*New Team Member Orientation*

# HIPAA Overview


**HIPAA Overview** **3**

- What is PHI? 3

HIPAA Privacy Rule 3

- What is the Privacy Rule? 3
- Privacy Officer 3
- TPO (Treatment, Payment, and Operations) 4
- Patient Rights 5

Releasing Medical Records 9

- ROI Authorization Forms 9
- Other Record Requests 10
- Requesting Medical Records 10
- Filling Out a Release of Information Form 10

Additional Rules 14

- Minimum Necessary 14
- Internet and Social Networking 14
- Need to Know 15
- Other Tips 16
- Disposing of PHI 18
- Consequences of Violating the HIPAA Privacy Rule 18
- Privacy Breach 19

HIPAA Security Rule 19

What is Your Role in HIPAA Security? 21

- Passwords 21
- Email 21
- Locking Your Computer 21
- Identity Theft 21

# HIPAA Overview

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) addresses both the security and privacy of PHI.

## What is PHI?

Protected Health Information (PHI) is any patient information that:

- Is individually identifiable and related to health care
- Is transmitted electronically, maintained electronically, or maintained in any other form or medium (EVERYTHING!)
- Includes billing and encounter information.

# HIPAA Privacy Rule

## What is the Privacy Rule?

The HIPAA Privacy Rule enables individuals who receive medical treatment to control the manner in which PHI is used and to whom it is disclosed.

The Privacy Rule also establishes specific responsibilities for the ways a practice and its employees used and disclose patient PHI.

## Privacy Officer

HIPAA requires the designation of a privacy officer.

**CommUnityCare's Privacy Officer:**

SHARON MOODY @ 512-978-8190

SHARON.MOODY@COMMUNITYCARETX.ORG

## TPO (Treatment, Payment, and Operations)

Currently, we can release "appropriate, need-to-know" types of PHI that fall into the categories of TPO. In other words, if the information needed falls into the category of TPO, you don't need to get an authorization.

- **Treatment**: ongoing coordination of treatment for our patient that CommUnityCare ordered, referred the patient to, or is aware of

### Treatment

If a CommUnityCare provider refers a patient to a podiatrist, this is a continuum of care. We can release a patient's chart information to the specialist. No authorization is needed!

- **Payment**: minimally necessary "need-to-know" PHI to get payment, based on date of service information for a specific claim

### Payment

If an insurance company refuses to pay a claim because a patient's visit for a sore throat is coded as a wart removal, we can share a patient's chart information for that visit only in order to get paid. No authorization is needed!

- **Operations**: as currently outlined in the Notice of Privacy Practices (NPP)

### Operations

CommUnityCare continually audits charts for a variety of reasons. No authorization is needed for our internal medical record reviews to look at patient charts!

If a request is outside the boundaries of TPO, you will need an authorization to release this information. Non-TPO requests include requests by the patient, an attorney, or maybe an agency regarding a disability, etc.

## Patient Rights

The HIPAA Privacy Rule says that all patient's have rights. These include:

- Right to receive a Notice of Privacy Practices
- Right to authorize
- Right to request a restriction
- Right to an accounting of disclosures
- Right to access
- Right to designate a personal representative
- Right to request an amendment
- Right to request records in an electronic format
- Right to request confidential communication

### Right to Receive a Notice of Privacy Practices (NPP)

The NPP is a paper copy of CommUnityCare's privacy practices. It has required content that describes how a patient's medical information may be used and disclosed, as well as how the patient can get access to this information.

The NPP must be posted in a prominent location in each clinic and must accommodate different languages. Each new patient must be provided with a copy. It's important for CommUnityCare staff to be familiar with the contents of the NPP so that we can help the patient understand their rights!

Any physician with a direct treatment relationship with the patient must obtain patient acknowledgement of receipt of the Notice of Privacy Practices (NPP). Once a patient has been provided with the notice, the practice must make a "good faith effort" to get written acknowledgement from the patient that they were given a notice. These written acknowledgements are scanned into the patient's chart.

It is important to document any instances where you are unable to get a written acknowledgement. However, if you cannot get a written acknowledgement, the patient can still be treated.

