security or your supervisor to assist the repair person in finding the contact.



Any questions?

Even if you do not use medical records as part of your job, by being on the lookout for potential violations of privacy, you help the facility keep its commitment to patient confidentiality.

You should feel comfortable going to your supervisor or your organization's privacy official with any questions about how to respond in situations in which privacy or confidentiality seem to be at risk.

Electronic confidentiality protections

Methods for protecting electronic information

Because so much information can be obtained so quickly in electronic format, special attention is paid to computerized patient health information.

Using e-mail on the job



Your organization has developed policies about the use of e-mail. Be sure to familiarize yourself with them if you use e-mail in your job. These policies will protect both confidentiality of information and the computers from viruses that can harm it.

Remember that work e-mail accounts are 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. Never send confidential information about a patient in an e-mail over a public network unless it is encrypted. When you send e-mails, always double-check the address line just before sending the message. Be sure that your email doesn't go to the wrong person or list by mistake!

Passwords

Passwords and other security features that restrict access to the computer system protect patient information.



If you have password access to your employer's system, never share passwords or log in to the health information system using borrowed credentials. Letting someone else use your password, or logging on and letting him or her use the system in your session, may seem like a timesaver. But it's essential that the organization be able to tell who gains access to what records. Don't write your password down, post it, or keep it where others can find it. These are all ways to put information at risk.

More steps for protecting electronic information

Make sure that computer screens are pointed away from the public and those computers are not connected to the patient information system when they are not in use. If you notice screens and information that appear easy for passersby to see or read, let the user or someone in the department know about the problem so that it can be corrected right away.

Because of the need to adequately protect patient information, you must never remove computer equipment, disks, or software from the facility even if you think they are no longer used, unless you first have permission from your supervisor. Special precautions must be taken to make sure that all patient information is removed from computer equipment before it is discarded.

Case scenario #8

You enter an unattended work area and notice a password for the computer system is posted on the wall.

Q What should you do?

A Notify your supervisor that a password appears to be publicly available and that you are concerned this might allow unauthorized access to the computerized health records of patients.

Case scenario #9

You find an old computer in the back of a room that's used for trash. You're certain that this machine is not being used any longer.

Q Can you take this computer to use in performance of your job?

A The thing to do is consult your supervisor. Any unauthorized removal of facility property is considered theft, so under no circumstances are you allowed to take the computer out of the facility without approval. But even if you intend to use the computer to do your job, you should first ask your supervisor to ensure that it never contained patient records or, if it did, that they have been adequately removed.

Case scenario #10

The hospital has, for many years, sent patients follow-up mailings, after they leave the hospital to market the hospital's services. The company that does the mailings calls and tells you they have lost the computer disk containing the names and addresses for letters to be mailed out. They want you to e-mail them the latest list of names and addresses.

Q

You know that the hospital notifies patients that they will be receiving this mailing, so can you send the requested information?

A

Most likely, the answer here is no. The best idea is to send the information offline via diskette. Check with your supervisor or the privacy and security officer about whether and how to send it. The facility might require it be sent by a contracted carrier.

Helpful Hints to Use When Working with Computers

- Review your organizations' 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 it is encrypted.
- Always double-check the address line of an email before you send it.
- If you use a password to access the organization's computer system, never share your password or log in to the system with 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.

Exceptions to the rules

There are some exceptions to confidentiality

You must be sure you know your organization's policies before releasing information and check that the particular

instance is approved. There are some cases in which patients do not have the right to keep their information private.

In these situations, your organization has a responsibility to release information, regardless of whether the patient agrees.

Seven reasons for releasing confidential information

1. Providers are required to report certain communicable diseases to state health agencies. The facility must report when patients have these diseases, even if the patient doesn't want the information reported.
2. The Food and Drug Administration (FDA) required providers to report certain information about medical devices that break or malfunction.
3. Some States require physicians or caregivers who suspect child abuse or domestic violence, report it to the police.
4. Police have the right to request certain information about patients to determine whether they are suspects in a criminal investigation.
5. The courts have the right to order providers to release patient information.

6. Providers must report cases of suspicious deaths or certain suspected crime victims, such as people with gunshot wounds.
7. The hospital or provider reports information to coroners and funeral directors in cases where patients die.

Understanding your role

In most cases, patients are informed when their health information is being reported to police or others outside the facility, but these are cases in which they do not have the right to control their information.

In all of these cases, the facility complies with the law and makes reports when necessary. Unless reporting this information is part of your job, you should not report this information yourself.

If you are interested in more information about what your state requires, you may find it useful to contact your facility's privacy official. That person can, if needed, check with legal counsel or the Attorney General.

There will be times when you will hear or see patient information. You are expected to not seek out information about patients unless it is job-related. But when you do see or hear information in the course of doing your job, remember that the information is confidential and you are not allowed to repeat it or share it with others. This applies even when you no longer work at this facility.

Reporting violations

The organization expects all employees to adhere to the privacy and confidentiality policies, but it recognizes there may be times when the policy is being abused.

Employees are encouraged to report violations or suspected violations to the facility's privacy official. You may report abuses anonymously, if you wish, by following the procedures in your privacy policy. However, do not fear any retaliation if you report a privacy violation.

The organization does not punish employees for reporting violations. In fact, it is considered part of your job to report instances where you suspect the privacy or confidentiality policies are being broken.