EMS IN THE AGE OF PHI

Topics covered

- HIPAA
- FIPA
- Other Laws regulating PHI

- Who must comply?
- How to comply?
- What to do in case of breach?

HIPAA –FLORIDA LAW

- Prior to HIPAA there was no uniform standard for medical privacy laws.
- HIPAA provides a consistent set of laws for all 50 states.
- HIPAA is the “floor” not the ceiling.
  - HIPAA would preempt a state law that is “contrary” to HIPAA unless the state law in question is more stringent than HIPAA with regard to privacy protections (45 CFR 160.203(b)).
  - There are a number of Florida laws that, while not “contrary” to HIPAA are more stringent than HIPAA and must be followed.

What is HIPAA?

- "HIPAA" stands for the Health Insurance Portability and Accountability Act of 1996
- Designed to regulate questionable policies and practices of health maintenance organizations
- Created *privacy practice* standards that the healthcare worker must follow

Why is it needed?

- Provides patients with legal rights and voices in how healthcare groups/companies use the protected health information (PHI)
- Other areas of HIPAA include ***"security requirements"*** for computer storage and transmission of healthcare data along with insurance claim "transaction ***requirements"***

Florida Information Protection Act of 2014

- SB 1524 – "Florida Information Protection Act of 2014" was signed into law by Governor Scott on June 20, 2014 and went into effect on July 1, 2014.
- Applies to Gov'tal and Non-Gov'tal entities:
  - Take reasonable measures to protect and secure personal information in electronic form;
  - Notify Dept of Legal Affairs of certain data security breaches;
  - Provide notice of breaches to individuals and others;
  - Properly dispose of consumer records;

Florida Information Protection Act of 2014 §501.171, F.S.

- Who does FIPA protect?
  - FIPA's purpose is to protect consumers by requiring certain entities to take reasonable measures to protect and secure data in electronic format that contains personal information.
- Who is required to adhere to FIPA requirements?
  - Businesses and government agencies that acquire, maintain, store or use the personal information of a consumer - this includes Health Information .

FIPA Key Terms

- "Personal Information"
  - An individual's first name or initial and last name in combination with any ***one*** of the following data elements:
    - Social security number;
    - DL or ID card number, passport number, military ID number or other similar government ID used for identification;
    - Financial account number (credit/debit card) in combination with any required security code, access code, or password needed to permit access to the account;
    - Any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional;
    - Health insurance policy/subscriber

Enforcement

- Violation of FIPA will be treated as an "Unfair or Deceptive Trade Practice" under 501.207, F.S.
  - Declaratory Relief
  - Actual damages caused by the practice
  - 501.207(3), F.S. remedies
- Additionally violations of provisions relating to individual and department notice are subject to additional penalties.
  - $1,000 for each day up to the first 30 days following any violations and $50,000 for each subsequent 30 day period up to 180 days.
  - If violation continues for more than 180 days, an amount not to exceed $500,000.

Violation of HIPAA

- Civil penalties for violation of HIPAA regulation include *fines*
  - *acted without knowing what you were doing was wrong*
- Criminal penalties can include ***fines and jail***
  - *knowing what you were doing is wrong and tried to get profit from it*
- Enforcement *targets the healthcare provider* and agency

No private right of Action for HIPAA / FIPA Violations

SO WHAT's THE BIG DEAL ANYWAY??

Financial risks are real (Recent OCR enforcement actions)

2016 NY Presbyterian pays $2.2 million after allowing ABC TV show to film 2 patients without consent

2015 Raleigh Orthopedic pays $750,000 for failing to have business associate agreement in place

2014 Skagit County, Washington pays $211,000 after compromise of 7 patients' information and potential exposure of 1,500 others via open server

Who Must Comply with HIPAA ?

- Healthcare providers that *charge* for services including EMS agencies. Those who do not charge such as Fire Departments, Vol. Rescue Squads & law enforcement are not covered.
- Local governments who operate EMS are considered "hybrid" entities. EMS operations are covered by HIPAA but not other governmental functions. Its important keep EMS operations separate and establish policies and procedures.
- Companies & individuals acting on behalf of such groups/agencies, more commonly called *"Business Associates"*

How does HIPAA Impact EMS?