## Right to Authorize

A patient has the right to authorize any use or disclosure of PHI not covered by TPO. However, the patient must give a completed written HIPAA compliant authorization that includes the following information:

- What information is being requested
- Name of person whose information is being requested
- Who is requesting the information
- Purpose of the request
- When the authorization expires or the date range it covers
- A written statement of the patient's right to revoke the authorization and instructions on how to revoke an authorization
- A statement that the information disclosed may be subject to re- disclosure by the recipient and is no longer protected by the rule
- Signature and date of patient

ALL requests for records must be forwarded to the ROI department for processing!

## Right to Request a Restriction

The patient has the right to request that a provider, health plan, or healthcare clearing house not use or disclose certain PHI. They also have the right to request that the provider make reasonable efforts to keep the communications or PHI confidential.

## Right to an Accounting of Disclosures

Patients have a right to receive an accounting of disclosures of protected health information (PHI) made in the six years prior to the date on which the accounting is requested.

## Right to Access Records

All patients have the right to request a copy of their medical records. This can be a physical copy or they can view their record electronically. A patient's records request must be processed within 15 days.

## Right to Designate a Personal Representative

A patient can also designate a personal representative. A personal representative is an individual who has been designated, in writing, by the patient to have the same authority or rights over the patient's PHI that the patient has.

### Designating a Personal Representative

For adult patients, we need a **Medical Power of Attorney Form** designating another person as their representative. This representative can make appointments, talk to the patient's doctor, and make medical decisions.

For minors, we need a **Consent for Treatment Without Parent Present Form** designating a step-parent, certain relatives or other caregivers as able to accompany the child for medical care.

The exception to needing this consent form is if the minor is being brought in by a grandparent, adult brother or sister, or adult aunt or uncle as stated in Family Code Chapter 32.

## Right to Request an Amendment

The patient has the right to request an amendment to their medical record. Amending a patient's medical record is not the same as altering the patient's medical record. All requests must be in writing and must be processed within 60 days. If an amendment is approved, it will be added to the patient's medical record. However, practices can also deny an amendment. Either way, all amendment resolutions must be in writing.

## Right to Request Records in an Electronic Format

The patient has to right to request an electronic copy of their medical record.

## Right to Request Confidential Communication

The practice must accept patient requests to restrict communication of PHI.

A practice is not required to agree with the restriction request but if the practice agrees, they must accommodate the patient's request.

A practice must also be able to share a patient's PHI in emergency situations and to comply with governmental authorities.

Additionally, the practice must be able to contact the patient for treatment and billing purposes.

### Confidential Communication

For example, a patient may request that lab results not be mailed to their home or that the clinic only call their cell phone with medical information.

# Releasing Medical Records

Authorization to release medical information is the written authorization from the patient when disclosure of protected health information (PHI) will be used for purposes other than treatment, payment or healthcare operations (TPO) and required non-routine disclosures. These authorizations go through the Release of Information (ROI) department.

## ROI Authorization Forms

An authorization form should be filled out when any patient, agency, or third party is requesting records. For example, these requests could come from patients, attorneys, Social Security, disability, or a life insurance company.

A valid authorization Must include:

- A specific description of the information to be used or disclosed.
- The name or identification of the person(s) or class of person(s) authorized to make the disclosure.
- The name or identification of the person(s) or class of person(s) to whom the provider may make the requested disclosure.
- A description of each purpose for the requested disclosure
- An expiration date or event that relates to the patient or the purpose of the disclosure (e.g., “until completion of the litigation.”).
- The date and signature of the patient or the patient’s personal representative.
- If the authorization is signed by the personal representative, a description of the personal representative’s authority
- The patient has the right to revoke the authorization at anytime (with certain exceptions) by submitting a written statement to the covered entity.
- The information disclosed per the authorization may be subject to redisclosure and no longer protected.All of the foregoing must be completely filled out, i.e., there should be no blanks concerning the required terms.

You must respond to these requests as quickly as possible. The Texas House Bill 300 (HB 300) and the Texas Medical Board require that requested records must be furnished by the physician within 15 business days after the date of the receipt of

the request. Patients who request an electronic copy of their health information must be provided the record within 3 business days. You should fax all record requests to the ROI. After these requests are processed they are scanned into the patient's chart.

If you receive a request from the Texas Medical Board, Nursing Board, or an attorneys office that we are a party to a lawsuit, you should notify Sharon Moody in Compliance as soon as possible!

