The New HIPAA Regulations –
Taking Patient Privacy to a Whole New Level

Presented by:
Steve Wirth, Esq., EMT-P

July 11, 2013

www.pwwemslaw.com

5010 E. Trindle Road, Suite 202
Mechanicsburg, PA 17050
717-691-0100
717-691-1226 (fax)
IMPORTANT NOTICE FOR SEMINAR ATTENDEES

The information presented in this seminar and these supporting materials does not constitute legal advice or a definitive statement of the law. These materials are for educational purposes only and to provide a general overview of the issues discussed.

The information contained in these materials and discussed at this seminar are subject to change at any time by new laws or regulations, repeals or modifications of existing laws and regulations, court and agency decisions, and in numerous other ways. While our materials are, whenever possible, based on official sources of information from Medicare and other government agencies, you must consult the official sources of materials from those agencies – including regulations, manuals, policies, advisory opinions, etc. – for official statements of the law and government policy. Of course, we cannot be responsible to update these materials for you, nor are we responsible for any documentation, billing, compliance, reimbursement, legal or other decisions you make based in whole or in part upon these materials.

We use examples of documentation, billing scenarios and other teaching illustrations throughout this seminar, and they are just that – examples. Do not use any wording in your own documentation unless it is truthful and accurate.

While we believe the information presented in this seminar and in these materials to be accurate, errors (such as typographical or other content errors) are possible. Ensure that your agency’s legal counsel is aware of any specific legal issues you may have.

All materials are the Copyright of Page, Wolfberg & Wirth, LLC unless otherwise noted. No part of this material may be duplicated, reproduced or distributed by any means. No audio, video and/or digital recording of any type is permitted at this conference.

By attending this seminar, and/or utilizing these materials, you agree to these terms and conditions.
HIPAA and Patient Privacy:  
*The New Wave of Regulations and Enforcement*

Presented by
Steve Wirth, Esq., EMT-P

© Copyright 2013 Page, Wolfberg & Wirth, LLC

---

**WARNING**

The unauthorized reproduction or distribution of this copyrighted work is illegal. Criminal copyright infringement, including infringement without monetary gain, is investigated by the FBI, and is punishable by up to 5 years in federal prison and a fine of $250,000.

---

**DISCLAIMERS**

This information is presented for educational and general information purposes and should not be relied upon as legal advice or definitive statements of the law. Consult applicable laws, regulations and policies for officials statements of the law. No attorney-client relationship is formed by the use of these materials or the participation in this seminar. The user of these materials bears the responsibility for compliance with all applicable laws and regulations.

---

What is HIPAA Anyway?

- "Health Insurance Portability and Accountability Act"
- Federal law passed in 1996
- Specifies what is required to protect the security and privacy of personally identifiable health care information
- Applies to most health care providers, including ambulance services

---

What is HIPAA Anyway?

- Initially intended to allow people to qualify immediately for comparable health insurance = "portability", but...
- Grew into concerns over privacy of medical information (Privacy Rule)
- Specifies what administrative code sets should be used (Transactions & Code Sets Rule)
- Specifies types of measures required to protect the security and privacy of personally identifiable health care information (Security Rule)
- Requires the use of national identification systems for health care patients, providers, payers, and employers (National Identifiers Rule)

---

Page 1

Sign up for our free EMS Law Bulletins at www.pwwemslaw.com
Why HIPAA?

- YOUR concern about the ability to get insurance when you have a preexisting condition!
- YOUR concern about privacy of personal health care information!
- YOUR concern about the use and distribution of your PHI!
- YOUR need for a right to get copies of, inspect, and correct your PHI!
- YOUR right to limit the distribution of it!

How Did We Get Here?

2003
HIPAA Privacy Rule

2005
HIPAA Security Rule

Sept. 2009
Interim Final Breach Notification Rule

July 2010
Proposed Rule with HITECH regulations

2009
Feb. 2009
American Recovery and Reinvestment Act including the HITECH Act

Oct. 2009
Interim Final Enforcement Rule

Jan. 2013
Final "Omnibus" Rule

A Quick HIPAA Refresher . . .

