# Is HIPAA Ready for the EHR?
## Practical and Legal Considerations of the Interoperable Electronic Health Record

**Barry S. Herrin, CHE, Esq.**
**Smith Moore LLP**

**The Twelfth Annual HIPAA Summit**
**April 11, 2006**
**Hyatt Regency Capitol Hill, Washington DC**

SMITH MOORE LLP
ATTORNEYS AT LAW

# Extraordinary Focus on EHR

- Financial and e-services industries way ahead of health care industry in customer access and data manipulation

- Technology for EHR exists in many facilities and some physician practices

- AHIMA and e-HIM Initiatives bringing more exposure to potential for EHR adoption and utilization

- Entrepreneurs have figured out you can make money doing this

# Patient Reluctance

- General distrust of "putting my information out there" overcomes acknowledgement that a universal EHR is probably a good idea
  - Harris February 2004 Polling Data
  - Harris February 2005 Polling Data
  - Modern Healthcare/California HealthCare Foundation November 2005 Survey
- Highly publicized information security breaches aren't helping matters
- How do you buy your gas?

# General HIPAA Issues

- Are You Establishing a Separate Legal Entity (RHIO, CHIN)?
- Covered Entity vs. Business Associate
- Organized Health Care Arrangement
  - Definitional Problems
  - No Clear Guidance
- State Law Pre-emption and Other Issues
  - Provider Licensing Statutes/Telemedicine
  - Notice of Privacy Practices

# HIPAA Privacy Concepts Implicated by the Interoperable EHR

- Authorization – 45 CFR 164.502(a)
- Minimum Necessary – 45 CFR 164.502(b)
- Patient Right of Access – 45 CFR 164.524
- Accounting for Disclosures – 45 CFR 164.528
- Physical Security - 45 CFR 164.530(c)
- Verification – 45 CFR 164.514(h)
- Research – 45 CFR 164.512(i)

# HIPAA Security Concepts Implicated by the Interoperable EHR

- Administrative Safeguards – 45 CFR 164.308
  - Access Management
  - Password Management
  - Verification of Risk Analysis/Assessment
- Physical Safeguards – 45 CFR 164.310
  - Access Control and Validation
  - Workstation Use
  - Data Backup and Storage
- Technical Safeguards – 45 CFR 164.312
  - Audit Controls
  - Data Integrity Procedures
  - Verification of Identity of Requesting Parties
  - Encryption

# Practical Issues - Verification

- What protocol to use?
  - Like financial access models?
  - Cookies/select terminal access?
- No requirement for a writing under HIPAA to verify identification
- Patient security concerns <u>must</u> be addressed here
- Sharing of password(s) eliminates audit trail required by HIPAA Security Rule

# Practical Issues – Record Maintenance

- Record retention/destruction standards vary widely by state
- "Sampling" risks
  - Providers
  - Patients
- Who maintains the record?
  - Relates <u>directly</u> to issues of provider trust
  - How are errors corrected and posted?

# Practical Issues – Release to Third Parties

- No Privacy Rule accounting required for authorized releases, but Security Rule requires audit trail
  - How to show <u>unique</u> authorization?
  - HIPAA requires a <u>writing</u> and <u>signature</u>
    - Security protocol and password authentication not the same
  - Authorization must expire (unless it doesn't)
  - Revocations of Authorization
- Authentication of Records – How?/Why?
  - Viewable or Printable? Or Both?

- How Does the PHR Fit In?

# Case Study – "Virtual PHR"

- Web-based tool that provides a "password vault" for an individual's access to multiple provider websites or databases

- Tool accesses the provider website/database, sorts data, and places in a common format for access

- Permits individuals to communicate with multiple providers in the same GUI format

# "Virtual PHR" - Desired Features

- Messaging
- Interaction with Business Offices (pay bills, get statements)
- Pre-registration
- Obtain test results
- Refill prescriptions/track meds/drug interactions
- Request copies of individual provider EHR

# "Virtual PHR" - Current Problems and Limitations

- Patient-only access; shared access only by sharing password, so no HIPAA-compliant audit trail

- Real-time access might release results before they can be explained by a health care provider

- Misunderstandings about patient access vs. third party access overcomplicate the process

- "Hub and spoke" access only; no interoperability

- Patient understanding limited by cultural differences and language barriers

# QUESTIONS?

- Answers?

**Contact Info:**

**Barry S. Herrin, Esq.**
**Smith Moore LLP**
**877-404-7466 x1027**
**barry.herrin@ smithmoorelaw.com**