## Other Record Requests

If you receive a records request related to a patient's referral, the referral coordinator for that clinic is responsible for processing the request.

You may also receive orders (e.g., durable equipment) that require supporting documentation. The nursing staff or designated staff at the clinic is responsible for processing the information and completing the order.

## Requesting Medical Records

Patients can request a copy of their medical records in person at their clinic and have the authorization forwarded to the ROI Department. However, they can also submit a request for medical records from CommUnityCare's website.

Patients get their first copy free, and any additional copies are priced according to the fee schedule as outlined by the Texas Medical Board.

## Filling Out a Release of Information Form

Authorization forms should be filled out completely. If all areas are not fully completed, the form is not valid and the ROI department won't know who is requesting the information or what information to send.

You should also make sure that either ***release*** or ***obtain*** is circled in the two sections at the top of the form. Release means a patient is authorizing us to release their medical records to the patient or another party. Obtain means that the patient is authorizing CommUnityCare to obtain their records from outside of CommUnityCare.

It is also very important that the **Dates of Service** field is filled out. This field refers to the date range in the patient's medical record that they would like to release or

obtain. For example, the patient might want to authorize chart information for one day, last month, or the entire chart.

CommUnityCare

AUTHORIZATION TO RELEASE MEDICAL INFORMATION

I authorize the CommUnityCare to *release/obtain* (circle one) medical information concerning:

Patient Name_____ Date of Birth_____ Soc. Sec. No._____

Address_____ Dates of Service_____

City_____ State_____ Zip_____ Telephone Number_____

**This information is to be** *released to/obtained from* (circle one):

Name_____

Address_____

City/State_____ Zip_____ Telephone #_____

**Return address for CommUnityCare:**

_____

_____

_____

The social security number field is the only field that is not required. You can enter the last four numbers of a patient's social security number or, if the patient declines, you can leave this field blank.

Under section titled **Please release the following information, indicated by an "X":** The items should reflect what the patient wants to be included in the released records.

**Please release the following information, indicated by an "X":**

| | | |
|---|---|---|
| ☐ History & Physical | ☐ Consultation | ☐ Nutrition Consultation |
| ☐ Lab Results/X-Rays | ☐ Operative Report (s) | ☐ Tuberculosis Elimination Records |
| ☐ Maternity Record | ☐ Psychotherapy Notes | ☐ WIC |
| ☐ Family Planning Records | ☐ Social Work Notes | ☐ Progress notes |
| ☐ Dental | ☐ Immunization record | ☐ Outside records |

I give special permission to release any information regarding items listed below

| | INITIAL |
|---|---|
| ☐ **HIV Medical Information** | _____ |
| ☐ **Psychiatric** | _____ |
| ☐ **Substance Abuse Records** | _____ |
| ☐ **Other** | _____ |

If the patient wants to include HIV, Psychiatric, Substance Abuse Records, or other specific chart information, they must check the checkbox and initial beside it.

The patient can choose to receive a copy of their records through the mail or in person at the clinic. We will not fax to a patient's home or business.

Please release my information via: ___Mail ___Orally ___Pick-up ___Electronic (CD) ___Fax (Emergencies Only) (Fax No._____)

Remember, the patient must show their ID to pick up their records!

Release of information forms expire after 12 months unless a patient specifies otherwise. The patient can document this is the middle section of the document.

*The patient or the patient's representative must read the following statements:*
*I, the undersigned, understand that I may revoke this consent at any time in writing by completing the revocation authorization form, except to the extent that action has been taken in reliance on it and that in any event this consent shall expires 12 months from when it is signed unless otherwise specified (Otherwise specified date_____). I understand that the provision of my health care and the payment for my health care will not be affected if I do not sign this form. Upon expiration, CommUnityCare can no longer use or disclose my information for the above purposes without a new authorization. All revocations will be sent to the CommUnityCare return address listed above.*

You should never put today's date in this field. That signifies that the authorization is only good for one day.

Once the patient has filled out the authorization form, you will need to review it for completeness and sign the **Witness** field.

## ROI Best Practices

- Check that all fields on the authorization form are completed!
- Fax all requests to the ROI Dept. ASAP
- Check person's ID when they pick up their records.
- Give ROI Department phone and fax numbers to the requestor if needed.
- Ensure referral and order requests are processed by clinic staff.