Security Rule vs. Privacy Rule

SECURITY RULE
- Administrative, physical and technical safeguards
- Protection of confidentiality, integrity and availability of electronic PHI

PRIVACY RULE
- Controlling uses and disclosures of PHI
- Granting rights to patients
- Informing patients of your organization's privacy practices

Security Rule vs. Privacy Rule

SECURITY RULE
- Safeguards to protect against unauthorized access, alteration, deletion and transmission
- More limited than Privacy Rule
- Electronic PHI only

PRIVACY RULE
- Broader than Security Rule
- Applies to PHI in any form (electronic, verbal, photographic, etc.)
### Safeguarding Patient Information

**Physical security**
- Store patient care reports (PCRs) in a secure area (locked office, locked cabinet, etc. with limited access) or secure data storage file

**Administrative security**
- Implement policies and procedures, as well as disciplinary standards, to ensure that your personnel protect your patients’ PHI

**Technical security**
- Implement protections such as passwords, backups and other security features on your computers, networks, PDAs, laptops, etc.

### What is PHI?

- **Protected Health Information (PHI)**
  - Individually identifiable or demographic information
    - Name
    - Social security #
    - Condition
    - Address
    - Age
  - Regarding past, present or future physical or mental health or the provision of care to an individual
  - Created by or received by a health care provider
  - Oral or recorded in any form

### Who Are Covered Entities?

- **Health Plans**
- **Health Care Clearinghouse**
- **Health Care Provider**
  - Who transmits any health information in electronic form in connection with a “covered transaction”
  - Claim filing is most common covered transaction, but there are others

### Are We a “Covered Entity?”

- **Health Care Provider**
  - Who transmits any health information in electronic form in connection with a “covered transaction”
  - Claim filing is most common covered transaction, but there are others

---

Sign up for our free EMS Law Bulletins at [www.pwwemslaw.com](http://www.pwwemslaw.com)
Basic HIPAA Requirements  
**IF You Are a Covered Entity**  
- Safeguard PHI  
- Implement “patient rights”  
- Appoint a privacy officer  
- Implement privacy and security policies, procedures and forms

Basic HIPAA Requirements  
**IF You Are a Covered Entity**  
- Train your “workforce” in privacy practices (includes volunteers!)  
- Execute agreements with your “business associates”

Three Basic Permitted Uses of PHI under the Privacy Rule  
1. Treatment  
2. Payment  
3. Health Care Operations  
Permission of the patient is NOT REQUIRED to use PHI for these three purposes

The Big EMS HIPAA Risks . . .

Top Risk Areas for EMS  
- Field data collection devices lost or stolen  
- Paper PHI lost or stolen  
- Talking about patient information with others inappropriately

Top Risk Areas for EMS  
- Improper disposal of paper or electronic PHI  
- Improper access of PHI by those without a need to access it  
- Patient images on “smart phones” and digital imaging devices going everywhere!
And NOW, The Final “Omnibus” Rule

Final Omnibus Rule Overview
- Published: January 25, 2013
- Effective date: March 26, 2013
- Compliance date: September 23, 2013 for CEs and BAs
  - Exception to revise existing BAAs (September 23, 2014)

What’s on the Omnibus?
1. Final HIPAA Privacy and Security regulations from HITECH Act
2. Final HIPAA Enforcement Rule
3. Final Rule on Breach Notification
4. Final Rule modifying HIPAA to include genetic information

What Missed the Omnibus?
- HITECH accounting rules proposed in May 2011
- Guidance on minimum necessary standard (HHS will issue future guidance)

What’s Already Effective?
- Increased CMPs ($100 - $50K per violation)
- Enforcement by state Attorneys General
- Breach Notification to affected patients, HHS and the media
- Breach Notification to Covered Entities

Recent OCR Guidance
- Guidance Regarding Methods for De-identification of PHI
- Guidance on securing Mobile Devices
- Guidance on Risk Analysis Requirements
- Audit Program Protocol

Page 5
Sign up for our free EMS Law Bulletins at www.pwwemslaw.com
Breach Notification Under the Final Rule

Current Breach Rules

- HHS Published Interim Final Rules August 24, 2009
- Effective for all breaches occurring on or after: September 23, 2009

