

Privacy Issues in the Physician Practice: It is not your father's physician practice

HCCA Physician Compliance Conference
Philadelphia, PA
October 1-3, 2008

AGENDA

- Brief discussion of HIPAA issues in maintaining privacy.
- Other laws, regulations and requirements that physicians need to think about
 - Payment Card Industry Data Security Standard
 - Other laws
 - State laws, including breach notification
 - Federal legislation

HIPAA- Are you thinking about this?

- HIPAA and
 - Research
 - Notice of privacy practices
 - Minimum necessary
 - Electronic Medical Records
 - Enforcement
 - OCR, CMS and the OIG
 - State law causes of action

3

Research

- Education and re-education
 - Most entities have educated their researchers on the requirements
 - Have you educated your staff on their response when a researcher approaches them?
 - Do you have a good process for monitoring access to your PHI for research?
 - Specifically in an electronic environment
 - What re-education have you done?

4



The Notice of Privacy Practices

- Are your clinical areas actually handing it out?
- Have your registration processes changed?
- Have you reviewed it to see if it matches your practices?
- Does your registration staff know where to find copies of the NPP?

5



Minimum Necessary

- What are you doing to remind staff of this provision?
- With technology changes how are you monitoring the application of minimum necessary?

6

Electronic Medical Records

- If your practice has or is switching to an electronic medical record does it change you current policies and procedures?
 - Role based access
 - Tracking disclosures
 - Tracking receipt of NPP
- Can you track what someone did in you EHR

7

Electronic Medical Records

- Who can access and download information?
 - To a paper document
 - To another electronic device
- Who can run reports?
 - Do they know enough to question a request
- Does the EHR change the way you provide access to information for your patients?

8

Electronic Health Record

- Access from home
 - Do you allow this?
 - Via what type of connection?
 - How do you ensure data does not end up on someone's home computer?

9

Enforcement

- Actions by the OCR, CMS, OIG and DOJ
 - OCR and CMS are still taking a complaint driven approach to enforcement.
 - CMS has hired PWC to conduct security rule audits.
 - Focus in on organizations that have had complaints in the past
 - Physician practices are the area were OCR receives the most complaints

10

Enforcement

- DOJ has had several convictions against individuals for their actions.
- On settlement and resolution agreement with CMS and OCR
 - Hospital paid \$100,000 and has entered a “Resolution Agreement”
 - Looks a lot like a Corporate Integrity Agreement

11

PCI Data Security Standard

- Applies if you store, process or transmit cardholder data
- If you take credit cards it applies to you
- Requires a number of measures for protecting cardholder data

12

PCI standard requirements


- **Build and Maintain a Secure Network**
 - 1. Install and maintain a firewall configuration to protect data
 - 2. Do not use vendor-supplied defaults for system passwords and other security parameters
- **Protect Cardholder Data**
 - 3. Protect stored data
 - 4. Encrypt transmission of cardholder data and sensitive information across public networks

13

PCI standard requirements

- **Maintain a Vulnerability Management Program**
 - 5. Use and regularly update anti-virus software
 - 6. Develop and maintain secure systems and applications
- **Implement Strong Access Control Measures**
 - 7. Restrict access to data by business need-to-know
 - 8. Assign a unique ID to each person with computer access
 - 9. Restrict physical access to cardholder data

14



PCI standard requirements

- **Regularly Monitor and Test Networks**
 - 10. Track and monitor all access to network resources and cardholder data
 - 11. Regularly test security systems and processes
- **Maintain an Information Security Policy**
 - 12. Maintain a policy that addresses information security

15



Other laws

- State laws
 - Breach notification
 - Tort and privacy laws
- Pending Federal legislation

16

State Law Activity

- www.ncsl.org/programs/lis/cip/priv/breach07.htm
- As of 6/20/08
 - 44 states, DC and Puerto Rico have notification laws
- The notification requirement varies widely among states
 - The data that is covered
 - The entities that are covered
 - The notification requirements
- Some states exempt entities that are required to comply with federal privacy laws such as GLB and HIPAA from the notification requirement.
- Many states do not require notification if the data was encrypted.

17

National Activity

- Activities in Congress
 - Legislation in both houses being proposed
 - Areas of contention are the definition of a security breach that would trigger notification requirements

18

Recent Breaches

- January 2007 Emory University notifies 38000 patients
 - Computer stolen from Emory's vendor
 - Theft affected at least four other healthcare providers
- Employee of Mayo Clinic facility in Florida allegedly stole the identity of 1100 patients and sold them to a third party
- VA medical center – information on over 25 million veterans
- www.privacyrights.org/ar/ChronDataBreaches.htm

19

What is being done to avoid breaches?

