



HCCA's 12TH ANNUAL COMPLIANCE INSTITUTE

APRIL 13–16, 2008 | NEW ORLEANS, LA | HILTON RIVERSIDE NEW ORLEANS

PRIVACY OFFICER ROUNDTABLE

HCCA



HEALTH CARE
COMPLIANCE
ASSOCIATION

www.hcca-info.org | 888-580-8373

HCCA

2008



**COMPLIANCE
INSTITUTE**

April 13–16, 2008

www.compliance-institute.org

888-580-8373



HCCA's 12TH ANNUAL COMPLIANCE INSTITUTE

APRIL 13–16, 2008 | NEW ORLEANS, LA | HILTON RIVERSIDE NEW ORLEANS

Session Facilitators

Marti Arvin, JD, CHC, CCEP, CIPP/G, CPC
University of Louisville
Privacy Officer

Cheryl Esters, CHC, BS
Compliance Officer
Solano County, California



www.hcca-info.org | 888-580-8373



RULES FOR THE ROUNDTABLE

- First – informal, flexible
- Second – You decide, we can talk at you or we can talk with you
- Third – Please, please put cell phones and pagers on vibrate or turn them off.
- Fourth – Hopefully you can stay for the entire session but if you need to leave we understand. Please do so quietly

PROPOSED AGENDA

- 8:00 – 8:45 When the Rubber Meets the Road
Who is in Charge
- 8:45 – 9:15 EMRs, EHRs, PHRs and Privacy
Concerns
- 9:15 to 9:30 Break
- 9:30 – 10:45 Hot Topics
- 10:45 – 11:00 Break
- 11:00 – 12:00 Open discussion

-
- We have our proposed agenda, BUT what topics do you want to talk about?



Who is on first?

- Who should be responsible for what aspects of compliance when there is a privacy officer, a security officer and a compliance officer?
- How are these positions structured at your organization?
- How do you determine who takes the lead on an issue?

Overlap between Privacy and Security

- Most security issues have a privacy component.
- Many privacy issues have a security component.
- There can be compliance issues that have privacy and/or security components
- Where do you draw the line?
- Methods for success.

Methods for Success

- Develop a collaborative relationship
 - Work with your counter part to define how you will handle issues
 - Define who will take the lead
 - Agree to follow-up with each other.
 - Define how reports will be issued
 - Identify reporting relationships
 - Compliance committee
 - Administrative organizational structure

Electronic Health Records and Privacy Concerns

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



National E Health Initiatives

- What is happening?
- Will we have a national interoperable health record by 2014?
- National legislation

Regional Initiatives

- Louisville
- Kentucky
- Michigan
- Alaska
- Kansas City
- Indiana
- Cal RHIO
- Santa Barbara - defunct



EHR/EMR/PHR

- National group established to define EHR/EMR and PHRs
- Electronic Health Record
 - Full record of the individuals 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

Why is important to understand this?

- Regional and national efforts to establish an interoperable electronic health record are fraught with privacy and security concerns
- There are many, many questions to answer regarding how such a system can be established.

Questions

- Do you inform the individual that his/her medical information is being submitted to the system?
- If yes, is there an opt in or opt out option?
- How do you comply with HIPAA?
- What about the differences between state laws if organization is multi-state?



Questions

- If you are submitting the information for treatment purposes only can it be used for other purposes if it is de-identified?
 - Research
 - Sold for commercial gain
 - Is the individual entitled to any part of the gain?

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
- Health Information Technology Promotion Act of 2006



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

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

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

Independent Health Record Trust Act of 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



Hot Topics

- Discussion of Data Breaches Laws
- Privacy Challenges
 - Authorization does not meet other legal requirements
 - Continual misunderstanding of HIPAA
 - Continual preemption analysis
- Enforcement Rule, OCR and CMS activities

Notification to Patients, Employees and Others when a Data Breach Occurs

- State Law Activity
- National Legislation
- Recent breaches
- Best Practices (not required but should you?)
- Identify Theft

State Law Activity

- www.ncsl.org/programs/lis/cip/priv/breach07.htm
- As of 1/24/07
 - bills introduced in 26 states in 2007
 - Most states have some form of notification requirement
 - Varies by type of data and nature of the organization
 - http://www.dwt.com/practc/privacy/bulletins/03-06_DataBreach.htm (good as of 1/24/07)



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
- Health Information Privacy and Security Act of 2007

What could it cost your organization?

