

**Healthcare Technology &
Privacy
November 9, 2011**

Daniel B. Vukmer
UPMC Health Plan
Stephanie W. Schreiber
Buchanan Ingersoll & Rooney PC

KEY DISCUSSION ISSUES

- Electronic Medical Records
- Privacy Concerns
- HIPAA- HITECH Issues
- Health Information Exchanges

**ELECTRONIC MEDICAL
RECORDS**

- Overview of Electronic Medical Records
- What is an EMR?
- Legal Concerns Associated with an EMR

PRIVACY CONCERNS

- State and Federal Laws Protecting Confidentiality of Health Care Information
- Greater Portability of Medical Information
- Greater Access to Medical Information
- Ability for Wide Range Distribution of Health Care Information
- BUT – Allows for the Potential of More Effective Medical Care

HIPAA 101

- Federal Law – Increased Confidentiality Obligations
- Prohibits Use and Disclosure of Protected Health Information – Other than for Treatment, Payment and Healthcare Operations, Subject to Limited Exceptions
- Allows Greater Access to an Individual’s Own Health Care Information
- State Laws Must Also be Followed if State Law Provides for Greater Confidentiality and Greater Access for Individuals

HIPAA 101 CONTINUED

- HIPAA Obligations Bind Covered Entities
- The Role of a Business Associates
- Obligation to Enter into Business Associate Agreements
- Increased Obligations for Business Associates Under HITECH
 - Additional Rules - Pending

HIPAA EVOLUTION

- Privacy Rule
- Inclusion of Electronic Protected Health Information
- Security Rule
- Transaction Rule – (will not be discussing)
- HITECH ACT OF 2009: Health Information Technology for Economic and Clinical Health Act

COSTS OF A DATA BREACH

- Data Breaches are Costly
- Data Breaches Erode Trust and Create Negative Publicity
- With the Passage Of HITECH Act There is Increased Focus on Healthcare Data Security
- 13.7% of All Recent Data Breaches Occurred in the Healthcare Sector – Popular Target of Hackers
- 41.5% of Hospitals Have 10 or More Breaches a Year

COSTS OF A DATA BREACH

- Average Cost of a Lost Laptop is \$49,246
- Average Data Breach Cost of a Lost Laptop Varies by Industry
 - Services (\$112,853); Financial Services (\$71,820) And Healthcare (\$67,873) Suffer From the Highest Data Breach Costs

COSTS OF A DATA BREACH

- Backup And Encryption Methods Affect the Average Cost of a Lost Laptop
 - Average Cost is About \$30,000 More When There is a Full Backup System
 - > The Backup Makes it Easier to Confirm Loss Of Sensitive or Confidential Data
 - Encryption Can Reduce the Cost of a Lost Laptop by More Than \$20,000

NEW OBLIGATIONS UNDER HITECH

- Extends the Reach of Privacy and Security Protections Beyond Covered Entities
- Imposes Additional Obligations on Covered Entities and Business Associates
- Authorizes Greater Access and Rights to Individuals
- Imposes State Attorney General Oversight and Additional Tiered Penalties

BREACH NOTIFICATION

- HIPAA Covered Entities Must Provide Affected Individuals With Notice of a Breach of Their Unsecured PHI Within 60 Days
- Covered Entity Must Evaluate The Risk of Harm of the Breach Before Providing Notice
- Notice Must Include a Brief Description of the Event, the PHI Involved and the Steps to Take to Protect From Future Harm

BREACH NOTIFICATION

- If Breach Involves More Than 500 Individuals - Covered Entity Must Notify the Media as Well as HHS
- If Breach Involves Less Than 500 Individuals it Must be Reported to HHS Annually

WHAT IS A BREACH

- Unauthorized Acquisition, Access, Use or Disclosure Of Unsecured PHI in a Manner Not Permitted by the Privacy Rule
- Compromises the Security or Privacy of the PHI
- Poses a Significant Risk of Financial, Reputational or Other Harm

WHAT IS NOT A BREACH

- Unintentional Good Faith Acquisition, Access or Use Of PHI (e.g. Nurse Mistakenly Sends a Billing Employee an Email With Patients' PHI)
- Inadvertent Disclosure of PHI From Authorized Person to Another Authorized Person
- Unauthorized Disclosures in Which Recipient Would Not Have Reasonably Been Able to Retain PHI
- Secured PHI
- Use or Disclosure of De-identified Information

**RISK OF HARM
INVESTIGATION**

- Poses a Significant Risk of Financial, Reputational or Other Harm To The Individual
- Covered Entity Must Conduct a Written Risk Assessment
 - Who Used PHI and to Whom was PHI Disclosed
 - Type, Amount And Sensitivity of the PHI Involved
 - Whether the Covered Entity has Taken Immediate Steps to Mitigate
 - Whether PHI was Returned Prior to Access

**HEALTH INFORMATION
EXCHANGES**

- What is a Health Information Exchange or an HIE?