- Regence Group of the Blue Cross and Blue Shield plans is notifying beneficiaries of the potential impact of lost ID cards.
- New York hospital is issuing smart cards for users that include a PIN.
- Some facilities will only provide services if the patient produces a photo ID.

20

Best Practices

- Notification requirements
 - HIPAA
 - Quasi notification requirement
 - Accounting of disclosure
 - Requirement to mitigate
 - State Laws
 - If not required to report – should you?

21

Decision Making

- Why would you notify?
 - Identify Theft
 - Medical
 - Financial
 - Credit freeze
 - Reputation
 - Organization
 - Individual

22

Decision Making

- Why would you not notify?
 - Cost of notification
 - Individual mailings
 - Other types of notification
 - Cost of credit monitoring
 - Reputation

23

What could it cost your organization?

- Recent reports of theft
 - Emory breach
 - 38000 patients x \$10 per patient = \$380,000
 - 38000 patients x \$30 per patient = \$1,140,000
 - Office of Veterans Affairs
 - Spent millions to hire a consultant to encrypt systems
- Potential state tort liability
 - Will failure to comply with HIPAA be the basis of a negligence action?

24

State Lawsuits

- HIPAA used as best practice:
 - Recent cases
 - Indiana
 - Fall of 2006 Indiana man sues St. Francis Health System for failure of vendor to secure PHI.
 - Seeks class action
 - Oregon
 - Providence Health System breach exposed data of 365,000 patients
 - Patients filing class action lawsuits
 - Illinois
 - Case against hospital regarding employees disclosure of information obtained at work. Employee was at a bar when disclosure occurred.

25

Electronic Health Records and Privacy Concerns

- National E-Health Initiatives
- Regional Initiatives
- EHR/EMR

26



National E-Health Initiatives

- What is happening?
- Will we have a national interoperable health record by 2014?
- Data mining and trend analysis

27



Regional Initiatives

- Louisville
- Kentucky
- Michigan
- Alaska
- Kansas City

28

EHR/EMR/PHR

- Electronic Health Record
 - Full record of the individual's health activities including insurance info
- Electronic Medical Record
 - Full record maintained by a single or multiple providers
- Personal Health Record
 - Record maintained by the individual with potential input from other entities like payors or providers

29

Electronic Health Record Legislation

- Health Information Privacy and Security Act of 2007
- Wired for Health Care Quality Act of 2007
- Independent Health Record Trust Act of 2007
- Technologies for Restoring User's Security and Trust in Health Information Act of 2008 "TRUST in Health Information Act"
- Protecting Records, Optimizing Treatment and Easing Communications Through Health Care Technology Act of 2008 (ProTech)T Act of 2008

30

Health Information Privacy and Security Act of 2007

- HIPAA on steroids
- Would require an “authorization” for TPO
- Requires notification of a breach
- Increases penalties
 - Violation of the individual’s rights \$500 per incident not more than \$5000 in aggregate
 - Improper use or disclosure \$10000 per incident not more than \$50000 in aggregate
 - Allows for a private right of action
 - Would allow patient to opt out of electronic record

31

Wired for Health Care Quality Act of 2007

- Codifies the ONC
- Sunsets ONC 2014
- Creates Partnership for Health Care Improvement
- American Health Information Community
- Facilitation of the widespread adoption of interoperable HIT

32



Wired for Health Care Quality Act of 2007

- Improve the quality of healthcare
- Privacy and Security
- Amendment introduced by Leahy would add significant privacy and security protections to this act

33



Independent Health Record Trust Act 2007

- Health records trust
- Controlled by the consumer
- Data input from a variety of providers
- Trust would be certified by the FTC
- Creates fiduciary duty to patient
 - Breach of duty could result in
 - Loss of certification
 - \$50000 fine and
 - up to 5 years in prison

34

TRUST in Health Information Act of 2008

- ❑ Proposed by Representative Markey (D-MA)
- ❑ Expands scope of entities that would be required to protect health information
- ❑ Codifies many HIPAA provisions in statute
- ❑ Has some provisions that are not consistent with HIPAA
- ❑ Endorsed by the Privacy Rights Clearinghouse

35

Pro(Tech)T Act of 2008

- ❑ Creates grants to encourage Health IT expansion
- ❑ Extends HIPAA requirements to BAAs
- ❑ Requires consent to use or disclose PHI for health care operations
- ❑ Requires notification of a data breach

36

QUESTIONS



37

Contact information

Marti Arvin
Phone: (502) 852-3803
Email: marti.arvin@louisville.edu

38