Carolina Family
Health Centers, Inc.

# HIPAA Training 2025

**Corina Buzard, Chief Compliance Officer**

# HIPAA

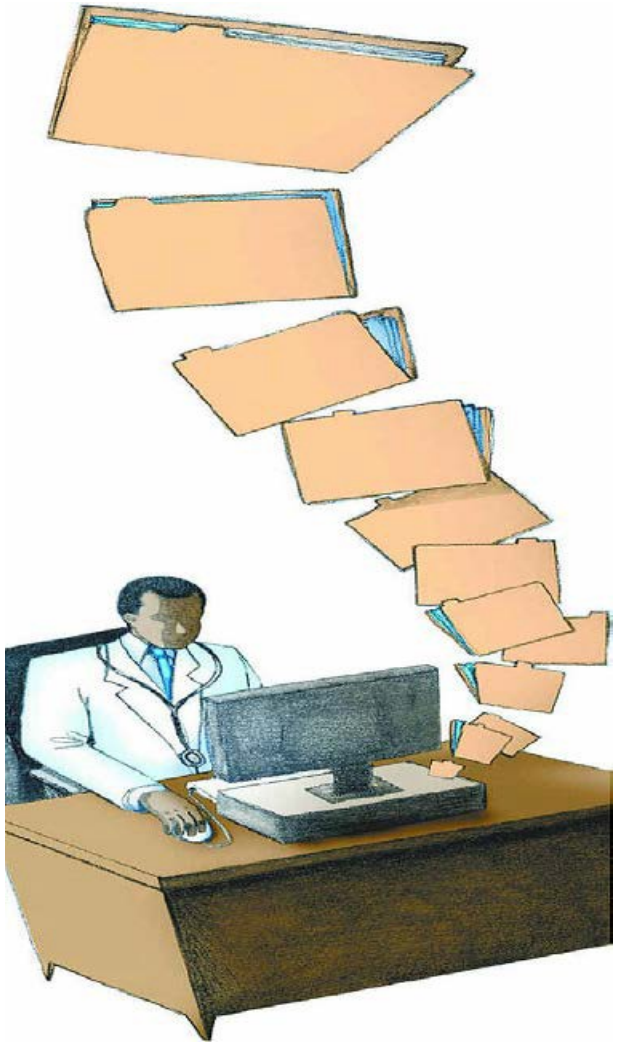
The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a federal law designed to protect a subset of Sensitive Information known as protected health information (PHI).

In 2009, HIPAA was expanded and strengthened by the HITECH Act (Health Information Technology for Economic and Clinical Health). In January of 2013, the Department of Health and Human Services issued a final rule ("Final Rule") implementing HITECH's statutory amendments to HIPAA.

# HIPAA

- In 2024, the HIPAA law was amended to add the HIPAA Reproductive Health Care Privacy Rule.

# HIPAA Privacy



# Covered Entities Have a Duty to Protect PHI

A "covered entity" is any person or organization that furnishes, bills, or is paid for health care services in the normal course of business.

Individually identifiable health information collected or created by a covered entity is considered PHI.

**CFHC, Inc. is considered a covered entity.**

# Protected Health Information (PHI)

PHI is any information in the medical record that can be used to identify a patient and that was created, used, or disclosed in the course of providing a health care service.

Note: The Final Rule now protects the PHI of a deceased individual for a period of **50 years following the death** of that individual.

# Any of the following are considered identifiers under HIPAA and are considered PHI

- Patient names
- Geographic subdivisions (smaller than state)
- Telephone numbers
- Fax numbers
- Social Security numbers
- Vehicle identifiers
- E-mail addresses
- Web URLs and IP addresses
- Dates (except year)
- Names of relatives

- Full face photographs or images
- Healthcare record numbers (Patient ID #, URN #)
- Account numbers
- Biometric identifiers (fingerprints or voiceprints)
- Device identifiers
- Health plan beneficiary numbers
- Certificate/license numbers
- Any other unique number, code, or characteristic that can be linked to an individual

# HIPAA regulations permit the use or disclosure of PHI for:

- providing medical treatment
- processing healthcare payments
- conducting healthcare business operations
- public health purposes as required by law

# Access Must be  Authorized

An employee may only access or disclose a patient's PHI when this access is part of the employee's job duties.