- Regulations affect how EMS personnel use & transfer protected health information (PHI)
- Requires EMS to give patients a Notice of Privacy Practices and obtain a signed acknowledgment if possible. The NPP explains how patient information is protected.
- Requires EMS agencies to appoint a *"Compliance Officer"* & create Policies and Procedures.
- HIPAA mandates training of EMS personnel and administrative support staff

Patient Privacy / HIPAA

- What is PHI?
  - Individually identifiable information dealing with past, present, or future physical or mental health care or payment that is created by or received by a health care provider.

  - Forms of PHI include:
    - Oral
    - Written
    - Photographic
    - Electronic / Digital

Patient Privacy / HIPAA

- Obligations of the provider:
  - Respect the privacy of the patient's information as you would your own.
  - Do not share PHI with others not involved in patient care except as permitted.
  - Keep disclosures to the "minimum amount necessary". This applies to outside disclosures of PHI and internal use of PHI.
  - Implement safeguards to protect PHI such as password protection on computers and encryption technology.

Knock Knock!
-Who's there?
HIPAA!
-HIPAA who?

I can't tell you that.

someecards
user card

Other Florida Laws prohibiting / limiting disclosures

- 456.057(7), F.S., (Consent for payment)
- 395.3025, F.S., (Consent for payment)
- 381.004, F.S. (HIV Test Results)
- 394.4615, F.S., (Behavioral Health)
- 397.501(7), F.S., (Substance Abuse) (42 CFR Part 2)
- 384.29, F.S., (STD)
- 760.40, F.S. (Genetic Information)
- 490.147, F.S., and 491.147, F.S., (Psychology and Counseling Services)
- 401.30, F.S., (EMS)

Treatment, Payment and Health Care Operations "TPO"

- 45 CFR 164.502(a)(1)(ii) and 45 CFR 164.506(c)(1-2) allows the use and/or disclosure of medical information ("PHI"), without written consent for treatment, payment or health care operations.
- However some Florida laws would be considered to have more stringent requirements than HIPAA and would require the patient's written consent prior to the release of information for TPO.

Patient Privacy / HIPAA

- Permitted uses of PHI:
  - Treatment
    - PHI may be freely shared with other health care providers who are also responsible for treating the patient.
    - Minimum necessary rule does not apply to treatment related disclosures.
  - Payment
    - PHI may be used to file claims for reimbursement with insurances and bill patients.
  - Health Care Operations
    - PHI may be used for Quality Assurance / Continuous Quality Improvement or Training following the minimum necessary rule. Do not disclose more information than necessary to perform the function.

Patient Privacy / HIPAA

- Protecting PHI
  - Dispatch and Response
    - PHI can be shared over the radio with responding agencies as needed for appropriate treatment purposes.
  - On Scene
    - PHI can be discussed with first responders or other on-scene providers.
    - Limit discussion with family members and friends, unless needed to treat the patient or disclosure is in the patient's best interest.
    - Do not discuss with Media or other third parties.
    - Minimize incidental disclosures.
  - Enroute to the Hospital
    - PHI can be shared as needed for appropriate treatment purposes.
    - Use secure communication methods when appropriate / available.

Patient Privacy / HIPAA

- Protecting PHI
  - At the Hospital
    - Verbal report and Written PCR may be given to hospital staff involved in caring for the patient. Minimum necessary rule does not apply.
    - You may obtain a face sheet from the hospital for the patient.
    - Take care to minimize incidental disclosures.
  - After the call
    - Discussions in the station, quality improvement activities, and CISD is all permissible. However, the minimum necessary rule does apply – limit disclosures as much as practical.

PHI – Family & Friends

- HIPAA permits your agency to share information with family members, friends and others involved in the patient's care or payment for that care when it would be in the patient's best interest. 45 CFR 164.510(b)
- When the patient is competent and able to make healthcare decisions, healthcare professionals should obtain patient's agreement to share health information or give an opportunity to object. If the patient cannot make medical decisions because of a physical or mental reason, then your agency may disclose PHI if it believes it is in the best interests of the individual in the exercise of its professional judgment.
- This is a lot easier to determine while care is being provided but may be trickier when family members call after care has been provided seeking records of other family members. Beware!

