The HIPAA Summit West IV

HIPAA Summit Day II
Afternoon Plenary Session: HIPAA Security

October 5, 2010

John Parmigiani

Summit Co-Chair

President

John C. Parmigiani & Associates, LLC

Agenda

- Important and Emerging HIPAA Security Areas of Concern

- The Featured Speakers and their Topics

Important and Emerging HIPAA Security Areas of Concern…

- Increased Enforcement and Heightened CMPS
- Business Associates and their Subcontractors
- Encryption (???)
- Increased Patient Rights – strengthening the Privacy-Security Connection
- New and developing data environments
  - RHIOs and HIEs
  - Social networks
  - Cloud computing

Important and Emerging HIPAA Security Areas of Concern

- Enhanced federal and state mandatory requirements for data protection and notification in the event of an alleged security breach
- New HITECH Regulations and Guidance
  - Standards
  - Emphasis on risk analysis and risk management as a first step in a secure environment for EHRs and HIE

HITECH Regulations and Guidance

Meaningful Use/Standards & Certification

- **CMS Final Rule Medicare and Medicaid EHR Incentive Programs (Meaningful Use of EHRs)**
  - One of the objectives is to protect electronic health information created or maintained by certified EHR technology through the implementation of appropriate technical controls
    - A measure for this is to conduct or review a security risk analysis per the Security Rule and implement security updates and correct identified security deficiencies as part of the risk management process
- **ONC Final Rule Initial Standards and Certification Criteria for EHRs**
- **ONC Rule on EHR Certification Process**

Privacy, Security, and Enforcement

- **OCR Proposed Rule for new CE and BA HITECH Privacy and Security Obligations and Enforcement Rule (Modifications to the HIPAA Privacy, Security, and Enforcement Rules under HITECH Act)**
  - Integral building block in:
    - The attainment of a fully functioning and complete EHR
    - The exchange of health information (HIE) in a secure environment
    - Strengthening perceived weaknesses in HIPAA Privacy and Security regulatory requirements
- **OCR IFR for Breach Notification for Unsecured PHI (Making PHI Unusable, Unreadable, or Indecipherable to Unauthorized Individuals)**
- **OCR Guidance on Security Rule Risk Analysis Requirements**

Our Speakers and their Topics…

- Ali Pabrai: *Applying NIST, ISO 27000 & PCI DSS to Address Compliance Mandates*
- Deborah Lafky: *The Safe Harbor Method of De-identification*
- Angel Hoffman and Phyllis Patrick: *Security Issues and Solutions Relating to Social Media in HIE*
- Dave Kirby: *Security Issues and Possible Solutions about EHRs and their Relationships to HIE*

Break @ 3:15 – 3:45 pm

- Jason Cuddy: *Security Issues and Solutions Regarding the use of SaaS (Software as a Service)/Cloud Computing/ Virtual Environments*
- Jack Gomes: *The Emerging "Meaningful Use" Security Requirements and How Those Definitions should be Imbedded in Developing Vendor System Solutions*
- Holt Anderson: *Taking the NHIN DURSA to the Community Level: Constructing Consistent Chain-of-Trust Agreements to Protect PHI*

Our Speakers and their Topics

- David Behnifar: *Working Through a breach Notification Analysis from Start to Finish*

End of Security Session ~ 5:45 pm

Thank You !

Any questions before we begin?

John Parmigiani
410-750-2497
jcparmigiani@comcast.net
www.johnparmigiani.com