Health Insurance Portability and Accountability Act (HIPAA)

Initial Training

Warren County Department of Fire Rescue Services
2018 Online Resource
Resources

  - “HIPPA For Professionals”
  - Updated June 16, 2017
What is HIPAA??

- HIPAA = Health Insurance Portability and Accountability Act. It is a Federal Law that was passed in 1996.

- Created by – United States Department of Health and Human Services (DHHS)
HIPAA is a common set of standards that protects certain health information. There are several components – but, we are most concerned with the “Privacy Rule.”
The Privacy Rule

- The intent of the Privacy Rule is to provide basic rights regarding the use of “Protected Health Information” (PHI).

- It protects all “individually identifiable health information.” It can be electronic, paper, or oral.

- Applies to “covered entities.”
Who or What is a “Covered Entity”?

Three Categories:

- Health plans.
- Health care clearing houses.
- Health care providers who transmit any health information electronically.

WCFR EMS Providers fall under the “Health Care Provider” category!
What’s Required?

The Privacy Rule requires “Covered Entities” to:

- Protect PHI
- Designate a Privacy Officer
- Develop a Notice of Privacy Practices
- When permitted, only disclose the minimum necessary PHI
- Conduct/document training for the entire Department
- Develop an Authorization Form for release of PHI
More Requirements

- Update policies and procedures
- Identify Business Associates and create contracts
- Apply reasonable administrative, technical, and physical safeguards
- Look for “leaks” in the policy.
Privacy Officer

- An individual within the organization that is responsible for developing and implementing policies and procedures required by HIPAA.

- Warren County’s HIPPA compliance officer is the Cost Recovery Manager.
Protected Health Information

• PHI is any information created or received by a health care provider which relates to:
  • Past, present, or future physical or mental conditions.
  • Provision of health care.
  • Past, present, or future payment for care.
Examples of PHI

- Name
- Address
- Date of Birth / Age
- Social Security Number
- **Scene pictures** that include license plates
- Medical condition / past medical history
- Full face photos
• HIPAA should NEVER negatively impact the quality of patient care or impede the ability to provide care!!

• The appropriate communication of PHI with other health care providers directly involved in providing patient care does not constitute a violation of HIPAA.
Safeguarding PHI

- PCR’s should be kept in a secure location.
- Networks containing PCR’s should be password-protected with user specific logins.
- Generic logins allow for anonymous access to PHI and set up the Department for liability.
- Include confidentiality statements on e-mails and faxes that contain PHI.
- *Never allow someone else to use your login information.*
Use Caution…

- Talking about current or prior incident(s) while re-stocking ambulance or typing your report at the ER.

- Discussing a call anywhere other than an official audit or review.

- Discussing “interesting” calls, famous patients, or neighbors.

- Sharing a co-worker or fellow responder’s PHI.

- Posting of scene photos on social media. Remember even off duty the public sees you as a representative of the Fire and Rescue Department.
PPCR Copies

- Who should get a copy of my patient’s PPCR?
  - The AIC in charge of patient care.
  - The hospital chart.
  - The person doing QA either at the hospital or for the agency providing care.
  - **Personnel not directly involved in patient care, QA, or billing are not permitted access to the patients PPCR.**

- For example:
  - If I transport in a ambulance from a different agency but no representatives from that agency rides on the call then they are not covered and can not obtain that patient’s PPCR.
Unsure About Discussing an Incident??

Ask yourself...

- Would a Judge agree that the disclosure benefited patient care AND was performed with the utmost discretion??

- If you were the patient, would you want an “embarrassing” injury or illness to be discussed?
Notice of Privacy Practices (NPP)

- The Department must make a Good Faith attempt to provide a NPP to each patient.

- The Department must also make an effort to get a signed “Acknowledgement of Receipt.”
Notice of Privacy Practices

- Any department that charges for service needs to give a NPP to every patient that is transported, including a signature form which acknowledges receipt and permission to bill insurance on the patient’s behalf.

- Every career and volunteer member of the Department must review and be familiar with this material.

- An example can be viewed on the next two slides.

- The NPP is also available on the internet at www.warrencountyfire.com.
During the emergency treatment of a patient, the NPP must be given as soon as practical as detailed in 45 CFR 164.520 of the privacy rule.

Providers may provide this information after the transfer of patient care at the receiving facility.

This ensures that the provision of this information does not interfere with patient care or become lost during the emergent phase of treatment. If after transfer of care it is still not feasible to present the patient with the NPP, then the EMS Provider may leave it with the assigned nurse to present when it is feasible.
Permitted Disclosures

Disclosure of PHI is acceptable in the following circumstances (contact Rick):

- Treatment
- Payment
- Operations
- Public Health Regulations
- Victims of Abuse
- Judicial Proceedings
- Law Enforcement
- Births and Deaths
- Research
- Protection of Public Safety
Treatment, Payment, and Operations

- Treatment – giving PHI to other providers involved in patient care, such as the hospital.