Current Breach Rules

- Upon the discovery of a “breach” of unsecured PHI
  - CE – must provide notice to all affected individuals, HHS and the media for breaches involving more than 500 individuals
  - BA – Must notify a CE of breaches

Current Breach Rules

- The acquisition, access, use, or disclosure of unsecured PHI
- In a manner not permitted under the Privacy Rule
- Which compromises the security or privacy of the PHI

“Compromises the Security or Privacy of PHI”

- Under the “old” rule, this meant: “poses a significant risk of financial, reputational, or other harm to the individual”

The “harm standard”

Say Goodbye to the Harm Standard

Page 6
Sign up for our free EMS Law Bulletins at www.pwwemslaw.com
The New “Presumption Standard”

- Impermissible use or disclosure of PHI is “presumed” to be a breach unless the CE or BA demonstrates that there is a low probability that the PHI has been compromised
- Must go through “risk assessment”

Risk Assessment Factors

1. The nature and extent of PHI involved
2. The person who used the PHI or to whom the disclosure was made
3. Whether the PHI was actually acquired or viewed
4. The extent to which the risk to PHI has been mitigated

Example 1

- An ambulance service intends to fax a PCR to the emergency room at Hospital A. But, the fax number actually belongs to Hospital B. Upon receipt of the misdirected fax, the receptionist at Hospital B contacts the ambulance service and notifies them. The ambulance service directs the receptionist to destroy the PCR.

Example 1

- Likely low probability that PHI improperly faxed was compromised
  - Faxed to another CE
  - Destroyed right away
  - No indication others accessed or retained the information

Example 2

- An ambulance service loses a toughbook with patient records which is recovered a few days later. A forensic analysis by IT shows the PHI was never accessed or otherwise compromised.

Example 2

- Likely low probability that PHI was compromised
  - No evidence that PHI was accessed, viewed, acquired, or transferred as required under breach rules
  - What if the toughbook was never recovered?
    - Password-protected?
    - Encrypted?
Example 3
- A billing company mails a bill containing the date of service, the patient’s name, the patient’s Blue Cross Number, and the level of service to an incorrect address. The wrong individual opens the envelope and then calls the ambulance service.

Example 3
- May be a higher probability that the PHI was compromised
  - An unauthorized individual, not covered by HIPAA looked at the information and could retain it
  - The bill contained the ID number of the patient
  - Chance of medical identity theft

Risk Assessment Must
- Address each factor
  1. Type of PHI
  2. Who saw the PHI
  3. Was the PHI was actually acquired
  4. Extent of mitigation
- Be completed in good faith
- Have reasonable conclusions

May Skip Risk Assessment
- A CE or BA may decide, without going through a risk assessment, to provide notification

What New Standard Means
- May be a lower threshold than the “significant” risk of harm standard
  - Potentially more notifications
- Not a huge change - still have to perform a risk assessment like before
- Must apply new standard as of September 23, 2013

One Clarification to Breach Rules
- CEs required to provide HHS with notice of all breaches involving less than 500 individuals within 60 days of the end of the calendar year
  - The current rule says notice of all breaches “occurring” during that year
One Clarification to Breach Rules

- Final Rule clarifies that CEs are required to notify HHS of all breaches affecting fewer than 500 individuals within 60 days of the end of the calendar year in which the breach was “discovered” not “occurred”
- May be instances where breaches go undiscovered

Breach Action Items

- Encrypt, encrypt, encrypt
- Update breach notification policies
- Train workforce on spotting and reporting breaches
- Involve legal counsel before making assumptions and to ensure you’re doing it right

Enhanced Enforcement Provisions

What HIPAA enforcement looked like, 2003 - 2011

What HIPAA enforcement looks like now
What's Changed?

- The HITECH Act
- The Government’s Enforcement Posture
- Technology
  - Mobile devices
  - Social media

HITECH - Where We're At

- Effective Now
  - Breach Notification Rules for CEUs and BAs
  - Increased penalties
  - State Attorneys General enforcement

Enforcement has Heated Up!