## Contacting the ROI Department

You can reach the Release of Information Department in the following ways:

| ROI Department: |
| --- |
| Email: *ROI |
| Phone: LINDA IHLO (512) 978-8513, ANDREA OLIVARES (512) |
| 978- 8515 or BREEANA RANGEL (512) 978-9948 |
| Fax: 512-901-9797 |
| Address: 2115 Kramer Ln., Suite 100, Austin, Tx, 78758 |

CommUnityCare

**AUTHORIZATION TO RELEASE MEDICAL INFORMATION**

I authorize CommUnityCare to ***release/obtain*** (circle one) medical information concerning:

Patient Name_____Date of Birth_____Soc. Sec. No. XXX-XX-_____

Address_____Dates of Service_____

City_____State_____Zip_____Telephone Number_____

**This information is to be *released to/obtained from*** (circle one)**:**

Name_____

Address_____

City/State_____Zip_____Telephone #_____

**Return address for CommUnityCare:**

_____

_____

_____

**Please release the following information, indicated by an "X":**

- ☐ Office Visit Notes
- ☐ Medication Record
- ☐ Outside records
- ☐ Lab Results
- ☐ Dental
- ☐ Other specify_____
- ☐ X-Ray results
- ☐ Dental films
- ☐ X-Ray Films
- ☐ Consultation Reports
- ☐ Immunization record
- ☐ Tuberculosis Elimination Records

**Your initials are required to release the following information:**

| | INITIAL |
|---|---|
| ☐ **HIV Medical Information** | _____ |
| ☐ **Behavioral Health Records (Psychiatric)** | _____ |
| ☐ **Substance Abuse Records** | _____ |
| ☐ **Genetic information (including genetic test results)** | _____ |

**This information is necessary for the following purposes:**

___Follow-up Care ____ Patient is requesting disclosure ___Disability Benefits ___Attorney

___Other Please Explain_____

**Will financial/compensation result in use or disclosure?** ☐ Yes ☐ No

Please release my information via: ___Mail ___Pick-up Format: _____ Paper ___Electronic (CD)

_____ Fax (To Providers or Emergencies Only) (Fax No._____)

***The patient or the patient's representative must read the following statements:***

***I, the undersigned, understand that I may revoke this consent at any time in writing by completing the revocation authorization form, except to the extent that action has been taken in reliance on it and that in any event this consent shall expires 12 months from when it is signed unless otherwise specified (Otherwise specified date_____). I understand that the provision of my health care and the payment for my health care will not be affected if I do not sign this form. Upon expiration, CommUnityCare can no longer use or disclose my information for the above purposes without a new authorization. All revocations will be sent to the CommUnityCare return address listed above.***

I understand that the above information may include records/reports from other health care providers involved in my care or treatment. I have read this authorization and understand what information will be used or disclosed, who may use and disclose the information and the recipient(s) of that information. I understand that any disclosure of information carries with it the potential for an unauthorized redisclosure and the information may not be protected by Federal confidentiality rules.

***I understand any of the above requested information may include results of sexually transmitted disease, acquired immunodeficiency syndrome (AIDS) Human Immunodeficiency Virus (HIV) tests if any were performed. Further, I understand any of the above requested information may include results of alcohol/drug (substance) abuse and/or diagnosis and treatment of psychological disorders.***

***I understand that I may see and obtain a copy of the information described on this form if I ask for it, and that I get a copy of this form after I sign it.***

***If form is not complete we may be unable to fulfill this request.***

**TO THE PARTY RECEIVING THIS INFORMATION:** This information is being disclosed to you from records where confidentiality may be protected by federal and/or state laws. If so, regulations 42 CFR, Part 2, prohibit further disclosure without specific written consent of the person to whom it pertains, or as otherwise permitted by such regulation.

_____ _____ _____

**SIGNATURE** of Patient or Authorized Party Date **RELATIONSHIP** to Patient

**WITNESS**_____ **REASON** Patient is not signing_____

Form # 2200 English 1-7-14

# Additional Rules

## Minimum Necessary

Under HIPAA, a medical practice must ensure that only the minimum necessary information is released (except where there is an authorization!).