- Payment – receiving PHI from other providers, as necessary for billing.

- Operations – audits, quality assurance assessments.
Public Health Activities

- Disclosures to public health authorities, as authorized by State Law.
- Also allows for notification of communicable diseases to EMS providers involved in an exposure.
The law requires (and HIPAA allows):

- Reporting an “endangered adult” believed to be a victim of battery, neglect, or exploitation to Adult Protective Services or law enforcement.

- Reporting a child that is believed to be a victim of abuse or neglect to the immediate supervisor, Child Protective Services, or law enforcement.
Disclosure must only be made when a Judge or Grand Jury orders disclosure through a subpoena or warrant.

**A private attorney does not have the authority to order a Fire Department provider to discuss a case. If contacted by an attorney, always contact the your county’s law office for advice before proceeding. An Authorization For Release of Medical Information is required to be signed by our patient/their client**
Disclosure of PHI to Law Enforcement is permitted when:

- Required by law.
- Ordered by a court.
- Ordered by Administrative Subpoena.
When assisting the police to identify or locate a suspect, missing person, or witness, the provider may release:

- Name / Address
- Date / Place of Birth
- Social Security #
- Blood Type
- Date / Time of Treatment
- Distinguishing characteristics – height, weight, tattoos, scars, etc...
Law Enforcement
Decedents

- In the Commonwealth of Virginia local law enforcement is required to respond to any unattended death and will conduct an investigation.

- You may request Law Enforcement anytime you feel an attended death is “suspicious” in nature.

- You may release PHI to alert law enforcement of a patient’s death, IF the death may have resulted from criminal activity.

- You are not required to make a “legal conclusion” that the death resulted from a crime.

- Only a “suspicion” is required.

- Note: there is a general exception for releasing PHI to coroners and funeral directors for non crime-related deaths.
As patient care advocates, EMS Providers should encourage law enforcement to gain information directly from the source, when possible.
Civil Penalties

The U. S. Department of Health and Human Services may impose civil penalties on a covered entity of $100 per failure to comply with a Privacy Rule requirement.
Criminal Penalties

- A person who knowingly obtains or discloses individually identifiable health information in violation of HIPAA faces a fine of $50,000 and up to one-year imprisonment.

- The criminal penalties increase to $100,000 and up to five years imprisonment if the wrongful conduct involves false pretenses, and to $250,000 and up to ten years imprisonment if the wrongful conduct involves the intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm.

- Criminal sanctions are enforced by the U. S. Department of Justice.

You and your partner respond for a neighbor who suffers from depression. You discover during your assessment that the patient has had suicidal thoughts. After the call, you are concerned that other First Responders in your community need to know the extent of the patient’s illness so they can watch for warning signs should the depression deepen.

Can you share what you have learned with your fellow First Responders?
No, this is a breech of confidentiality.
There is a call in your town. It involves the treatment of an entrapped farmer who subsequently dies from his injuries. You are concerned that a Critical Incident Stress Debriefing might lead to a violation of HIPAA. Should you be concerned?
Answer

- No, a Critical Incident Stress Debriefing is held with only those providers involved in the call. The rules of CISM is that everything said at the debriefing is confidential.
You are in charge of presenting a CE session for the monthly meeting of First Responders. You want to share some of the details of a recent call, but you are concerned you will be in violation of HIPAA because the patient is a resident in your town.

Can you do case review as education? If so, what precautions should you take to protect the patient’
You can use the details of the call as education as long as you do not give out identifying information such as name, address, etc.
HIPAA

Scenario Four

The First Responders in your fire department routinely use a break room in the station to fill out their paperwork. The room is not secure. How can you ensure that confidentiality is not compromised?

Can you work on paperwork while non-FRs are in the room?
• If you are working on EMS First Responder paperwork, you need to be sure to put everything away when you are done. Do not leave call reports with confidential information on the table where anyone can pick it up. You can work on paperwork with non EMS personnel in the room, but do not share the information with them.
HIPAA
Scenario 5

- You have just assisted with your first field delivery of a newborn. You are so excited you post it on Facebook with pictures from your cell phone. Can you do this and still comply with HIPAA?
Answer

- No. Putting information about EMS calls on Facebook is a breech of confidentiality. Even if you use no names it would be very easy in a small community for people to figure out who the mother and child are.
Take-Aways:

- Rick Farrall is the WCFR HIPPA Officer; contact Rick with any PHI or HIPPA questions

- WCFR 2014 Notice of Privacy Practices located:
  - Warren County Fire and Rescue Administration
  - Warren County Fire and Rescue Fire Manager
  - Warren County and Rivermont Ambulances
  - Warren Memorial Hospital EMS Room

- Always safeguard your patient’s Protected Health Information; share ONLY with those directly involved in their emergent care (scene to E.R./transfer of care)