- Overview of an HIE

**HEALTH INFORMATION
EXCHANGES AND PRIVACY**

- **Why have a Health Information Exchange**
 - Provide Safer, More Timely, Efficient, Effective Patient Care
 - Reduce Expenses Associated With Duplicate Tests
 - Help Avoid Missing Patient Data
 - Verify Delivery of Traditional Communications, Referrals and Test Results
 - Avoid Scanning and Faxing of Documents, the Physical Mailing of Entire Patient Charts, and Manual Phone Communication

TYPES OF HIEs

- **Regional Health Information Organizations**
- **Statewide Health Information Exchanges**
- **Nationwide Health Information Network**
- **Community Health Information Exchanges**
- **Hospital Based Health Information Exchanges**

POTENTIAL PARTICIPANTS

- **Who are the Potential Participants:**
 - Providers
 - Payors
 - Patients
 - Other Entities
 - Potential Conflict Issues

LEGAL CONSIDERATIONS

- **HIE Participation Agreements:**
 - Written Agreement
 - Operational Issues
 - HIPAA Compliance
 - Business Associate Provisions
 - Proprietary Information Protections

**ADDITIONAL LEGAL
CONSIDERATIONS**

- **HIE Participation Agreements:**
 - Intellectual Property Rights
 - Software Licensing
 - Insurance
 - Indemnification
 - Audit Rights
 - Breach Issues
 - Dispute Resolution

**ADDITIONAL LEGAL
CONSIDERATIONS**

- **Specific HIPAA Compliance Issues:**
 - Privacy Rule
 - Security Rule
 - Use and Disclosure in Accordance with State and Federal Laws
 - Various Policies and Procedures for Compliance Among Users

**ADDITIONAL LEGAL
CONSIDERATIONS**

- **Minimum Necessary Rules:**
 - Proposed Rule Retains Current Carve-outs for Treatment
 - May Require Standard Protocols for Disclosures
 - Non Treatment Uses
- **Individuals May Request Additional Restrictions:**
 - May request that a covered entity not disclose PHI to a health plan if the disclosure is for payment or healthcare operations (not treatment) AND the PHI pertains solely to a healthcare item or service for which the provider has been paid in full

**ADDITIONAL LEGAL
CONSIDERATIONS**

- **Who Has Access to Information:**
 - Organizational Restrictions
 - Auditing
 - Authentications
 - Patient Access
 - Limited
 - HIPAA Protections
 - Disclosures of Who Accessed Records

**ADDITIONAL LEGAL
CONSIDERATIONS**

- **Identity Management Issues:**
 - Is the Correct Patient Identified
 - Identification Process
 - How Much to Initially Disclose
 - Social Security Numbers and Other Identifiers
 - Search Process
 - Corrections for Wrong Patient
 - Access Disclosures

**ADDITIONAL LEGAL
CONSIDERATIONS**

- **Quality of Information:**
 - Need for Rules Regarding, Timeliness, Accuracy, Reliability, and Comprehension
- **Security Standards:**
 - Uniformity
- **Multi-State Considerations:**
 - Responding to Requests
 - Breach Notification Issues

**ADDITIONAL LEGAL
CONSIDERATIONS**

- **Notifications:**
 - Privacy Notices
 - Consent Forms
 - Opt-In and Opt-Out Forms
- **Patient Education Issues:**
 - Benefits
 - Risks of Non-Participation
 - Address Privacy Concerns

**ADDITIONAL LEGAL
CONSIDERATIONS**

- **Opt-In/Opt-Out Considerations:**
 - HIPAA is Just a Floor
 - State Law Considerations
 - Implied vs. Explicit Model
 - Implied – Opt-out Required
 - Explicit – Opt-In Model – No Consent/No Data
 - Forms to Use for Opt-In
 - Don't Confuse with HIPAA Authorization Form
 - Treatment

**ADDITIONAL LEGAL
CONSIDERATIONS**

- **Opt-In/Opt-Out Considerations:**
 - Technical Considerations
 - Is Data Imported but Hidden
 - Is Data Not Imported
 - Uniform Consents
 - Special Care Used for Heightened Privacy Issues
 - Break the Glass Scenarios

QUESTIONS

- Stephanie W. Schreiber
- 412 392 2148
- stephanie.schreiber@bipc.com

- Daniel B. Vukmer
- 412 454 5618
- vukmdb@UPMC.EDU