- HHS announces first HIPAA breach settlement involving less than 500 patients - December 30, 2012
- Massachusetts Provider settles HIPAA Case for $1.5 Million - September 17, 2012
- Alaska OTSA Settles HIPAA Security Case for $1,700,000 - June 30, 2012
- HHS settles HIPAA case with Phoenix Children's Hospital for lack of HIPAA Safeguards - April 10, 2012
- HHS settles HIPAA case with BWH for $1.5 Million - March 15, 2012
- Resolution Agreement with the University of California at Los Angeles Health System - July 6, 2011
- Resolution Agreement with General Hospital Corp. & Massachusetts General Physicians Organization, LLC - February 14, 2012
- Civil Money Penalty issued to GunIt Health of Prince George’s County, MD - February 4, 2011
- Resolution Agreement with Management Services Organization, Washington, Inc. - December 13, 2010
- Resolution Agreement with HHS - July 6, 2011
- Resolution Agreement with CVUs, Inc. - January 10, 2010
- Resolution Agreement with Providence Health & Services - July 10, 2008

EMS and Ambulance Services

- HIPAA enforcement is drastically increasing
- Make sure policies and procedures are updated by compliance deadline
- Train staff
- Handle potential breaches and complaints properly

Breach Reporting

- All Breaches Must be Reported to HHS
- Big Breaches are Posted Online

Increased Penalties

- “Violation Occurred after Reasonable Precautions”
  - Minimum Penalty: $100
  - Maximum Penalty: $25,000

- “Violation Resulted from Reasonable Cause”
  - Minimum Penalty: $1,000
  - Maximum Penalty: $100,000

- “Willful Neglect – Corrected Within 30 Days”
  - Minimum Penalty: $10,000
  - Maximum Penalty: $250,000

- “Willful Neglect – Uncorrected Violation”
  - Minimum Penalty: $40,000
  - Maximum Penalty: $1,000,000

© Copyright 2013 Page, Wolfberg & Wirth, LLC

Sign up for our free EMS Law Bulletins at www.pwwemslaw.com
State AG Enforcement

- State Attorneys General can now bring civil actions on behalf of state residents for HIPAA violations
  - Damages on behalf of state residents
  - Enjoin further violations of the HIPAA Privacy and Security Rules

Investigation - New Rule

- HHS “will” investigate any complaint filed when a preliminary review of the facts indicates a possible violation due to willful neglect

“Willful Neglect”

- Willful neglect means conscious, intentional failure or reckless indifference to the obligation to comply with the HIPAA provision violated

45 CFR 164.401

Compliance Reviews – New Rule

- HHS must conduct compliance review where preliminary review of facts indicates possible violation due to “willful neglect”

Mandated Audits

- HITECH Act also required HHS to conduct periodic full scale random audits to ensure compliance with HIPAA
- OCR piloted a program for 115 audits of CEs in 2012
- More to come!

Sign up for our free EMS Law Bulletins at www.pwwemslaw.com
Resolution - New Rule

- HHS "may" attempt to reach a resolution through "informal means"

Gives HHS discretion to proceed directly to a CMP in all cases

Civil Monetary Penalty Amounts

- Interim Final Rule (IFR) significantly increased penalties
- Previous penalty amounts:
  - Up to $100 for each violation, with a total amount not to exceed $25,000 for all violations of the same HIPAA provision in a year

New 4-Tiered Penalty Scheme

<table>
<thead>
<tr>
<th>Violation category—Section 117(b)(1)</th>
<th>Each violation</th>
<th>All such violations of an identical provision in a calendar year</th>
</tr>
</thead>
<tbody>
<tr>
<td>(A) Did Not Know</td>
<td>$100-50,000</td>
<td>$1,500,000</td>
</tr>
<tr>
<td>(B) Reasonable Cause</td>
<td>1,000-30,000</td>
<td>150,000</td>
</tr>
<tr>
<td>(C)(i) With Negligent Corrected</td>
<td>10,000-60,000</td>
<td>1,500,000</td>
</tr>
<tr>
<td>(C)(ii) With Negligent Not Corrected</td>
<td>50,000</td>
<td>1,000,000</td>
</tr>
</tbody>
</table>

Definition of Business Associates (BAs)

- BA is a person/entity who performs functions or activities on behalf of a CE that involves use or disclosure of PHI

Expanding Types of Activities that Make Organizations BAs

Current BA Definition

- BA is a person/entity who performs functions or activities on behalf of a CE that involves use or disclosure of PHI

