

# BASIC HIPAA TRAINING



**CRMC Workforce With Access to PHI**



**COOKEVILLE REGIONAL  
MEDICAL CENTER**

*It's the Way WeCARE*



# Who Needs Training and Why?

All members of our workforce may come in contact with “Protected Health Information” (or PHI) and are Federally required to attend training.

This training is designed to:

- Summarize important HIPAA regulations
- Provide information regarding our privacy and information security policies.
- Ensure Federal compliance

All policies can be found on Policy Stat through the CRMC Intranet Page

## What Exactly Is HIPAA?

The Health Insurance Portability and Accountability Act of 1996

Enforced by the U.S Department of  
Health & Human Services  
Office for Civil Rights (OCR)

Includes Regulations Regarding:

- Privacy and Security of health information
- Several patient rights related to health information
- Notification of breaches of confidentiality
- Substantial penalties for violations

## What is Protected By HIPAA?

Protected Health  
Information (PHI)

Patient’s individually identifiable  
health information that:

- Is created, stored, transmitted or received by a health care provider, health plan, or health care clearinghouse
- Relates to the past, present, or future of an individual’s physical or mental health or condition, the provision of health care to an individual, or the payment for an individual’s health care.

EXAMPLES OF PHI:	Medical charts	Billing records
	Problem logs	Health plan claims records
	Photographs and videotapes	Health insurance policy number
	Communications between health care professionals	

Health information is protected if it can directly or indirectly identify someone. If any direct or indirect identifiers are present, the information is PHI and subject to HIPAA protection.

Information can be “de-identified” – but the Privacy Officer must review to ensure all direct and indirect identifiers have been properly removed.



# How HIPAA Protects PHI

- Limits what PHI an employee may use or disclose.
- Limits the purposes for which PHI may be used or disclosed.
- Limits the amount of information that may be used or disclosed. (Minimum Necessary Rule)
- Requires use of safeguards over how PHI is used, disclosed and stored.

## Who May Access or Use PHI?

**CRMC workforce members trained on HIPAA Privacy and Security Rules.**

### However:

- You must only access PHI if you need it in order to perform your job.
- You must agree to protect the confidentiality of the information.
- You are subject to discipline if you violate CRMC's privacy policies and procedures.

## Permitted Uses For PHI

**Workforce members may use or disclose PHI only as needed for:**

- Treatment
- Payment
- Health Care Operations
- Specified public policy exceptions, such as Public Health and Law Enforcement

---

**All other uses  
required the patient's  
written authorization.**

---

## Minimum Necessary Rules

### MINIMUM AMOUNT NECESSARY

The use or disclosure of PHI must be limited to the Minimum Amount Necessary to accomplish the purpose.

### NEED TO KNOW BASIS

**For example** – A receptionist probably doesn't need to see the X-rays of a patient to do his or her job.

### RULE DOES NOT APPLY FOR TREATMENT PURPOSES

Using your professional judgement, you can use or disclose any information that is needed for actual treatment purposes.



# Safeguarding PHI

**Patients consider health information their most confidential information and we must protect it accordingly.**

- **Do not access** PHI that you do not need to do your job.
- **Do not discuss** PHI with individuals who do not need to know it.
- **Do not provide** PHI to anyone not authorized to receive it.

*Misusing PHI can result in discipline, legal penalties, and loss of public trust.*

## When using or disclosing PHI think about:

- Where you are.
- Who might overhear.
- Who might see.
- Discussing PHI in front of others who do not need to know  
*(Including other employees in your department or other departments, visitors, and your own family members or friends.)*
- Leaving records accessible to patients or others who do not need to see them.
- Positioning PC monitors where others can view them.
- Using printers located in public or unsecured areas.

## REMEMBER

- Keep your user ID and password confidential and secure.
- Use strong passwords that are hard to guess.
- Never write it down and “post it”.
- Do not allow anyone else to access the computer system under your user ID.
- Never share your log-in credentials.
- Never leave computer station unattended without logging off or locking it first. (Remember, Press F11 to log-off)
- If you come to a workstation that another USER is logged onto, report it to your supervisor or Privacy Officer, log the other USER off and then log-on with your own USER log-on credentials.
- Never perform any duties using another USER’s log-on credentials.
- NEVER insert a CD, DVD, USB thumb drive or other removable media into a workstation without prior authorization from I.S.

# Safeguarding PHI

**Do not engage in risky practices  
with computers used to access PHI.**

- Do not surf the internet.
- Do not open e-mail attachments unless you know it's from a trusted source. Report all suspicious emails to I.S.
- Do not install applications (ex: Java, Adobe, Coupon printer, etc.) Contact IT/IS if your PC is requesting an application installation.
- Do not unnecessarily print or copy PHI. (Paper is too easy to misplace.)
- When faxing PHI, carefully verify the fax number, and use a fax cover page with your contact information.
- Do not send PHI in email unless first cleared by your supervisor. (must be encrypted)
- Dispose of PHI when it is no longer needed. Use approved shredding bins for documents containing PHI.

---

**If something makes you feel uncomfortable...report it!**  
**Privacy Officer needs to be aware of ALL privacy concerns.**

---

## **REPORT:**

- Unusual activity to your supervisor immediately.
- If you observe questionable practices.
- If you find PHI in inappropriate areas.
- If you suspect unauthorized use of your user ID/password.
- If a patient complains to you about a privacy issue.





# Why Should We Care About The HIPAA Rules?

**Loss of our patients' trust:** Patients expect us to protect their private information

**CRMC:** Disciplinary action up to and including termination. Your professional license or certification could be jeopardized.

**Civil & Criminal Penalties:** Up to \$1.5 million per year per violation. Possible imprisonment of up to ten years.

**Lawsuits:** Invasion of Privacy/negligence



**Thank you for protecting  
the privacy of our patients!**

**Please contact your  
Supervisor or our Privacy Officer  
(ext. 5842 or [privacy@crmchealth.org](mailto:privacy@crmchealth.org))  
if you have any questions or concerns.**





COOKEVILLE REGIONAL  
M E D I C A L C E N T E R

*It's the Way* **WeCARE**

OCTOBER 2022

