



PRIVACY OFFICER ROUNDTABLE

Session Facilitators

Marti Arvin, JD, CHC, CCEP, CIPP/G, CPC

University of Louisville
Privacy Officer

Deann Baker, CHC, CCEP

Alaska Native Tribal Health Consortium
Compliance and Privacy Officer



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 – 8:20 Introductions
- ❑ 8:20 – 9:00 Discussion of Data Breaches and Notification Requirements
- ❑ 9:00 – 9:15 Break
- ❑ 9:15 – 10:15 Hot Topics
- ❑ 10:15 – 10:30 Break
- ❑ 10:30 - 11:00 Electronic Health Records and Privacy Concerns
- ❑ 11:00 – 12:00 Open discussion



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
 - 35 states have notification laws
 - 10 states have pending legislation
 - 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



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



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.



Best Practices

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



Decision Making

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



Decision Making

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



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?



Hot Topics

- ❑ Enforcement Rule
- ❑ State laws using HIPAA as best practice
- ❑ Employees working from home
- ❑ Telemedicine



Enforcement Rule

- ❑ OCR, what are they doing with complaints?
- ❑ OCR's privacy investigator
 - Complaint driven enforcement
 - Likely increased fines and penalties
- ❑ 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:
 - 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 365000 patients
 - Patients filing class action lawsuits



Employees working from home

- What are adequate safeguards?
 - P&P?
 - Encryption?
- In foreign countries:
 - What are adequate safeguards?
 - How do you enforce?
 - BAA?
 - Encryption?
- CMS guidance document



Telemedicine

- Foreign providers
 - Data in foreign lands
 - Transcription
 - Radiology
 - Agreements
 - jurisdiction
 - enforcement



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?
- ❑ Data mining and trend analysis



Regional Initiatives

- ❑ Louisville
- ❑ Kentucky
- ❑ Michigan
- ❑ Alaska
- ❑ Kansas City



EHR/EMR/PHR

- 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

QUESTIONS





Contact information

Marti Arvin

Phone: (502) 852-3803

Email: marti.arvin@louisville.edu

Deann Baker

Phone: (907) 729-1992

Email: dmbaker@anthc.org