Sign up for our free EMS Law Bulletins at www.pwwemslaw.com
New BA Definition

- Changes "use or disclosure" to state that a BA is a person/entity who, on behalf of a CE:
  - Creates PHI
  - Receives PHI
  - Maintains PHI, or
  - Transmits PHI

Transmits PHI

- An organization is a BA if:
  1. Provides data transmission services with respect to PHI
  2. Requires "access on a routine basis" to PHI

Access on a Routine Basis

- Not much guidance in Final Rule
- HHS instructs organizations to look to see if the organization is acting as a "mere conduit"
  - If a mere conduit ≠ BA
  - If more than mere conduit = BA

Conduit Exception

- Narrow exception for organizations that just transport PHI and do not access PHI other than on a random or infrequent basis (couriers)
  - U.S. Postal Service
  - UPS
  - Electronic equivalent of these organizations like internet service providers

Conduit Exception

- Ex: Telecommunications company may have occasional, random access to PHI when it reviews whether data is arriving at correct location but this does not make them a BA

Should We Have a BAA?

- If the organization transmits data on your behalf and needs access to PHI should have BAA
  - ePCR vendors
  - Clearinghouses
  - Health exchange organizations

Page 13

Sign up for our free EMS Law Bulletins at www.pwwemslaw.com
Maintains PHI

- An entity that maintains PHI on behalf of a covered entity for a HIPAA function or activity is a BA, **even if the entity does not actually view the PHI**

Maintains PHI

- A data storage company that has access to your protected health information (whether digital or hard copy) likely qualifies as a business associate despite the fact that they may not look at it

Should We Have a BAA?

- Safest practice is to have a BAA in place with any organization that maintains your PHI and might have access to your PHI
  - Cloud servers
  - Any data hosting site
  - Organizations that back up your PHI
  - Physical sites that maintain your PHI

Application of HIPAA Security Rule to Business Associates

New Rule – Security and BAs

- Final Rule directly applies to BAs:
  - Administrative safeguards (§164.308)
  - Physical safeguards (§164.310)
  - Technical safeguards (§164.312)
  - Security policies and procedures (§164.314)

Direct Liability Under HIPAA

- Failure to comply with applicable Security Rule provisions can subject BAs to liability under HIPAA
Business Associate Agreements

Amendments to BAAs

1. Business associate shall comply, where applicable, with the Security Rule with regard to electronic protected health information
   • Many agreements already mandate Security safeguards

2. Business associate shall report breaches of unsecured protected health information to covered entity, as required by 45 CFR § 164.410

3. Business associate shall ensure that any subcontractors that create, maintain or transmit PHI on behalf of the business associate agree to the same restrictions and conditions that apply to the business associate with respect to such information

4. To the extent that the business associate is to carry out covered entity’s obligation under HIPAA, the business associate shall comply with the requirements of the Privacy Rule that apply to the covered entity in the performance of such obligation

BAA Compliance Dates

- CEs and BAs may continue to operate under existing BAAs entered into before January 25, 2013 for up to one year beyond compliance date in Final Rule (September 24, 2014)
  - So long as they complied with old BAA provisions

Page 15
Sign up for our free EMS Law Bulletins at www.pwwemslaw.com
### Fundraising Changes

<table>
<thead>
<tr>
<th>Date BAA Entered Into</th>
<th>Compliance Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Before January 25, 2013</td>
<td>September 23, 2014</td>
</tr>
<tr>
<td>After January 25, 2013</td>
<td>September 23, 2013</td>
</tr>
<tr>
<td>After September 23, 2013</td>
<td>Date on which BAA entered into</td>
</tr>
</tbody>
</table>

### Does it Apply to Me?
- Most ambulance services do not use PHI to conduct fundraising activities
  - Usually use publicly available information
- If you do not use PHI to conduct fundraising, these new rules do not affect you

### Current Fundraising Rule
- A CE can only use PHI to fundraise if:
  - All fundraising materials include description of how an individual may opt out of future communications
  - CE must make “reasonable efforts” to abide by an opt out

### New Fundraising Rule
1. Each fundraising communication that meets the definition under HIPAA must provide a “clear and conspicuous opportunity” for the recipient to elect not to receive future fundraising communications