As a user of PHI, your role is to comply with all of your organizations policies to make sure that you don't create a situation where information is:

- seen by someone who shouldn't have access to it
- corrupted
- rendered unavailable

### Minimum Necessary – True or False?

True or **False**: An insurance company asks for copies of Jane Doe's record because she got into a car accident. Should CommUnityCare release Janes entire record?

## Internet and Social Networking

Social networking has become a prevalent method of self-expression in our culture (e.g., Facebook, blogs, Instagram, twitter, websites). Employees are responsible for the content they publish on these types of sites and should never disclose any PHI or publish photos of our patients.

If PHI is disclosed in this way, sanctions will be imposed, up to and including termination, as specified in our policies.

### Social Networking – True or False?

1. **True** or False: An employee posts a picture on Facebook of their favorite patient celebrating the patient's birthday during a clinic visit. Has the team member violated HIPAA?

2. **True** or False: Dr. Miller took a picture on his cell phone to record a skin disorder to upload it into the EHR. Did he violate HIPAA?

## Need to Know

HIPAA laws and privacy rules regarding personal health information require CommUnityCare staff to protect a patient's privacy. The "need to know" concept provides guidance for us in complying with current privacy laws and rules.

It's important to understand what "need to know" means because it:

- Protects patient medical and billing records
- Helps you comply with privacy laws and regulations
- Helps you avoid violating privacy laws and regulations.

Before looking at a patient's health information, ask yourself one simple question:

*"Do I need to know this to do my job?"*

If the answer is no, then you should stop. Unauthorized or unnecessary access into a patient's medical and/or billing records is a violation of CommUnityCare policies and could result in your immediate termination.

### Need to Know – True or False?

**True** or False: Your cousin is a patient at CommUnityCare and you checked her chart to find out if she's pregnant or not. Have you violated the HIPAA Privacy Rule?

**True** or False: Your minor daughter is a patient at CommUnityCare and you want to see her lab results. Have you violated the HIPAA Privacy Rule? T or F

**True** or False: Even though you have the right to access those records as the parent of a patient, you need to go through the proper channels to request records.

Also remember that once your employment ends, you are still bound by the confidentiality agreements you signed when you were hired.

If you know a patient at CommUnityCare, email the Helpdesk and ask them to block you from accessing their records in NextGen.

Additionally, be aware that federal and state law enforcement agencies are currently focusing attention on audits and prosecution of privacy violations. In a recent case, a healthcare employee pleaded guilty to violating the federal privacy provisions of HIPAA by obtaining individuals' PHI without a valid reason. The employee faces a maximum penalty of four years in prison.

## Other Tips

- When sending faxes, always double-check the fax number and that you have the correct patient's information.
- Never take PHI home with you. Be extremely careful if you are transporting PHI from one site to another.
- If you are ever unsure about accessing a patient's records, you can always ask your supervisor or manager for clarification. If you ever have a question about patient privacy, call or email CommUnityCare's Privacy Officer, Sharon Moody (512-978-8190).

## Workers Fired in Privacy Breach at LA Hospital Popular with Stars

Five medical workers have been fired over a patient data breach at Cedars-Sinai Medical Center, the Los Angeles facility said in a statement, while celebrity website TMZ reported on Saturday that the hacking effort targeted reality star Kim Kardashian.

Cedars-Sinai, a favorite destination for celebrities seeking medical care, said in the statement it has a "high standard for security" and "in this case that standard was violated." Kardashian, the star of the reality television show "Keeping Up With the Kardashians," gave birth on June 15 at Cedars-Sinai to daughter North West, whose father is Grammy-winning rap star Kanye West.

Cedars-Sinai officials declined to say whose privacy had been breached, but the hospital said it "informed the affected patients" and apologized to them.

The breach of 14 patient records occurred between June 18 and June 24, the hospital statement said. TMZ reported that Kardashian checked out of Cedars-Sinai about a week after she gave birth and was contacted by the hospital and told she was one of the patients whose records were accessed.

TMZ, which cited unnamed sources, said Kardashian's family suspected a leak of information at Cedars-Sinai after media reports disclosed details Kardashian had not revealed to anyone.

