The Twenty-First National HIPAA Summit

HIPAA Summit Day II
Morning Plenary Session: HIPAA Security

February 20, 2013

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…

- Omnibus Rule
  - Finally (a "Waiting for Guffman" event)
  - HHS: " the need to protect patient information in an ever expanding digital age"
  - Symbiotic relationship between MU and Omnibus
    - Perform security risk assessment/explicitly address encryption
      - Necessary for "attestation" and enforcement (OIG) audits
- Breaches … and the beat goes on
  - More in 2012 than 2011 (21% increase) but fewer patients affected (77% decrease)
  - 538 breaches of 500 or more reported to OCR since 2009
    - 21.4 M records
    - Two-thirds result from theft or loss
    - 38% from unencrypted laptops and portable devices
    - 57% involve business associates

(Redspin 3rd Breach Report/Protected Health Information)

Important and Emerging HIPAA Security Areas of Concern…

- Increased Enforcement Actions (now both small and large breaches}
  - Hospice of North Idaho – a small non-profit
    - First settlement ($50,000) involving fewer than 500 individuals (441)
  - Utah Medicaid (6,000+ patients)
  - Packard Children's Hospital at Stanford University (57,000 patients)
  - Skewed by HHS(OCR) region: 11 settlements to-date nationally, Seattle has 5
  - OCR has now become "an enforcement-oriented culture" with "more assertive enforcement" and the expectation of "more monetary settlements"
    – Leon Rodriguez
    - Striving to have CES, BAs, and subs to BAs to attain and maintain a "culture of compliance"

Important and Emerging HIPAA Security Areas of Concern…

- An increased emphasis on Cyber Security
  - President's Executive Order (2/12/13)
  - Not just PHI but also financial, competitive, and intellectual property data
  - NIST to test tools and technologies/develop a framework to support the exchange of electronic health information
    - All organizations, especially small providers, and EHR users invited
  - NIST has three reports on Cyber-physical systems (for the 21st Century)
    - Strategic R&D opportunities
    - Strategic vision and business drivers
    - Foundations for innovations

Important and Emerging HIPAA Security Areas of Concern…

- Patient monitoring and interaction
  - Patient portals – more dialogue between patients and caregivers
    - Taking place in a secure environment
  - Use of sophisticated sensors, computerized pattern recognition, human responders toward greater surveillance of patients in everyday life
    - Intended to reduce the need for physical visits and to save time and money but there are increasing privacy concerns - -"make them stop looking at me"! or in the words of Sting and the Police: "every breath you take, every move you make, we'll be watching you"
    - Acceptance will be heavily based on patient trust/ intrusion of privacy balance with benefits derived
- HIT in the Cloud
  - Better ROI re resource usage but…how much risk?

Important and Emerging HIPAA Security Areas of Concern…

- Emerging Legislation
  - Regulating how developers of mobile applications, including mHealth, would collect personal data
    - "Application Privacy, Protection and Security (APPS) Act of 2013" (Johnson, D-GA)
    - Growing concern about data collection on mobile devices
    - FTC to be enforcing agency
    - Developers to "prevent unauthorized access to user's data through reasonable and appropriate security measures"
      - Vulnerability of medical systems and devices
      - Intercepting signals and interacting with a patient's device could result in adverse outcomes and death
    - Data mining of EHRs

Important and Emerging HIPAA Security Areas of Concern…

- Emerging Legislation (cont'd.)
  - All covered entities to encrypt portable devices that store PHI, restrict the use of PHI by medical contractors, and require agencies to report any privacy breaches and enforcement actions to Congress
    - "Protect Our Health Privacy Act of 2012" (Fradkin, D-MI)
  - Uniform privacy and security requirements for data protection by states
    - Texas enacted privacy laws in September, 2012 that are broader and more stringent than HIPAA
    - "patient consent" for exchanging PHI in EHRs and HIEs

Our Speakers and their Topics

- Ali Pabrai: *Firewalls to Encryption: Compliance Mandates and Cyber Security*
- Rebecca Williams: *Into the Breach: Breach Notification under the Omnibus Rule*
- Dave Kirby: *Emerging Security and Privacy Feature Needs in EHRs Employed in Academic Medical Centers*

Break @ 10:00 – 10:30 am

- Susan Miller: *NIST HIPAA Security Toolkit*
- Phyllis Patrick: *Information Security in 2016: What will your Program look like?*
- Camilla Brown: *The Changing Roles of HIEs: Impact on Privacy and Security*

Lunch: 12:00 – 1:00 pm

Thank You !

Any questions before we begin?

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