Disclosure with consent
HIPAA Patient Authorization Requirements

- Description of the PHI to be used or disclosed
- Name of the person(s) authorized to make the requested disclosure
- Name or identity to whom the disclosure may be made
- Purpose of the requested disclosure (“at the request of the individual” is sufficient)
- Expiration Date
- Signature and Date

Disclosure – Other than TPO

- 45 CFR 164.512 – Disclosure w/o consent (Non-TPO)
  - As required by law;
  - Public health activities;
  - Victims of abuse and neglect;
  - Health oversight;
  - Judicial and administrative;
  - Certain law enforcement activities;
  - Notification of decedents;
  - Organ donation;
  - Certain research purposes;
  - Avert serious threat to health or safety;
  - Specialized government functions;
  - Worker's Compensation.

For guidance visit www.hhs.gov

Discovery Issues
Subpoenas & Qualified Protective Orders

- HIPAA permits a Covered Entity to disclose PHI in response to a subpoena **if** the Covered Entity has received satisfactory assurance that reasonable efforts have been made by the party requesting the information to notify the subject whose PHI is being disclosed.
- Covered entities may also disclose PHI in response to a qualified protective order provided that a written statement and accompanying documentation are received demonstrating that: The parties have agreed to a qualified protective order from the court or administrative tribunal or the parties have requested a qualified protective order from the court or administrative tribunal.

Patient Privacy / HIPAA

- Protecting PHI
  - Disclosures to Law Enforcement
    - HIPAA greatly limits disclosures by EMS to law enforcement.
    - EMS personnel are patient care advocates – not law enforcement tools.
    - Permitted disclosure:
      - A police officer who is a medically trained First Responder was on scene assisting with patient care. The police officer needs additional information to complete their PCR.
      - Mandatory reporting cases such as abuse, neglect cases
    - Restricted disclosure:
      - A police officer stops by the station and asks for a copy of a PCR from a vehicle crash.
    - Law enforcement have appropriate channels to request this information if needed for a report.

- **Disclosures Required by Law**: If your state law requires you to make a certain disclosure, then its permitted under HIPAA. For example, some states require EMS providers to notify law enforcement of gunshot wounds, burn injuries or child abuse. This would also permit you to release PHI in response to subpoenas and search warrants. Check your state laws.
- **Disclosures for Identification and Location Purposes**: Under HIPAA, covered entities may disclose a limited amount of PHI in response to requests to identify or locate a missing person, material witness, suspect or fugitive.

- **Disclosures Regarding Crime Victims**: EMS providers may release PHI pertaining to a crime victim based on request if the patient agrees (even verbally) to the disclosure. If the victim is incapacitated, the disclosure is permissible if you determine its in the patients best interests, and law enforcement officials document that they need the information immediately and don't intend to use it against the victim.

- **Disclosures Regarding Reporting Crime in Emergencies**: An EMS provider may disclose PHI to alert law enforcement to the commission of a crime, as well as the location of the crime victim, and provide information about the perpetrator. For example, if you arrive on scene and find an enraged male and a female patient who's the apparent victim of an assault following a domestic dispute, its permissible to notify the police of the situation, provide the address, request a law enforcement response and provide information about the alleged perpetrator.„

- **Disclosures Regarding Decedents**: EMS providers may release PHI to the police when it appears that a person died as a result of a crime.
- **Disclosures Regarding Crime on Premises**: An EMS provider may disclose PHI regarding a crime that occurred on their premises, including an ambulance. For instance, if a crewmember is assaulted by a patient, this exception would permit you to share all information necessary to report the crime.

