The Twenty- Ninth National HIPAA Summit

HIPAA Summit Day II
Morning Plenary Session:
HIPAA Policy Update & HIPAA Security

March 4, 2020

John Parmigiani

Summit Co-Chair

President

John C. Parmigiani & Associates, LLC

HIPAA Summit Security…
Welcome, Introduction, and Important and Emerging Healthcare Security Issues

- **Morning PLENARY SESSIONS: (4 sessions) 8:00 am – 10:30 am**

❖ ***Transition Break*: 10:30 am – 11:00 am**

\>>

- **MINI SUMMITS (12 sessions)**
  - **Mini Summit Group I (I – IV): 11:00 am – 12:00 pm**

❖ ***Networking Luncheon and Presentations*: 12:15 pm – 1:15 pm**

  - **Mini Summit Group II (V –VIII): 12:30 pm – 1:30 pm**
  - **Mini Summit Group III (IX – XII): 1:30 pm – 2:30 pm**

❖ ***Transition Break: 2:30 pm – 3:00 pm***

Our Speakers and their Topics…

- **Welcome and Introduction / Security Issues**
  - **John C. Parmigiani, MS**
    President, John C. Parmigiani and Associates, LLC; Former Director of Enterprise Standards, HCFA, Ellicott City, MD (Co-Chair)
- **HIPAA Policy Update**
  - **Marissa Gordon-Nguyen, MPH, JD**
    Senior Advisor for HIPAA Policy, US Department of Health and Human Services, Washington, DC.
  - **Timothy Noonan, JD**
    Deputy Director, Health Information Privacy, US Department of Health and Human Services; Former Supervisory General Attorney, US Department of Education, Washington, DC
- **HITRUST CSF: A Credible Standard for Ensuring HIPAA Compliance**
  - **Uday O. Ali Pabrai, MSEE, CISSP, HITRUST (CCSFP)**
    Chief Executive and Co-founder, ecfirst (A HITRUST Authorized External Assessor), Irvine, CA

Our Speakers and their Topics

Healthcare Chief Security Officers Best Practices Roundtable

- **Anahi Santiago, MBA**
  Chief Information Security Officer, Christiana Care Health System; Former Director, Information Security and Support Services, Albert Einstein Healthcare Network, Philadelphia, PA
- **Frank Ruelas, MBA**
  Facility Compliance Professional, St. Joseph's Hospital and Medical Center/Dignity Health, Phoenix, AZ
- **Timothy Torres, MBA, CISSP, ISSMP, CISM, HCISPP**
  Senior Deputy Chief Information Security Officer, Sutter Health, Sacramento, CA
- **John C. Parmigiani**, **MS**, President, John C. Parmigiani & Associates, LLC; Former Director of Enterprise Standards, HCFA, Ellicott City, MD

Break : 10:30 am – 11:00 am

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
    - Right to be forgotten /right to delete / right to control access
    - Emphasis on notice, transparency, and consent
    - Being modeled in 20 other states, so far…Washington, New York, Illinois, Maine, Nevada already passed
  - Biometric Information Privacy Act (BIPA) – Illinois
  - National Privacy Bill that preempts State Laws / ePrivacy Directive ???
    - HIPAA/HITECH Privacy Rule is a "floor preemption"; stricter requirements in state laws have precedence
  - Data Breach Notification Laws
    - All 50 states, DC, Puerto Rico now have some form of individual data protection laws

Some Important and Emerging HIPAA Security Areas…

- **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*
  - IoT devices proliferating from introduction of the smart phone by Apple in 2007 to an estimated 2.4 B in 2020 and >40 B by 2025
    - How to manage a diverse and inconsistently secured enterprise – wide collection of apps and devices
    - Tangle of interrelationships; enormous number of new and nested end points to protect – a different universe to manage and control – could a digital "Pearl Harbor" be in our future?
    - More sophisticated threat environment (artificial intelligence /machine learning – enabled) capable of hitting specified targets with precision and infestation with minimal or no identification by the enterprise
    - Medical devices and wearables with insufficient safeguards and controls to protect patent identity and health safety
    - Need to know user habits, how they'll use the IoT device, and where there are gaps in the process. Once you understand user interaction, you can design around security

Some Important and Emerging HIPAA Security Areas…

- **…Ever-increasing digitization of healthcare and the resulting massive volumes of data that need to be protected**
  - 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 all have to be identified and controlled.
    - 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 – biometrics now usually one of the factors
- **Network segmentation to reduce damage from ransomware and to make backup and recovery less cumbersome**
  - Ransomware not only affects availability and healthcare operations but also can affect confidentiality and integrity of patient data.
- **Blockchain**
  - Will it be the preferred app in safeguarding multiple events and affording greater interoperability from diverse data sources in a secured data sharing environment?
  - Widespread initiatives ranging from supply chain, patient enrollment, provider data, payment , data collection, clinical trials, research
- **Remember regulatory compliance is not the same as an enterprise – wide risk analysis** – is a part of having met the documented existence of the HIPAA/HITECH requirements but not an effort that creates a measured assessment of the impact of identified threats to organizational assets and their respective vulnerabilities based on likelihood of occurrence and severity of damage.

Thank You !

Any questions before we begin?

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