Representatives for Kardashian did not return calls or emails seeking comment on Saturday. The Cedars-Sinai statement said four of the workers who inappropriately logged onto the hospital's information system to access patient records were employees of local physicians with staff privileges at the hospital.

The other workers were a medical assistant employed by the Cedars-Sinai Medical Care Foundation and a student research assistant who was a volunteer, the hospital said. As a result of the privacy breach, the five medical workers with ties to Cedars-Sinai were fired and the volunteer barred from working there, it said.

Cedars-Sinai said that while it had no indication "any criminal acts were committed by the individuals" it was reaching out to law enforcement agencies in "an abundance of caution."

In another high-profile privacy breach at a Los Angeles hospital, authorities in 2008 charged a former employee at UCLA Medical Center with obtaining patient information for commercial gain after she leaked details on the late actress Farrah Fawcett's deteriorating condition. The former worker pleaded guilty later that year.

http://www.nytimes.com/reuters/2013/07/13/arts/13reuters-usa-hospital-privacy.html?hp&_r=1&

## Disposing of PHI

Each clinic facility and all administrative offices are required to have designated "Confidential Trash/Shred" containers in all patient care areas, pharmacies, HIM units, and any other locations where patient information is being handled. Any unlocked container must be emptied daily into a secure container. Routine audits are in place to ensure compliance.

If you see PHI in an open trash container or recycling bin, tell your supervisors or privacy officer. He or she can get rid of it properly, either by placing it into a locked bin until it can be destroyed or by placing it into a paper shredder.

## Consequences of Violating the HIPAA Privacy Rule

Any privacy gaffes – even unintentional ones – could undermine patient trust in our organization and jeopardize CommUnityCare's credibility.

Additionally, employees who break this law could face lawsuits, fines, and even jail time. Civil monetary penalties for violating provisions of the HIPAA statues can range from $100 up to $50,000 with a $1,500,000 cap for violations of each identical requirement prohibition.

Penalties can now apply to individuals!

### Privacy Breach

The HIPAA Privacy Rule establishes the HITECH Privacy Breach Act, which identifies how to handle a privacy breach.

If PHI is released without the proper authorization, it is considered a privacy breach. If a privacy breach occurs, you need to take the following steps.

1. The employee must immediately report any breaches that occur to your immediate supervisor, manager, or the Compliance Officer.
2. A HIPAA incident report is filed in compliance 360.
3. The compliance department will investigate and determine whether PHI has been breached and if reporting or disclosure to patient is necessary.

You can prevent privacy breaches by complying with all security measures for protecting PHI.

## HIPAA Security Rule

The HIPAA Security Rule requires medical practices to put reasonable measures in place to protect electronic PHI from internal and external security threats. Practices must document the steps they are taking to ensure best practice security measures. Without documented efforts, practices are liable for damages in the event of a security breach.

## Privacy refers to:

THE RIGHTS OF THE PATIENT TO LIMIT THE USE AND DISCLOSURE OF PHI.

## Security refers to:

PROTECTING THE PHI THAT IS COLLECTED, CREATED, OR MAINTAINED BY THE PRACTICE IN AN ELECTRONIC FORMAT.

## CommUnityCare's Security Officer:

Edward O'Connor You may reach Ed and his team by emailing:

CUCSecurity@communitycaretx.org

# What is Your Role in HIPAA Security?

## Passwords

Access to any electronic medical information will be by password. Under no circumstances may an employee tell another his/her password. Our electronic medical records software will produce an audit trail that will show all users who have accessed a patient's medical record. Employees should be able to explain and justify any audit trail demonstrating that their password was used to access patient-related information. Failure to do so will results in appropriate disciplinary action, up to and including termination of employment. Never give out your passwords!

## Email

If you send an email that contains PHI (e.g., patient's name, MRN) outside of CommUnityCare's network, you must encrypt the email. You can do this by typing PHI (in all caps!) in the subject line of the email.

If you want to receive work email on your phone, you must password protect your phone!

## Locking Your Computer

You need to secure your computer when leaving your workstation by locking the screen. This will prevent anyone else from accessing patient information. You must perform this function any time you step away from your computer!

## Identity Theft

To avoid identity theft, get a picture ID whenever possible or have the patient (or the patient's guardian) provide three of the following identifiers:

- Full patient name
- Patient's date of birth
- Patient's social security number
- Address on file