Case Scenarios

- Pt. walking across intersection is hit by car at 55 MPH. The vehicle was involved in MVA just prior to striking the pt.
- EMS, Fire, Police & SPD all have responded
- Pt has multiple injuries, is unresponsive, open Fx both legs, with lots of bleeding and vitals are deteriorating

Case Scenario

- Fire & Police on scene first
- Fire starts treating pt. in front of many bystanders that were helping the victim

- ***<u>Did a HIPAA violation occur?</u>***

Scenario

- No – First responders need to treat pt. in the environment found, no reasonable measures could be taken to assure privacy
- Ambulance arrives, crew goes to pt. The first responder gives a detailed report to the crew in front of bystanders and Police.
  - ***Did HIPAA violation occur?***

Examples

- NO – First responders need to give report to the crew

- The crew loads the pt into the ambulance and starts treating pt.
- A few minutes later a firefighter brings a priest over that says he know the pt.
- The priest ask about pt condition and ask if the pt is going to die?
- Is this a HIPAA issue?

Example

- YES – The information request means PHI would be given out. The relationship between pt and priest would have to be verified. Proceed with caution, minimum necessary information requirement in place

- A few minutes later a Police officer brings an obviously upset woman to the rig who states that is her son and ask will he live and what is his condition?
- Is this a HIPAA issue?

Example

- Yes -The information request means PHI would be given OUT. The Police say yes this is his mother, proceed with caution again in what information you share and determine whether disclosure is in the patient's best interest.
- You leave the scene with pt. You give a radio report to MC with PHI exchange.
- Is this a HIPAA issue?

Example

- No & Yes – PHI is given out, generally pt ID is not given over radio. If that is needed or requested via MC use a cell phone

- You arrive at Hospital and you transfer care over to them. While writing your PCR a crew member from another department (apparently looking over your shoulder), states “WOW” that was a bad one, huh?
- HIPAA issue / violation?

Example

- Yes – Only crew members directly involved with the call, supervisors or other administrative personnel should be reading PCR's.
- Police officers on the scene and at the hospital requested certain information including pt identity and condition. They are requesting this information as part of a potential fatality investigation
- Is it a HIPAA violation to provide this information?

Example

- NO
- In this case of a potentially fatal MVC, providing the Police with certain information for the investigation is appropriate. This is limited "minimum necessary information requirement".
- Several weeks later you are contacted by patients attorney, who wants to talk with you about the incident and pt injuries.
- Is it a HIPAA violation to speak with this individual?

Example

- Possibly – Confirm ID and make sure he has authorization as the pt. representative. This is better handled with a subpoena for deposition or trial.

When do you need a Business Associate Agreement?

Business Associate – Person (company) who performs or assists in the performance of a function or activity involving the use or disclosure of individually identifiable health information.

Forms for Business Associate Agreement can be found at
www.hhs.gov/ocr/hipaa/contractprov.html
or see the OCR "Business Associate" Guidance

Business Associate Agreement Requirements

- **Establish the permitted and required uses and disclosures of PHI;**
- **Appropriate safeguards to prevent improper use or disclosure of PHI;**
- **Report improper use or disclosure of PHI;**
- **Require agents and subcontractors to follow same restrictions;**
- **Make PHI available for amendment or access;**
- **Provide information related to certain disclosures**
- **Make internal practices available to HHS for compliance review;**
- **Call for the return or destruction of PHI upon contract termination;**
- **Sanctions for breach of agreement**

What if a breach occurs?

Max was shocked and outraged to find cell phone photos of his recent neuter procedure posted on his veterinarian's FaceBook page.

FIPA Breach – HIPAA Breach

- HIPAA Breach definition is much more specific than the FIPA Definition
  - Acquisition, access, use, or disclosure of PHI in violation of HIPAA which compromises the security or privacy of the PHI
  - Has more specific language regarding good faith (***unintentional and/or inadvertent)*** access, use or disclosure of information.
  - Presumes a breach has occurred unless it can be demonstrated that there is a low probability the ***PHI*** has been compromised based on a risk assessment of the at least the following
    - Nature and extent of PHI involved;
    - Unauthorized person who used PHI or to whom the disclosure was made;
    - Whether the PHI was actually acquired or viewed;
    - Extent to which risk to PHI has been mitigated.

