HIPAA Compliance Is Not Enough to Curtail PHI Data Breaches, Says FairWarning CEO at HIMSS’16

Regulation alone is not enough to meet today’s escalating threats to healthcare; Calls on care providers to secure and protect their applications

Las Vegas (HIMSS’16) – March 2, 2016 – Speaking at HIMSS’16, FairWarning, Inc.’s CEO, Kurt J. Long, called on care providers to secure and protect their applications that hold the “crown jewels” of their patient information, citing that HIPAA compliance is not enough to protect patient health information and curtail data breaches.

“As the value of protected health information soars for a host of nefarious purposes, there is now a need for the convergence between privacy, compliance and security in healthcare,” said Long. “It is no longer ‘am I simply compliant with HIPAA.’ It’s ‘will my hospital be offline for a week because of a ransomware attack.”

Long continued, “Information security bad actors are moving faster than ever in attacking healthcare providers in compromising patient information and institutions. For businesses relying strictly on HIPAA compliance and an industry waiting on OCR enforcement of HIPAA, this approach is simply not enough. Care providers need to secure and protect their applications that hold the mother-load of patient information, their Electronic Health Records as well as all the supporting applications.”

Since the introduction of the Health Information Technology for Economic and Clinical Health (HITECH) Act in 2009, the technology and threat landscape to healthcare has changed dramatically. “HIPAA was written for a different time – when these threats didn’t even exist. If you assume because you’re HIPAA compliant it means you’re protected, you’re in trouble.”

So what can care providers do, if HIPAA is not enough? Organizations need to closely monitor what is happening at the application level, including Electronic Health Records and fast growing cloud applications like Salesforce and Office 365. “They must consider every possible attack vector, assume we can be compromised from every vector until we have proven we have not (repeat this every day), monitor, analyze and respond in near real-time and coordinate across traditional vendors lines against coordinated external and internal attacks -- the lines have completely blurred in this area.”

If you’d like to join in on the conversation, please use the hashtag #HIPAAisnotenough on Twitter.
About FairWarning®

FairWarning® is a leading provider of solutions that deliver information security intelligence and insights for mission critical applications, such as Salesforce, Office 365, Electronic Health Records (EHRs) and cloud-based applications. Auditing over 350 business applications, FairWarning inspects immense volumes of application security information and provides visibility related to application risk, security, and governance through deep insights into user access behaviors. FairWarning provides a comprehensive platform and managed services for real-time and continuous monitoring, advanced threat detection and filtering, performing forensic investigations and incident containment, enforcing access policies, conducting legal investigations, and improving compliance effectiveness with complex federal and state privacy laws such as HIPAA, PCI, SOX, FISMA and EU Data Protection Act. FairWarning delivers insights 24x7x365. FairWarning catches people stealing your data.