If an employee accesses or discloses PHI without a patient's written authorization or without a job-related reason for doing so, the employee violates CFHC, Inc.'s policy and HIPAA.

# Unauthorized Access

It is never acceptable for an employee to look at PHI "just out of curiosity," even if no harm is intended (i.e., retrieving an address to send a 'get well' card).

It also makes no difference if the information relates to a "high profile" person or a close friend or family member – ALL information is entitled to the same protection and must be kept private.

Be aware that accessing PHI of someone involved in a divorce, separation, break-up, or custody dispute may be an indication of intent to use information for personal advantage. This can have more serious consequences.

**Employees cannot look at their own health record at CFHC, Inc. without consent of their primary care provider. Employee's must follow CFHC, Inc.'s HIPAA procedures to gain access to their PHI.**

# HIPAA Breach

A breach is the acquisition, access, use, or disclosure of protected health information in a manner not permitted under the HIPAA Privacy Rule which compromises the security or privacy of the protected health information.

# Examples of Breaches

- The electronic health record system was hacked and patient files were taken
- A medication was delivered to the wrong person
- An employee accessed their spouse’s PHI.

# Employees Must Report Breaches

Part of your responsibility as a CFHC, Inc. employee is to **report privacy or security breaches to your supervisor or** one of the following persons:

- HIPAA Privacy Officer (Corina Buzard, CCO);
- HIPAA Security Officer (Danielle Peyatt, DRMQI or Jason Terry DIT);
- Chief Executive Officer (Laura Owens, CEO)

*Reports of possible information privacy violations can be made through CFHC, Inc.'s Compliance Hotline at 252-243-1239, CFHCCompliance@cfhcnc.org, or through incident reporting policy and procedure.*

Employees, volunteers, students, or contractors of the CFHC, Inc. may not threaten or take any retaliatory action against an individual for exercising his or her rights under HIPAA or for filing a HIPAA report or complaint, including notifying of a privacy or security breach.

# When a Breach Occurs

- CFHC must notify the individual(s) affected within 60 days
- The notification must meet reporting requirements
- The Department of Health and Human Services must be notified

# Patient Rights

# Patient Rights Under the Privacy Law

- To receive a copy of CFHC,  Inc.'s Notice of Privacy Practices
  - HIPAA-500 Notice of Privacy Practice
- To request restrictions and confidential communications  of their PHI
  - HIPAA-400.01 Requests for Restrictions
  - HIPAA-400.02 Request for Confidential Communications
- To inspect and/or receive an electronic copy of their healthcare records
  - HIPAA-400.03 Request for Access
- To request corrections of their healthcare record
  - HIPAA- 400.04 Request to Amend

# Patient Rights Under the Privacy Law - continued

- To obtain an accounting of disclosures (i.e., a list showing when and with whom their information has been shared)

  HIPAA-200.02 Authorizations for Uses and Disclosures

- To file a complaint with a healthcare provider or insurer and the U.S. Government if the patient believes his or her rights have been denied or that PHI is not being protected

  HIPAA-103 Privacy Complaint

- To receive notice of a breach of their unsecured PHI

  HIPAA-600 Breach

- To have someone act on his/her behalf (designate a personal care representative)

  HIPAA-400.06 Designation and Authority of a Personal Representative

# Request for Access

- Patients have the right to access their PHI (inspect or receive a copy).
- CFHC must respond to a patient's request within 30 days.
- If CFHC is unable to fulfill this request, CFHC can provide a written statement to the patient for an additional 30 days.
- All patients requesting access to their PHI are directed to the front office staff to sign the *Authorization for Uses and Disclosures for PHI* form and submit the Release of Information (ROI) request within Epic.
- The request is reviewed by the Medical Records staff for unreviewable grounds for denial of the request (i.e., request for psychotherapy notes, information compiled for civil, criminal proceedings, etc.) or reviewable grounds
- The provider is sent the request and must review the request for reviewable grounds to deny the request

# Reviewable Grounds

CFHC, Inc. may deny access on any of the following grounds:

- CFHC, Inc.'s providers in their professional judgement determine that the requested access is reasonably likely to endanger the life or physical safety of the patient or other person.

- The information references another person and CFHC, Inc.'s providers in the exercise of professional judgment determine that the requested access is reasonably likely to cause substantial harm to the other person.