- Recent reports of theft
 - Emory breach
 - 38000 patients x \$10 per patient = \$380000
 - 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?

Recent Breaches

- www.privacyrights.org/ar/ChronDataBreaches.htm
- Dec 2007 Sutter Lakeside Hospital
 - Laptop stolen from employee's home
 - Names and other personal information on approximately 45000 former patients.
- Dec 2007, West Penn Allegheny Health System,
 - Names, addresses, SSNs, phone number and health information on 42000 patients on a laptop stolen from a nurse's home.

Recent Breaches

- Dec 2007 Beacon Medical Services
 - Unknown number of victims
 - Information exposed on a non-secure internet site
- Dec 2007 Memorial Blood Center
 - Records of 268000 donors exposed after a laptop was stolen.
- Jan 2008, Healthnet
 - had a computer stolen with the names and SSNs of employees

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.

Enforcement Rule

- OCR and CMS, what are they doing with complaints?
 - OCR added 3 new investigator positions in December 2007
 - CMS contracted with PWC to conduct security audits
- OCR's privacy investigator
 - Complaint driven enforcement
 - Likely increased fines and penalties

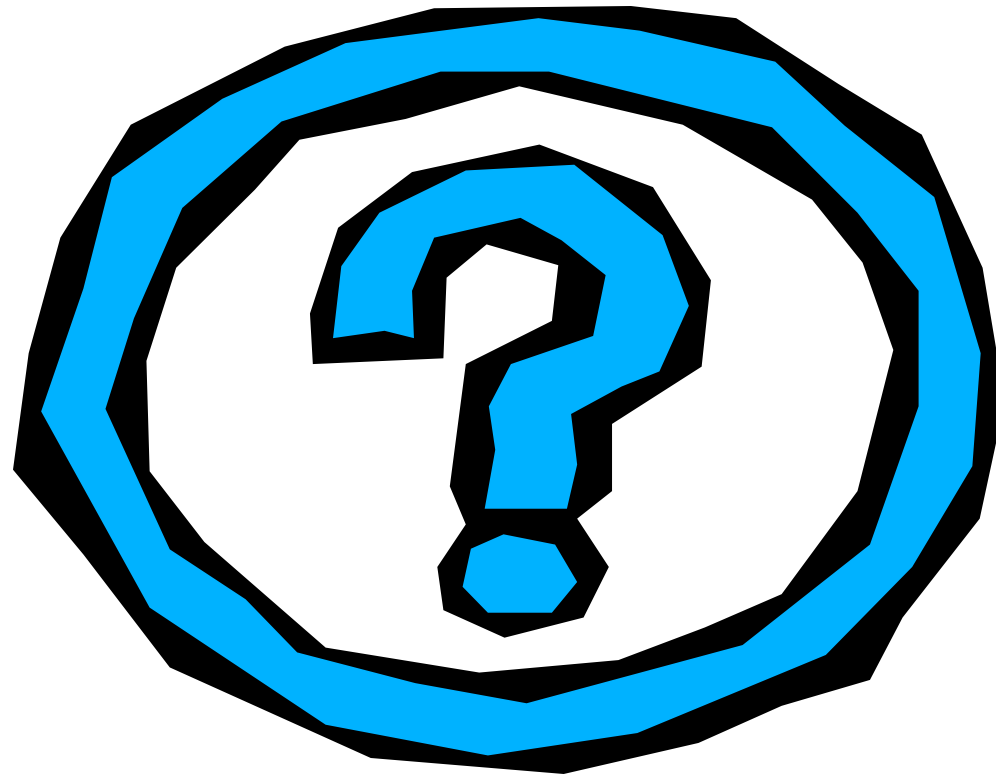
Enforcement

- What are you seeing?
 - Type of complaints
 - Type of patient requests
 - OCR investigations/inquiries
 - P & P revisions:
 - More stringent
 - Less stringent

State Laws

- HIPAA used as best practice:
 - 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 365000 patients
 - Patients filing class action lawsuits

QUESTIONS



Contact information

Marti Arvin

Phone: (502) 852-3803

Email: marti.arvin@louisville.edu

Cheryl Esters

Phone: (707) 784-3199

Email: cdesters@solanocounty.com