FIPA Breach – HIPAA Breach

- Notice that the risk assessment focuses on the risk to the PHI or information as opposed to the risk of financial, reputational, or other harm to the individual.
- Although included in the definition of “Personal Information” rather than the “Breach” definition both FIPA and HIPAA recognized that information that is, in general, encrypted will not be the subject of a breach.

FIPA Requirements – Notice Requirements

- FIPA – Notice to Individuals of Breach
  - If Personal Information was accessed, or reasonably believed to have been accessed, as a result of breach
  - Notice should be made expeditiously as practicable and without unreasonable delay, but no later than 30 day after determination of breach unless authorized.
    - If requested in writing by federal, state or local law enforcement, notice to individuals may be delayed as specified in the law enforcement request.
  - Notice to individuals is not required if, after and appropriate investigation ***and consultation with relevant federal, state, or local law enforcement agencies,*** the covered entity reasonably determines that the breach has not and will not likely result in identity theft or financial harm to the individual. Such determination must be documented in writing and maintained for 5 years. ***The covered entity shall provide the written determination to the department within 30 days after the determination.***

Compare with HIPAA Notice

- HIPAA – Notice to Individual
  - Shall notify each individual whose unsecured PHI has or is reasonably believed to have been accessed, acquired, used or disclosed as a result of a breach.
  - Notice is to be provided without unreasonable delay but in no case longer than 60 calendar days after breach.
    - Like FIPA there is a law enforcement delay provision, however, if the request is only made orally the delay is not longer than 30 days.
  - FIPA does allow notice to individuals pursuant to rules, regulations, procedures, or guidelines establish by the covered entity's functional federal regulator. So this would seem to allow up to 60 calendar days, however, primary focus should be on notice ***without unreasonable delay.***

Risk of Harm and Notice

- FIPA and HIPAA use different risk of harm methodologies for determining whether a breach requires notice to the individual.
- FIPA focuses on a risk assessment related to the harm the individual (financial and identity theft) whereas HIPAA focuses its risk assessment on the probability that PHI could been (further) compromised.

- Content of Notice to Individuals
  - FIPA and HIPAA are fairly consistent on what information is to be provided to individuals.
- Method of Notice to Individuals
  - FIPA and HIPAA both require written notice to the individual, however, FIPA allows for email notification whereas HIPAA only allows email notification if the individual has agreed to receiving email notice.
  - Both FIPA and HIPAA have similar (but not the same) substitute notice provisions for situations in which contact information for the individual is insufficient.
  - FIPA also has a substitute notice provision for instances in which the cost of notice would exceed $250,000 or in which notice is to made to more that 500,000 individuals. (HIPAA has no similar provision).

- Other FIPA Notice Requirements
  - FIPA only requires notice to media for substitute notice purposes whereas HIPAA requires media notification for breaches involving more than 500 residents of the state.
  - Under FIPA a breach involving more that 1,000 individuals at a single time require the prompt notification of all consumer reporting agencies.

- Notice to the Department and/or HHS
  - HIPAA: Breaches of 500 or more individuals requires notice contemporaneous with notice to individuals
    - Less than 500 required notification within 60 days of the end of the calendar year.
  - FIPA: Breaches of 500 or more individuals require notice to the Department of Legal Affairs. Notice should be provided expeditiously as possible but no later than 30 days after the determination or reasonable determination of the breach. Can get an extra 15 days for good cause.
    - Content of notice to HHS and Department are similar
  - FIPA: Requires, upon request, a copy of a police report, incident report, or computer forensics report.
    - Also requires policies regarding breaches and corrective actions.

3rd Party Agents and Business Associates

- 3rd Party Agents are the FIPA equivalent of Business Associates under HIPAA. Like the Business Associates, 3rd Party Agents have certain responsibilities relating to the maintaining the security of personal information.
- 3rd Party Agent Notice Requirements
  - Required to notify covered entity no later than 10 days following the determination or reasonable determination of a breach.
  - Must provide covered entity with all information needed to comply with notice requirements.
  - May provide notice for covered entity but covered entity is responsible for failed or insufficient notice.

?? QUESTIONS ??