- The request is made by the patient's personal representative and CFHC, Inc. providers determine, in the exercise of professional judgment, that the requested access is reasonably likely to cause substantial harm to the patient or another person.

The providers and staff need to expedite these requests promptly to prevent penalties.

# HIPAA Reproductive Health Care Rule

# What is reproductive healthcare?

**Reproductive healthcare** means healthcare that affects the health of an individual in all matters relating to the reproductive system and to its function and processes.

# HIPAA Reproductive Healthcare Privacy Rule

HIPAA Reproductive Healthcare Privacy Rule strengthens privacy protections by prohibiting the use or disclosure PHI by CFHC, Inc. or its employees to:

1. Conduct a criminal, civil, or administrative investigation into or impose criminal, civil, or administrative liability on any person for the mere act of seeking, obtaining, providing, or facilitating reproductive healthcare, where such healthcare is lawful under the circumstances in which it is provided.
2. Identify a person to conduct such investigation or impose such liability.

# Prohibition

The prohibition applies where CFHC, Inc. or its staff has reasonably determined that one or more of the following conditions exist:

1. Reproductive healthcare is lawful under the law of the state in which such healthcare is provided under the circumstances in which it is provided.
2. Reproductive healthcare is protected, required, or authorized by federal law, including the U.S. Constitution, regardless of the state in which healthcare is provided.
3. Reproductive healthcare was provided by a person other than CFHC, Inc. or its staff and it is presumed the provider of the care was lawful.

# Presumption

The rule includes the presumption that the reproductive healthcare provided by a person other than the covered healthcare provider (i.e., CFHC, Inc.), health plan, or healthcare clearing house (or business associate) receiving the request was lawful.

In such cases, reproductive healthcare is presumed to be lawful under the circumstances in which it was provided unless one of the following conditions are met:

# Presumption (cont.)

- CFHC, Inc. or its staff has actual knowledge that the reproductive healthcare was not lawful under the circumstances in which it was provided; or

  Example: An individual disclosed to their doctor that they obtained reproductive health care from an unlicensed person and the doctor knows that the specific reproductive health care must be provided by a licensed health care provider.

- CFHC, Inc. or its staff receives factual information from the person requesting for the use or disclosure of PHI that demonstrates a substantial factual basis that the reproductive health care was not lawful under the circumstances in which it was provided.

  Example: A law enforcement official provides CFHC, Inc. with evidence that the information being requested is reproductive health care that was provided by an unlicensed person whereas the law requires that such health care be provided by a licensed health care provider.

# Break it down

- CFHC, Inc., nor its employees,  can use or disclose protected health information regarding reproductive health care to investigate or bring a criminal or civil action against a patient if the treatment provided was lawful in the State and circumstances for which it was provided.

Example: A person living in another State, where it is against the law to have an abortion, travels to NC where it is legal.  The law protects the patient from litigation being brought against them in their home State where abortion is illegal. The patient's NC reproductive health care records cannot be used against them to bring about criminal or civil charges.

- The intent is to protect the privacy of women so that they can openly share concerns and their reproductive history with their providers and provide protections from litigation in their home State where the laws may differ.

# Attestation

The CFHC, Inc.is required to obtain a signed attestation that the use and disclosures **are not for a prohibited purpose** when it receives a request for PHI potentially related to reproductive health care. This attestation applies when the request is for PHI for any of the following:

- Health oversight activities
- Judicial and administrative proceedings
- Law enforcement purposes
- Disclosures to coroners and medical examiners

# Attestation (Cont.)

- Under those circumstances, individuals or agencies will have to attest that the reason for the request of records is not prohibited under the HIPAA Reproductive Health Care Privacy Rule.
- And acknowledge that they could face criminal charges if they in violation.

# Attestation Form

- When requests for PHI are received, the request is forwarded to the medical records staff for processing.
- If the request is from law enforcement, a coroner/medical examiner, the health department/public health agencies, or a court of law, the staff ensures the attestation is signed before releasing records.
- A copy of the valid attestation form attached to the  ROI request in EPIC.

# HIPAA Security

# HIPAA Security Rule

- The HIPAA Security Rule concentrates on safeguarding PHI by focusing on the confidentiality, integrity, and availability of PHI.

- Confidentiality means that data or information is not made available or disclosed to unauthorized persons or processes.

