The Twenty- Eighth National HIPAA Summit

HIPAA Summit Day II
Morning Plenary Session: HIPAA Security

March 5, 2019

John Parmigiani

Summit Co-Chair

President

John C. Parmigiani & Associates, LLC

HIPAA Summit Security…
Welcome, Introduction, and Annual Health Care Security Update

- **PLENARY SESSIONS: (5 sessions) 8:00 am – 11:00 am**

❖ ***Transition Break*: 11:00 am – 11:15 am**

>>

- **MINI SUMMITS (11 sessions)**
  - **Mini Summit Group I - IV: 11:15 am – 12:15 pm**

❖ ***Networking Luncheon and Presentations*: 12:30 pm – 1:30 pm**

  - **Mini Summit Groups V -VII: 12:30 pm – 1:30 pm**

❖ ***Transition Break*: 1:30 pm – 1:45 pm**

Some Important and Emerging HIPAA Security Areas…

- **Privacy tidal wave across the globe driving more security supporting controls**
  - General Data Protection Regulation (GDPR)
    - Not only PHI and PII but location also
  - California Consumer Privacy Act (CCPA),
  - NY Cybersecurity Mandate for Financial Services Firms (23 NYCRR 500)
  - Massachusetts Data Breach Notification Law
    - All 50 states now have some form of individual data protection laws
  - House Committee on Energy and Commerce *Cybersecurity Strategy Report* (12/2018)
  - *Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients* (HICP) from DHHS

Some Important and Emerging HIPAA Security Areas…

- **……Privacy tidal wave across the globe driving more security supporting controls**
  - Ever-increasing digitization of healthcare and the resulting massive volumes of data that need to be protected
  - HIPAA Regulatory compliance = data privacy + data protection
    - *Can't have privacy without security*
  - Paradigm shift toward increased data governance strategy as the rights to one's personal data becoming more universally accepted. and privacy more important than convenience. Social media vulnerabilities and gaps; pathways to impermissible accesses
    - Need to have an inventory of the data, where it travels and is stored, etc.
    - Rudyard Kipling (1902) **"**I keep **six honest serving men** (they taught me all I knew); Theirs names are **What** and **Why** and **When** and **How** and **Where** and **Who**."

  We need to know these facts about all of our data if we are to provide the "appropriate and reasonable" level of security

Some Important and Emerging HIPAA Security Areas…

- **Now have a "zero-trust" environment**
  - No longer "trust but verify" replaced by "never trust, always verify"
  - Audit everything
  - Least privilege more strongly enforced enterprise-wide
  - Multifactor authentication becoming the rule
- **Network segmentation to reduce damage from ransomware and to make backup and recovery less cumbersome**
- **Medical device security**
  - Artificial Intelligence / Machine Learning
    - for radiology, diagnosis, genomics, research
    - IBM Watson Health (early use of AI -2011) a ten-year, $50 million investment in (AI) research partnerships with Brigham and Women's Hospital and Vanderbilt University Medical Center to explore how to use AI to improve EHR usability, support precision medicine, bolster patient safety, and foster health equity across communities.
    - to better safeguard hacking, but: Dichotomy - to enforce security safeguards; to decipher and break down security safeguards

Some Important and Emerging HIPAA Security Areas…

- **… Medical device security**
  - Medical Devices issued by Healthcare and Public Health Sector Coordinating Council (HSCC)
  - Wearables – heart rate trackers – Fitbit; Google; Toilet seat sensors – blood pressure/stroke/blood oxygenation; infusion pumps; etc.; etc.
  - Big Tech moving into healthcare -Google, Apple, Amazon, Uber
    - Amazon is partnering with JPMorgan Chase and Warren Buffett for a "healthcare initiative"(?)
    - Apple is planning a line of medical clinics.
    - Google's (Alphabet, Verily, is looking at the Medicaid market.
    - Uber wants to disrupt ambulance services

Some Important and Emerging HIPAA Security Areas…

- **IoT – how to manage a diverse and inconsistently secured enterprise -wide collection of apps and devices**
  - Approximately 7 billion internet-enabled devices in the world and this number is expected to reach 21.5 billion by 2025
  - Need to know user habits, how they'll use the IoT tool, and where there are gaps in the process. Once you understand user interaction, you can design around security
  - Secure messaging for clinicians
  - Just announced at HIMSS: a medical wearable Sensor Platform, which comes with a range of sensors, edge computing technologies, and an "Internet of Health Things" data cloud. It captures human vitals and biometrics, and delivers data from the patient (heart and respiratory rates, temperature, ECG rhythms, activity and more) to edge computing devices of IoT technology partners, as well as to the cloud, for application integration and analysis.
  - California Senate Bill No. 327 – covers all IoT devices sold in California with security requirements.

Some Important and Emerging HIPAA Security Areas

- **Blockchain**
  - Widespread initiatives ranging from supply chain, patient enrollment, provider data, payment , data collection, clinical trials, research
  - Possible use as a means to increase interoperability of patient clinical data in a secured data sharing environment to provide a Continuity of Care Record (CCR) standard or HL7 Continuity of Care Document (CCD) standard
    - longitudinal health record, regardless of the system of data capture, that serves the patient as well as population health studies in a secured environment

- **And, the recommended mind set for meeting the HIPAA Risk Analysis requirement:**
  - **Risk-based approach** vs. a compliance/checklist-based approach **to enterprise -wide security – assets, vulnerabilities, threats, probability of occurrence, business impacts, available safeguards**

Our Speakers and their Topics…

- ***Trends and Characteristics of Reportable Health Data Breaches, 2010-2017*** **; Thomas H. McCoy, MD**
  Director of Research, Center for Quantitative Health, Massachusetts General Hospital, Boston, MA
- ***FBI Keynote*****; Tonya Ugoretz,** Deputy Assistant Director, Cyber Division, FBI; Associate Professor, Center for Security Studies, Georgetown University; Adjunct Faculty, Center for Intelligence Training, FBI Academy, Washington, DC
- ***DHS Keynote*****; Jeanette Manfra, MA**
  National Protection and Programs Directorate (NPPD), Assistant Secretary, Office of Cybersecurity and Communications, Department of Homeland Security (DHS); Former Director for Critical Infrastructure Cybersecurity, National Security Council, the White House, Washington, DC

Our Speakers and their Topics…

Healthcare Chief Security Officers Best Practices Roundtable

- **Julie Chua,** Chief, Risk Management Branch, Office of Information Security, Department of Health and Human Services, Washington, DC

- **Josh DeFrain, MS,** Chief Information Security Officer, Flatiron Health; Former Global CyberSecurity Operations Director, Capital One, Washington, DC

- **John C. Parmigiani, MS,** President, John C. Parmigiani and Associates, LLC; Former Director of Enterprise Standards, HCFA, Ellicott City, MD

- **Jon Moore, MS, JD, HCISPP,** Chief Risk Officer, Clearwater Compliance, New York, NY (Moderator)

Break : 11:00 am – 11:15 am

Thank You !

Any questions before we begin?

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