The Twenty-Second National HIPAA Summit

HIPAA Summit Day II
Morning Plenary Session: HIPAA Security

February 5, 2014

John Parmigiani
Summit Co-Chair
President
John C. Parmigiani & Associates, LLC

Agenda

- Important and Emerging HIPAA Security Areas of Concern
  - Threats
  - Issues
  - Enforcement
  - Breaches
  - Possible Legislation
- The Featured Speakers and their Topics

Important and Emerging HIPAA Security Areas of Concern…

Threats (new ones being created daily)

- Cyberterrorism
  - National effort
  - Not just PHI but all sensitive data (financial, proprietary, competitive, intellectual property)
  - BlackPOS - Target, Neiman Marcus, + six other retail stores; Businesses in US, Australia, and Canada – malware developed by 17 years old Russian; malware named Kaptoxa (Russian slang for "potato"), built 40 different versions, sold at $2,000 each and to makers of illegal credit cards; the buyers also modified the code
  - Healthcare data especially attractive for medical identity theft and illegal aliens

- BYOD/Mobile devices
  - More and more data subject to unauthorized access / lost devices

- Business Associates
  - Subcontractors ("Achilles Heel")

Important and Emerging HIPAA Security Areas of Concern…

Threats

- EHR weaknesses
  - OIG on CMS and its contractors for not paying more attention to EHR vulnerabilities that could produce fraudulent records

- HIPAA Security compliance in the "Cloud"
  - Reduced resource requirements but how much risk

Issues

- MU Attestation
  - Security assessments
  - Encryption of stored data ("data at rest")
- Confusion over breach notification
  - How to apply the four factors in assessing a breach
  - Possibility of more breaches being reported

Important and Emerging HIPAA Security Areas of Concern…

Issues

- Securing patient data in a mobilized healthcare environment
  - mHealth technology / Telehealth / Sharing patient data – the maturation of HIEs /Wearable devices
  - Optimizing the balance between patient treatment and patient engagement in their care
    - more dialogue between patients and caregivers
  - MU stage 3 will likely strive to expand more patient-generated data by healthcare organizations, linking patients to caregivers through
  - Patient portals
  - But there is much more digitized patient information on mobile devices
    - Secure messaging
    - Encrypted mobile devices
  - Acceptance will be heavily based on patient trust that their information will be both safe in transmission and in storage; patients will only actively participate if there is assurance of their information being safeguarded

Important and Emerging HIPAA Security Areas of Concern…

Issues

- Next round of OCR audits
  - Mandatory by HITECH
  - Ongoing program
  - Covered Entities and Business Associates
  - Lack of thorough risk assessments; little understanding or application of encryption technologies from 2012 audits; this round will focus on these and ways to prevent / mitigate breaches
  - Unintended consequences of either a breach investigation or a compliance audit: discover lack of policies, training, risk analysis, risk management, sanctions, etc. which can lead to CMPs and CAPs

Important and Emerging HIPAA Security Areas of Concern…

Enforcement still a driver toward compliance:

Increased Enforcement Actions for both small and large breaches:

- Externally
  - OCR has now become "an enforcement-oriented culture" with "more assertive enforcement" and the expectation of "more monetary settlements" (former Director Leon Rodriguez)

  while

- Internally
  - OCR is striving to have CES, BAs, and subs to BAs attain and maintain a "culture of compliance"
- Some other players in the enforcement arena:
  - Additional compliance/enforcement concerns for healthcare organizations
  - FTC and FDA

Important and Emerging HIPAA Security Areas of Concern…

FTC v. OCR

- FTC (protect consumers' personal information) and OCR (protect patients' health care information – PHI)
- OCR – CMPs and CAPs (usually 3 years)
- FTC – no CMPs but CAPs (usually 20 years)
  - Either one or both can investigate health data breaches
    - Accretive Health, Rite Aid, CVS Caremark,

FDA v. OCR

- FDA (*product-centric*) with Medical Device Data Systems Regulation (MDDS) v. OCR (patient/healthcare - *organization-centric*)

Important and Emerging HIPAA Security Areas of Concern…

- Breaches … and the beat goes on
  - 35 in 2013 affecting 1.2 +M patients in December alone
  - More "wallpaper" for the "Wall of Shame" – approximately 800 "residents"
  - 5 big ones accounted for 90% in 2013
    - Indiana Family and Social Services Administration – Indianapolis, IN : 187,533 (April) – programming error, business associate
    - Texas Health Harris Methodist Hospital – Fort Worth, TX: 277,000 (May) – sheets of microfiche scheduled to be destroyed found in dumpster, business associate
    - Advocate Medical Group – Chicago: 4.3 M (July) 2nd largest ever – 4 unencrypted desk tops
    - AHMC Healthcare – Alhambra, CA (6 hospitals): 729,000 (October) – 2 unencrypted laptops
    - Horizon BC/BS of NJ – Newark, NJ: 840,000 (November) - 2 unencrypted laptops
  - All of the breaches involved PHI that was not unreadable, unusable, or indecipherable
  - Encryption is still "addressable" but… using it avoids a lot of headaches!

Important and Emerging HIPAA Security Areas of Concern…

- Emerging Legislation
  - Every year there is discussion and proposals for a pre-emptive national data protection law that would be stronger than the current 46 states, DC, Guam, Puerto Rico, and the Virgin Islands individual data protection laws (only Alabama, Kentucky, New Mexico, and South Dakota do not have any) both for consistency and administration, but, as yet, there is not one other than the breach notification rule

  - Likewise, as we move quickly to a predominant E-Health environment, there is growing concern over the need to more closely regulate mobile applications that collect personal data, in particular, health information. There is also growing anxiety about the vulnerability of medical systems and personal medical devices and any external threat to intercept and/or inject signals that would cause adverse outcomes for the wearer, even death. Regulating how developers of mobile applications, including mHealth, would collect personal data is also a topic of discussion.

Important and Emerging HIPAA Security Areas of Concern…

- Emerging Legislation
  - And, as we move to a more robust, all-inclusive HER, guarding against unauthorized access and impermissible uses of the data and the possibility of data mining for commercial and/or espionage purposes

So, keep an eye out for possible proposals and maybe even new regulations to address these concerns.

Our Speakers and their Topics

- Ali Pabrai: *Cyber Attacks and HIPAA Compliance: Prepared?*
- Rebecca Williams: *Breach Notification Incident Response*
- Phyllis Patrick: *Meaningful Use Audit Process: Focus on Outcomes and Security*
- Robert Michalsky: *Cyber Security Metrics (Dashboards and Analytics)*

  Break : 10:05 – 10:35 am
- Mac McMillan: *Out of Sight, Not Out of Mind: The Growing Risks of Medical Devices*
- Rick Kam and Larry Ponemon: *Data Breach Lessons from the Trenches: A Retrospective and a Forecast*
- Security Faculty Q&A (***New!***)

Networking luncheon: 12:00 – 1:00 pm

Thank You !

Any questions before we begin?

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