---

Sign up for our free EMS Law Bulletins at www.pwwemslaw.com
Opt Out Method

- Method for opting out “may not cause the individual to incur an undue burden or more than a nominal cost”
- HHS suggests:
  - Toll-free number
  - Email
  - Or similar mechanism

New Fundraising Rule

2. Individual’s choice to opt out must be treated as a “revocation of authorization” under HIPAA
   - i.e., reasonable efforts will no longer cover it, the CE must absolutely abide by an opt out

If You Use PHI for Fundraising

- Include conspicuous opt out statement in all fundraising communications
- Carefully track opt outs and abide by them

Sample Opt Out Language

"You have the right to elect not to receive any further fundraising communications from ABC Ambulance. Please contact the HIPAA Privacy Officer of ABC Ambulance at 1-800-555-5555 or HC@abcambulance.com if you wish to opt out of receiving future fundraising communications from our ambulance service."

New Marketing Rule

- Like fundraising, most ambulance services do not use PHI to conduct marketing activities
- If you do not use PHI to conduct marketing, these new rules do not affect you

Does it Apply to Me?

- Like fundraising, most ambulance services do not use PHI to conduct marketing activities
- If you do not use PHI to conduct marketing, these new rules do not affect you

Page 17
Sign up for our free EMS Law Bulletins at www.pwwemslaw.com
Current Marketing Rule

- CE may use PHI to make a communication that encourages the recipient to use (or purchase) a service if the communication describes a service that the CE provides
  - i.e., no authorization is necessary if the ambulance service makes a communication about its own services

New Marketing Rule

- A CE must get authorization from the patient before using their PHI if CE receives "financial remuneration" in exchange for making a marketing communication

Example

A dialysis center approaches an ambulance service and asks the service to distribute brochures about its center to all of its dialysis patients. The center offers $1,000 for the marketing campaign. The ambulance service uses clinical information (PHI) to target all ESRD patients.

What About Subscription Programs?

- Not affected by new rule
  - Ambulance services not receiving money in exchange for sending out the subscription communication

Bottom Line

- Rule will not affect most types of communications that ambulance services make
- But, if approached by third party about distributing marketing materials and you have to use PHI, may have to get patient authorization

New Patient Rights
New Restriction Rule

- Gives patients the right to pay out of pocket for a healthcare service and require the CE to not submit a claim to insurance for that service

New Access Rule

1. Grants patients the right to get an electronic copy of their PHI
2. Requires a CE or BA to transmit a patient’s PHI to a third party if requested by patient
3. Caps the response period for access requests

New Access Rule

- If PHI requested is maintained electronically in a designated record set, CE must provide individual with access in electronic form and format requested, if it is readily producible in that form and format

New Access Rule

- If not producible in electronic form and format requested, then must produce in a “readable electronic form and format as agreed to by the covered entity and the individual”

New Access Rule

- HHS expects production of PHI in a “machine readable copy”
  - Word
  - Excel
  - Text
  - HTML
  - PDF

Patient makes request for electronic access to PCR

Does ambulance service maintain the information electronically?

Yes

Ambulance service must provide copy in electronic format requested or, if not available, in an alternate electronic format agreed to by the parties

No

Ambulance service can provide hard copy of PCR to patient

Page 19
Sign up for our free EMS Law Bulletins at www.pwwemslaw.com
Request to Transmit PHI

- A CE is also required to transmit a copy of the PHI directly to another person designated by the patient if requested by patient

Request to Transmit PHI

- Request to transmit PHI must:
  - Be in writing
  - Be signed by the individual
  - Clearly identify the designated person and where to send the copy of PHI
  - An electronic request with an electronic signature is acceptable

Action Steps for Patient Rights

- Make sure you can produce PHI in an electronic format if you store it electronically
- Have a secure way to transmit PHI electronically
- If you store PHI off-site (cloud, storage facility, etc.) make sure you can readily access the PHI

Notice of Privacy Practices (NPP)

- If Notice could not be furnished, and/or signed acknowledgment could not be obtained, document the reason why
- In emergency, Notice can be provided after the fact
- While there are detailed requirements for the Notice itself, there is no specific type of acknowledgment form prescribed by the regulations

