

AAA HIPAA WORKSHOP
*“THE TYPICAL AMBULANCE
CALL”*



www.pwwemslaw.com

Copyright 2003, Page, Wolfberg & Wirth, LLC. All Rights Reserved.

Congrats to Steve Wirth!

The Newest Member of the CAAS
Panel of Commissioners!

Before we get to “the typical
ambulance call” . . .

. . . some *new* HIPAA news!

Final HIPAA Security Rule

- Requires technical, administrative and physical safeguards to protect electronic PHI
- Data backups, recovery plans, access control, password protections, authentication, encryption, evaluation, training, etc.
- Rule divided into “required” and “addressable” provisions

Compliance Deadlines Security Rule

- Final rule published in February 20, 2003 Federal Register
- Effective date: April 21, 2003
- Compliance date: April 21, 2005

Common Station Banter:

“Hey, did you hear about that call last night at 123 Main Street? That patient, Waylon Yelp, was really messed up! Let me tell you what happened....”

**Common Billing Office
Banter:**

“Oh my gosh . . . You won’t believe what this patient did to himself, come here, you guys HAVE to read this run report!”

**What Are Your Primary
Obligations?**

Follow the “The Golden Rule” of
HIPAA!!

**Remember
The “Golden Rule” of HIPAA:**

What You See Here
What You Hear Here
When You Leave Here
Let It Stay Here!



Your Primary Obligations

- Don't share PHI with others who aren't involved in the patient's care, except when permitted or required by HIPAA

Your Primary Obligations

- Limit PHI disclosures to the "minimum necessary" to get the job done BUT NOT WHEN IT COMES TO Treatment Information!
- TREATMENT = Disclose everything you need to disclose!

Your Primary Obligations

- Take reasonable steps to minimize "incidental disclosures"

**The Three Basic
Permitted Uses of PHI**

1. **T**reatment
2. **P**ayment
3. Health Care **O**perations

Treatment

- You may freely share PHI with other health care providers who also treat the patient
- On scene agencies, hospitals, nursing homes, etc.

Payment

- You may use PHI to file claims with payers and send bills to patients
- You may obtain PHI from facilities and other providers for payment purposes
 - “Minimum Necessary” Rule Applies

Health Care Operations

- Includes QA/QI and certain management functions
 - “Minimum Necessary” Rule Applies

Understanding HIPAA

Privacy:

The Typical Ambulance Call



THE BIG QUESTIONS

Can You Use It?

Can You Disclose It?

To Whom Can You Disclose It
and When?

How Do You Protect It?

Dispatch and Response

- Can the dispatch center transmit patient information or PHI over the radio?
 - YES! How else would you know where to respond?!
- Can you share patient information or PHI over the radio with other responding agencies?
 - YES! HIPAA does not prevent oral communications for treatment purposes!

Dispatch and Response

- You are dispatched to a call on Privacy Place. You are having trouble finding the house. Can the dispatcher give you the name of the residence on the mailbox?

Dispatch and Response

- First in ambulance calls on the radio to advise you, the incoming medic unit that they have a 58 y/o patient with chest pain and they provide a list of other complaints and the treatment they have initiated.

Dispatch and Response

- The dispatch center transmits the call information to a printer at the station. The information includes the address and name of the residence, as well as a history of prior calls to that area. Is this acceptable? What should you do with the printout after the call?

Dispatch and Response

- Keep in mind that the dispatch information you receive may contain PHI and thus must be protected or disposed of properly!

Dispatch and Response

- Be sure to document the nature of the dispatch!
 - Example: “dispatched by 911 for a patient with chest pains . . .”
- Important for consideration of: 1) Providing the NPP for HIPAA, and 2) Use of “emergency response” modifier in billing

On Scene

- Can you discuss the patient's condition and share PHI with first responders or other on-scene providers?
- Family members?
- News media?
- Bystanders?

On-Scene

- You may engage in ANY discussions necessary to treat the patient!
- Take care to minimize "incidental disclosures"
- Use common sense approaches!

On Scene

- You are at the scene and you need to get important patient information to your partner who is about 20 feet from you so that he can relay it to the hospital. You are with the patient. There are bystanders and other people standing around, including the news media.