- Integrity means that data or information has not been altered or destroyed in an unauthorized manner.

- Availability means that data or information is accessible and useable upon demand only by an authorized person.

# Security and Safeguards

**CFHC, Inc. is required to have administrative, technical and physical safeguards to protect the privacy of PHI.**

**Safeguards must:**

- Protect PHI from accidental or intentional unauthorized use/disclosure in computer systems (including social networking sites such as Facebook, Twitter and others) and work areas.
- Limit accidental disclosures (such as discussions in waiting rooms and hallways).
- Include practices such as encryption, document shredding, locking doors and filing storage areas, and use of passwords and codes for access.

# Malware

- Your antivirus and spyware applications are deployed and maintained by the IT Department. It is your duty to report any suspicious activity to the IT Department.

- Safe Internet browsing habits can also reduce the likelihood of an infection; do not open email or click on embedded links from an unknown or untrusted site.

- If the computer or mobile device you are using stores work-related sensitive information, personal use of the web is not recommended

# Email and Mobile Devices

- Encryption is required when a CFHC, Inc. employee sends or receives PHI via email.
- Do not open email attachments if the message looks the least bit suspicious, even if you recognize the sender. “When in doubt, throw it out.”
- Do not respond to “spam” – simply discard or delete it, even if it has an “unsubscribe” feature.
- All mobile phones containing PHI must be encrypted and password protected.
- Employees must utilize the following security controls when storing and transmitting sensitive information via mobile devices:
    - strong power-on passwords
    - automatic log-off
    - display screen lock at regular intervals while the device is inactive
    - Encryption
- Never leave mobile computing devices unattended in unsecured areas.
- Immediately report the loss or theft of any mobile computing device to your supervisor and the Director of IT.

# Communications in Public Areas

- Be aware of your surroundings when discussing sensitive information, including PHI.
  - Do not discuss sensitive information or PHI in public areas such as in restaurants, at the gym, or while riding the bus.
  - Be mindful when in the pods or other areas within our facilities

# Appropriate Disposal of Data

- Hard copy materials such as paper must be properly shredded or placed in a secured bin for shredding later.

- Magnetic media such as diskettes, tapes, or hard drives must be physically destroyed or “wiped” using approved software and procedures. Contact the Director of IT for more information.

- CD ROM disks must be rendered unreadable by shredding, defacing the recording surface, or breaking

# Physical Security

- Computer screens, copiers, and fax machines must be placed so that they cannot be accessed or viewed by unauthorized individuals
- Computers must use password-protected screen savers
- PCs that are used in open areas must be protected against theft or unauthorized access.
- Servers and mainframes must be in a secure area where physical access is controlled.

# Penalties for Breaches and HIPAA Violations

- Corrective action, ***HIPAA-104 Sanctioning Employees***
- Monetary fines to an individual and the organization
- Criminal Penalties

# Penalties for Breach and HIPAA Violations

- The four categories used for the penalty structure are as follows:
- **Tier 1:** A violation that the covered entity was unaware of and could not have realistically avoided, had a reasonable amount of care had been taken to abide by HIPAA Rules
- **Tier 2:** A violation that the covered entity should have been aware of but could not have avoided even with a reasonable amount of care. (but falling short of willful neglect of HIPAA Rules)
- **Tier 3:** A violation suffered as a direct result of “willful neglect” of HIPAA Rules, in cases where an attempt has been made to correct the violation
- **Tier 4:** A violation of HIPAA Rules constituting willful neglect, where no attempt has been made to correct the violation within 30 days

# Minimum fines 

- **Tier 1:** Minimum fine of $100 per violation up to $50,000
- **Tier 2:** Minimum fine of $1,000 per violation up to $50,000
- **Tier 3:** Minimum fine of $10,000 per violation up to $50,000
- **Tier 4:** Minimum fine of $50,000 per violation

These fines are adjusted annually to take into account inflation

# Criminal Penalties

- The tiers of criminal penalties for HIPAA violations are:
- **Tier 1:** Reasonable cause or no knowledge of violation – Up to 1 year in jail
- **Tier 2:** Obtaining PHI under false pretenses – Up to 5 years in jail
- **Tier 3:** Obtaining PHI for personal gain or with malicious intent – Up to 10 years in jail

# Questions?