The NPP

- Must adopt a detailed “Notice of Privacy Practices”
- Must make good faith effort obtain patient’s signed acknowledgment of receipt of the Notice
- Must post Notice on your web site if you have one

The NPP

- If Notice could not be furnished, and/or signed acknowledgment could not be obtained, document the reason why
- In emergency, Notice can be provided after the fact
- While there are detailed requirements for the Notice itself, there is no specific type of acknowledgment form prescribed by the regulations

Page 20
Sign up for our free EMS Law Bulletins at www.pwwemslaw.com
What do we have to add to the NPP under the new rules?

<table>
<thead>
<tr>
<th></th>
<th>Emergencies</th>
<th>Non-Emergencies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Notice of Privacy Practices (NPP)</td>
<td>Provide as soon as practical after the emergency</td>
<td>Provide at or before the time of service</td>
</tr>
<tr>
<td>Acknowledgement</td>
<td>No need to obtain it or attempt to obtain it</td>
<td>Must attempt to obtain it and document good faith efforts to obtain it and why it was not obtained</td>
</tr>
</tbody>
</table>

What Does the Final Rule Do?

- Mandates several amendments to NPPs to incorporate new patient rights and new HIPAA restrictions

When Authorization is Required

- Must include a statement that patient authorization is required for
  - Sale of PHI
  - Disclosures of psychotherapy notes
  - Marketing (where the CE is receiving payment to make marketing)

Fundraising Opt Out

- If CE intends to contact individuals to conduct fundraising activities that fall under HIPAA (using PHI):
  - NPP must inform individuals of the right to opt out of receiving fundraising communications

Right to Pay Out of Pocket

- NPP must contain provision stating that the patient has the right to request restrictions on disclosures of their PHI when paying out of pocket and that the CE must abide by that request

Page 21
Sign up for our free EMS Law Bulletins at www.pwwemslaw.com
Breach Notice

- Statement informing individuals that the CE has a duty to notify them following a breach of their unsecured PHI

Action Steps

- More guidance could be issued regarding NPP
- NPPs must be updated by September 23, 2013 according to the individual practices of the organization
  - Until then, current NPP is ok

PHI About Decedents

New Decedent Rule

- CEs and BAs only have to comply with the requirements of HIPAA with regard to PHI of a deceased individual for 50 years after the date of death

Disclosures About Decedents to Family Members and Others

New Rule

- CEs may disclose decedent’s information to family members and others who were involved in patient’s care or payment for care prior to death of patient - unless doing so would be inconsistent with patient’s expressed preference that CE knows about
HIPAA and Social Media

Issues

- EMS providers have been in “hot water” and have lost their jobs for what their employer believed were inappropriate images, videos, or comments.

Issues

- Social networking has “revolutionized” information sharing changing the way we work and communicate with each other.

Issues

- EMS agencies – both public and private alike – have a legitimate interest to ensure that social networking is used in a way that does not violate patient confidentiality, harm the organization’s reputation and business interests, or interfere with the work of others.

Issues

- The new “free flow” of information sharing brings legitimate patient privacy and business concerns for the EMS agency.

- EMS providers - have a professional obligation to ensure that social networking is used in a way that does not violate patient confidentiality, harm the organization’s reputation and business interests, interfere with the work of others – and reflects favorably on our professional status!
Simple Advice:

Don’t Post Pictures or Make Comments About Patients!

How would you feel if that patient was a family member, friend or loved one?

*It doesn’t matter that the posting didn’t specifically identify the patient by name! In many communities, the identity of the patient may be well-known to many!*

REMEMBER!

What May Be Someone’s High, May Also Be Someone’s Low

Posting Images of Patients

- Duty under HIPAA to secure and not disclose “Protected Health Information” or PHI
- Any information about a person’s past, present or future health care
- Wide range of media: documents, verbal conversation, recordings, images are included!