Enroute to the Hospital

- You are permitted to transmit PHI to the receiving facility
- May apprise them of patient condition, etc.
- Again, take care to minimize incidental disclosures
- Use most secure transmission option

Enroute to Hospital

- You are enroute to the hospital with a cardiac patient. You have given all the patient information via med radio. You advised the hospital that the patient had been seen in the ER earlier in the day but was discharged. The hospital asks you for the patient's name.

At the Hospital

- You may (and should!) give your PCR to the hospital
 - The "minimum necessary" rule doesn't apply
- You may give a verbal report to the hospital staff
 - Take care to minimize incidental disclosures, but a sound proof room is not required
- You may obtain a face sheet or billing information from the facility

After the Call

- Discussions in the station?
- Quality improvement activities?
- Reports back from air medical crew?
- CISD?

After the Call

- The incoming shift asks you about interesting calls you had on your shift. The pile of trip sheets are in an open bin on the counter in plain view and the incoming crew leafs through them.

After the Call

- For QA purposes, the supervisor posts on the bulletin board in the crew lounge, a "Trip Sheet of the Month" displaying a good example of a trip sheet for everyone to review.

Billing Questions

- A customer comes into the billing office with questions about a bill. He is brought back into the main billing area (a room full of small cubicles) and is asked to sit at the corner of a billing clerk's desk at one of the cubicles.

Law Enforcement Disclosures

- HIPAA greatly limits the disclosures that EMS personnel can make!
- EMS personnel are patient care advocates, not law enforcement tools
- Permissible law enforcement disclosures are limited to specific situations

Examples

- After an accident call, police officer stops by the station and asks for a copy of your PCR for the patient you transported to the hospital

Examples

- A police officer on scene investigating an accident in which a alleged drunk driver struck a minivan seriously injuring the patient, a young mother and her two children. Police officer asks you her name, extent of her injuries and the name of the hospital you are transporting her to.

Examples

- A police officer asks you if the driver of a car that hit a tree appears to have been drinking and if he said anything to you about if he had been drinking
- A police officer who is a medically-trained First Responder assisting you asks for the patient's blood pressure and pulse to record on the first responder scene report

ON SCENE REQUIREMENTS

- "Notice of Privacy Practices" (NPP)
 - Written document describing patient rights
- Two obligations:
 - 1) Give the NPP to the patient;
 - 2) Obtain signed acknowledgement of receipt in non-emergency situations

	“Emergency Treatment Situations”	Non-Emergencies
Notice of Privacy Practices (NPP)	<i>Provide as soon as practical <u>after</u> the emergency</i>	<i>Provide at or before the time of service</i>
Acknowledgement	<i>No need to obtain it or attempt to obtain it</i>	<i>Must attempt to obtain it and document good faith efforts to obtain it and why it was not obtained</i>

NOTICE

- If Notice could not be furnished, and/or signed acknowledgment could not be obtained, instruct crews to document the reason why
- While there are detailed requirements for the Notice itself, there is no specific type of acknowledgment form prescribed by the regs

Lifetime Signature Authorization

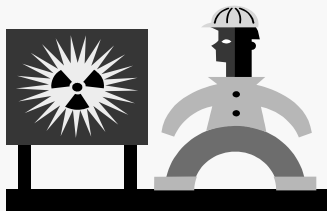
- TIP: You can combine the acknowledgement of the NPP with the insurance signature authorization!
- “I hereby acknowledge receipt of the ABC Ambulance Notice of Privacy Practices”

Can I release PHI in response to a subpoena?

Can I release PHI to provide my required reports to the state?

If state law in my jurisdiction requires me to report child abuse or gunshot injuries, can I still do so?

Safeguarding Patient Information



As Pentagon computerizes medical records, contractor suffers theft

WASHINGTON (Associated Press, 12/31/02)- The Defense Department is computerizing the medical records of all military personnel and their families, but just as the project gets past the experimental phase officials are grappling with the theft of thousands of records from a Pentagon health care contractor. The theft earlier this month of computer hard drives containing more than 500,000 records with Social Security numbers, medical claims histories and other private information from an Arizona company could become one of the largest identity thefts on record if the information is misused, the Federal Trade Commission said.

