hfma™ region 11
healthcare financial management association

thrive

HITRUST, ePHI and HIPAA Compliance

Wednesday, June 29, 2016 | 12:00 - 1:00 pm PST

FREE Webinar

Register Online
http://bit.ly/hfma-r11-HITRUST

Digitization and exchange of protected health information is now mandated. Companies that process, store and transmit electronic records or "ePHI" are working with more and more vendors (aka Business Associates) as data continues to flow more freely between entities. **How do covered entities and their patients know if they can trust their associates?** The value of a medical record on the street is over 10x that of a credit card and as businesses continue to embrace mobile and remote computing, breaches are similarly on the rise. HIPAA and related laws and regulations are written in a way to allow for interpretation and flexibility so that businesses can apply controls that fit their specific strategic objectives, budget and data processing requirements. The disadvantage is that so-called **HIPAA compliance reports are only as good as the auditor's interpretation of the law and how businesses have chosen to implement controls**. HIPAA compliance audits are typically not peer reviewed nor subject to any trust and assurance certification. SOC audits are certified and peer-reviewed but are not specific to HIPAA and still leave a significant amount of wiggle room on which controls are applied and how they are applied.

The HITRUST Alliance is a non-profit organization founded by several major healthcare agencies that seeks to standardize the implementation of controls relevant to HIPAA and the related laws and regulations. HITRUST has developed the Common Security Framework (CSF), which is based upon ISO 27001 and includes controls and standards from several other frameworks including NIST, PCI and others. CSF contains a prescriptive approach to implementing controls based upon the scope and size of an entity and its data processing requirements. HITRUST validated assessment reports and certification creates a common methodology for validating trust and assurance between entities.

In this talk, we will discuss some of the challenges facing security in healthcare, and how HITRUST and the common security framework are helping to lead the way to creating a more secure environment to protect patient data from unauthorized disclosure.

Learning Objectives:

- Learn some of the challenges of managing HIPAA compliance for entities that process, store or transmit ePHI
- Learn how HITRUST and the common security framework helps to standardize the way controls and standards are applied across various entities that need to be compliant
- Learn how validated HITRUST assessment reports provide a means for companies to validate a vendor's trust and assurance claims before exchanging sensitive data, and how these can be more informative than SOC audit reports.

Speaker: Erik D. Jones, CEO, Jacobian Engineering Inc.

Erik D. Jones is a certified HITRUST practitioner with over 24 years of experience working in Information Technology and Security. He currently holds CISSP, AWS Solutions Architect and HCISPP certifications. Erik founded Jacobian Engineering 10 years ago and the company provides managed IT services, compliance certification, risk assessment, audit services and forensics. Erik also serves as Chief Architect for PreciseQ, a silicon valley based firm specializing in enterprise software development for the healthcare industry. Erik studied Electrical Engineering at The University of California, Davis where he graduated with high honors and holds several information security certifications from ISC2, Stanford University, HITRUST and SANS Institute.