Posting Images of Patients

- Improper to post if image can be used to “reasonably identify” the patient

We had a gnarly trauma call last night out on Interstate 80 at Exit 10. Boy was that driver’s head really smashed in. He looked like a road pizza.
Ethical Obligations

- Our patients’ information is not ours to give out
- It belongs to the patient
- Effective health care depends upon trust in the provider-patient relationship

The Father’s Policy...
“I feel they need to come in, do their job, protect the people that are there, do anything they can to help them – not videotape, not do anything of that nature to disrespect that person, whether they are deceased or not.”

Not a Bad Policy for YOUR Organization!

Videos and Photos

- Images can have a place in EMS operations
  - Documenting the scene
  - Documenting mechanism of injury
  - Potential crime scene
  - Documenting unusual circumstances
  - Adjunct to PCR

However . . .

- Videos and photos are included under HIPAA’s definition of “Protected Health Information” (PHI) if they either:
  - Identify the patient
  - Could reasonably be used to identify the patient

Photos and Videos as PHI

- Photos and Videos that identify patients must be protected in the same manner as any other PHI, such as:
  - Patient care reports
  - Hospital face sheets and facility records
  - Physician certification statements
Ways to Minimize HIPAA Issues

- Personal cell phones cameras and recorders should not be used on duty
- If cameras or recorders are used as part of EMS operations, should only be a device issued and owned by the agency

Questions

It’s Coming – Very Soon!

- All the HIPAA forms and policies automatically generated
- Easy-to-follow discussions of all of the new HIPAA regulations

Sign up for our free EMS Law Bulletins at www.pwwemslaw.com
Certificate of Completion

is presented as evidence of completion, by the Certified Ambulance Coder™ whose Signature and CAC™ Number appear below, of the NAAC™ approved Continuing Education course entitled NCAEMS - The New HIPAA Regulations - Taking Patient Privacy to a Whole New Level

Course ID: 948  Vendor Code: 6  Topic Code: 1  CEU Units: 1.5
Education Provider: Page, Wolfberg & Wirth  Presenter: Stephen R. Wirth, Esq., CAC

I hereby certify that I have completed the continuing education training as represented on this certificate.

Signed: _____________________________________________ Certified Ambulance Coder™ Number: ____________________________

Marisa L. Francis  NAAC™ Executive Director

Certificate is invalid without the signature and CAC™ number of the attendee.

7/11/2013  Date of Training
Stephen R. Wirth, Partner
swirth@pwwemslaw.com

Steve Wirth is an attorney and partner, along with Doug Wolfberg and the late Jim Page, of Page, Wolfberg & Wirth, LLC. The firm represents ambulance services, municipalities, fire departments, hospitals, and other organizations across the country in a wide range of medical transportation, reimbursement, compliance, labor and employment, and corporate law issues. Steve has over 35 years of experience as an EMT, paramedic, flight paramedic, EMS instructor, fire officer, and EMS administrator. He recently completed two terms as a member of the Panel of Commissioners for the Commission on Accreditation of Ambulance Services (CAAS), the national ambulance service accrediting body, and served as Chair during his final term.

Steve is a dynamic and frequently sought after speaker at regional, state and national conferences on a variety of EMS, fire service and public safety subjects. He has authored numerous articles and book chapters on a wide range of EMS management, reimbursement, risk management, corporate compliance and workplace law topics. He is a contributing writer for *Journal of Emergency Medical Services (JEMS)*, and *EMS Insider*. Steve co-authored the highly acclaimed *Ambulance Service Guide to HIPAA Compliance* and numerous other popular compliance manuals and video training programs produced by PWW. He enjoys teaching and is an adjunct professor for the University of Pittsburgh and George Washington University EMS degree programs.

Steve graduated *cum laude* from Duquesne University School of Law and was a member of the school’s national trial advocacy competition team. He also has a Masters Degree in Health Services Administration from Gannon University in Erie with an emphasis in organizational behavior. He remains in touch with patient and field provider issues as an active EMT and nationally certified firefighter with Hampden Township Fire Rescue where he serves as Incident Safety Officer and Medical Officer.

Steve is also a life member of the Nippenose Valley Vol. Fire Co. near Jersey Shore, PA where he started his public safety career as a junior firefighter and served as Deputy Fire Chief. He serves on the boards of the Pennsylvania Fire and Emergency Services Institute, the Pennsylvania EMS Providers Foundation, and the Hampden Township Fireman’s Relief Association.