Safeguarding *Written* PHI

- PCRs should not be left unattended in the open
- PCRs should be maintained in a locked location with limited, role-based access
- Must also safeguard written notes, call intake records, physician certifications, etc. that contain PHI
- Trip sheets and other PHI should not be posted or used as "examples" unless identifying information is removed

Safeguarding *Electronic* PHI

- Implement password protection to computers or networks where PHI is maintained
- Include confidentiality statements on e-mails and fax cover sheets
- Keep fax machines which receive PHI in a secure location and ensure others to whom you fax PHI do the same

Safeguarding *Verbal* PHI

- Use most secure method available to communicate with dispatch, hospital, etc.
 - Example: cell phone vs. VHF radio
- Conduct conversations about PHI with other treatment providers in most secure location available
- Use appropriate voice volume
- No inappropriate banter

Your Service's Policies on Privacy Practices



Service Policies

- Policy on Confidentiality of Patient Information
- Policy on Security, Access, Use and Disclosure of Protected Health Information
- Other policies that the law requires that the Service have in place and enforce

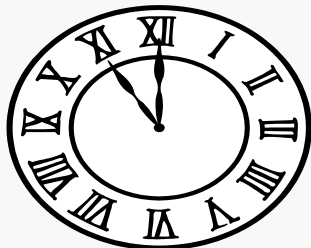
Key Points for Privacy Policies

- “Role Based” Access
- Disclosure of PHI to Others
- Handling Company Requests for PHI
- Verbal Security of PHI
- Physical Security of PHI
- Complaints

Key Points for Privacy Policies

- Penalties for violation
- Privacy Officer role and responsibilities
- Staff member questions on privacy issues
- Complaints from patients

“11th Hour Steps” Toward
HIPAA Compliance



Step One: Appoint a Privacy
Officer

- Devise a job description
- Appoint a person with authority to carry out the necessary tasks to achieve compliance
- The “Go To” Person for Privacy
- Keeper of the Policies and Coordinator of Training
- Ideally should be a member of management
- Must oversee that process is in place

Step Two: Conduct a “Gap
Analysis”

- Identifies how PHI moves through your organization and how it might slip through the cracks
- In broad terms, a Gap Analysis must:
 - Evaluate how you handle PHI
 - Identify how PHI comes into your organization
 - Identify how PHI is handled within the organization
 - Identify who has access to PHI
 - Identify how much PHI they need (“role-based access”)
 - Identify how PHI leaves the organization

Step Three: Identify Your Business Associates

- Mechanisms to identify your business associates
 - Gather and review all existing vendor contracts
 - Examine your accounts payable
 - Examine purchase orders or work orders
- Develop standard BA agreement or addendum with your legal counsel
- Revise your agreements by deadline

Step Four: Identify Existing Privacy Practices and Procedures

- Identify all of the sources of existing privacy-related documents in your organization
 - SOPs or SOGs
 - By laws
 - Personnel manual
 - Memos, policies, etc.
- Compile all policies and procedures in one place!

Step Five: Compile New Policies and Procedures

- Implement NPP, forms and other policies which conform with requirements of final privacy rule
- Must maintain all required documents for possible compliance checks by DHHS
 - Six-year retention period (for HIPAA forms only; does not effect state law medical record retention requirements)
- Have personnel sign off on acknowledgment of your privacy policies
- Establish clear expectations and disciplinary standards for privacy violations

Step Six: Conduct HIPAA Training

- Select a training mode (audio, video, computer based, in person)
- All existing staff must be trained by April 14th and training documented! New staff trained within a reasonable time frame ---includes volunteers!
- Must cover your policies and procedures on privacy practices!

Step Seven: Monitor and Revise Policies as Necessary

- Undertake periodic internal compliance reviews of your privacy practices
- Update policies, procedures, forms and notices as necessary to ensure maximum compliance
- Make sure you are doing what you say you are doing! Put privacy in action!

Training Requirements

- Existing staff before April 14, 2003!
- New staff and ongoing training
- Volunteers, students, etc.



Bottom Line on HIPAA:

- Change the CULTURE of your organization so that you pay more attention to respecting and protecting patients' health care information!
- It is a change in BEHAVIOR as to how you approach the patient's fundamental right to privacy
- As health care providers, EMS is held to the same standards as doctors, nurses, hospitals when it comes to HIPAA

Remember

The "Golden Rule" of HIPAA:

What You See Here
What You Hear Here
When You Leave Here
Let It Stay Here!



HIPAA Compliance
Products from PWW . . .
www.pwwemslaw.com

- **"The Ambulance Service Guide to HIPAA Compliance"**
- **"HPTV: HIPAA Privacy Training Video" for EMS**
- **Spring 2003 National EMS Law Audioconference Series**
 - March 13, 2003 "Role of the Privacy Officer"
