Safeguarding Health Information: Building Assurance through HIPAA Security

An OCR & NIST HIPAA Security Rule Conference

Agenda

Conference Day 1: Tuesday May 11, 2010			
Time	**Session**	**Abstract**	**Speaker(s)**
7:30-9:00	**Registration**		
9:00-9:10	Introduction and Logistics		
9:10-9:20	Welcoming Remarks from OCR		Susan McAndrew – Deputy Director for Privacy, HHS Office for Civil Rights
9:20-9:30	Welcoming Remarks from NIST		William Barker – Chief Cybersecurity Advisor, NIST Information Technology Laboratory
9:30-10:15	Tips and Techniques for Conducting Risk Assessments	Risk Assessment, one component of an overarching risk management strategy, is the process of identifying risks to an organization's operations, assets, or individuals. This session will discuss a risk assessment process, use of risk assessment results to improve organization-wide security, and a summary of the HIPAA Security Rule risk analysis and management requirements.	Pat Toth – NIST Marissa Gordon-Nguyen – HHS/OCR
10:15-10:30	**Break**		
10:30-11:00	Keynote Address		Georgina Verdugo—Director, HHS Office for Civil Rights Howard Schmidt – White House Cybersecurity Coordinator
11:00-11:45	Standards and Certification Interim Final Rule	Providers and patients must be confident that the health IT products and systems they use are secure, can maintain data confidentially, can work with other systems to share information, and can perform a set of well-defined functions. The HHS Office of the National Coordinator for Health Information Technology (ONC) will provide a general overview of the Standards and Certification Interim Final Rule (IFR) and its relation to the Meaningful Use criteria and the Certification Programs for Health IT, and key security capabilities within the context of the IFR. NIST will then provide a summary discussion of the meaningful use test method development process in support of the health IT certification program.	Steve Posnack – HHS/ONC Lisa Carnahan – NIST

Safeguarding Health Information: Building Assurance through HIPAA Security

An OCR & NIST HIPAA Security Rule Conference

Agenda

Conference Day 1: Tuesday May 11, 2010			
Time	**Session**	**Abstract**	**Speaker(s)**
11:45-1:00	**Lunch**		
1:00-2:00	Panel: Breach Notification	OCR's Christina Heide and the FTC's Cora Tung Han will provide an overview and update on the federal standards for breach notification implementing the HITECH Act, who they impact and the critical elements in protecting data and responding appropriately when data is compromised.	Christina Heide – Health Information Privacy Division, HHS/OCR Cora Tung Han – Division of Privacy and Identity Protection, Federal Trade Commission (FTC)
2:00-2:45	Security of Health Devices	The HIPAA and HITECH regulations include many personal health security requirements - and penalties - that actually can affect mobile and fixed medical devices in unexpected ways. This session will identify these issues, and will discuss emerging remediation strategies.	Elliot Sloane – Drexel University
2:45-3:00	**Break**		
3:00-3:45	Security Considerations for New Media and Healthcare	As healthcare organizations continue to adopt technologies at an increasing rate, how does the organization secure its confidential information and protect its reputation while applying the "latest and greatest" mediums for communication? Sharon Finney, Corporate Data Security Officer for Adventist Health System, will discuss the approach, policies, standards, technology solutions and auditing techniques used by Adventist Health System to build the foundation for adoption and integration of new (social) media.	Sharon Finney – Corporate Data Security Officer, Adventist Health System
3:45-4:30	Update on OCR Enforcement of the Privacy and Security Rules	HHS' Office for Civil Rights is responsible for enforcing the HIPAA Privacy and Security Rules. This presentation will provide an update on OCR's approach to enforcement through voluntary compliance and corrective action to obtain systemic change in the health industry. The program will also provide information on the HITECH Act significantly gave OCR improved enforcement tools with which to obtain compliance including increased amounts of up to $1.5 million per violation that can be levied as civil monetary penalties where noncompliance is found.	Marilou King – Civil Rights Division, HHS Office of General Counsel David Holtzman – Health Information Privacy Division, HHS/OCR

Safeguarding Health Information: Building Assurance through HIPAA Security

An OCR & NIST HIPAA Security Rule Conference

Agenda

Conference Day 2: Wednesday May 12, 2010			
Time	**Session**	**Abstract**	**Speaker(s)**
7:30-8:30	**Registration**		
8:30-8:45	Welcome and Recap		OCR/NIST
8:45-9:30	FTC Information Security	This session will discuss the broad information security matters in which the Federal Trade Commission (FTC) is involved, the kinds of vulnerabilities and practices that have arisen, and the lessons learned through these matters in the context of the phases of a breach. This session will also generally discuss the P2P project.	Alain Sheer – Attorney, Division of Privacy and Identity Protection, FTC
9:30-10:15	Strategies for Developing and Implementing Contingency Plans	Information and information systems are vulnerable to a variety of disruptions from a variety of sources. While vulnerabilities may be minimized or eliminated through the implementation of management, operational, and technical safeguards, it is virtually impossible to eliminate all risk. Effective contingency planning, execution, and testing are essential to mitigate the risk of system and service unavailability. This session will begin with a summary of the HIPAA Security Rule contingency planning requirements, followed by a discussion of strategies for developing and implementing contingency plans.	David Holtzman – Health Information Privacy Division, HHS/OCR Marianne Swanson – NIST
10:15-10:30	**Break**		
10:30-11:15	Logging and Auditing in a Healthcare Environment	Healthcare has made progress in the area of collecting and analyzing network and user activity but still falls short of what is required and needed. There are a number of challenges that the healthcare industry faces that make this critical function more difficult. Some of these challenges are cultural and some are technical. Despite these challenges, virtually every regulation and security standard that applies or touches healthcare expects logging and auditing. HITECH increases this need and will place the focus more on proactive monitoring to protect patient information and avoid costly incidents. This presentation will discuss the current landscape in healthcare logging and auditing and associated challenges, as well as offer observations for what needs to be considered to meet current and emerging requirements.	Mac McMillan – Cynergistek, Inc

Safeguarding Health Information: Building Assurance through HIPAA Security

An OCR & NIST HIPAA Security Rule Conference

Agenda

Conference Day 2: Wednesday May 12, 2010			
Time	**Session**	**Abstract**	**Speaker(s)**
11:15-12:15	Panel: HIPAA Security Compliance: An Industry Perspective	The HIPAA Security Rule mandates have been required for many years now, yet it is well known that some segments of the industry have not implemented, or not implemented well and completely, the security technology controls, and administrative and physical security controls and policies. This panel will discuss what security implementation looks like in the spring of 2010, outline barriers to implementation, and suggest some areas where federal guidance would be useful.	Sue Miller – WEDI Lisa Gallagher – HIMSS Robert Tennant – MGMA Dan Rode – AHIMA
12:15-1:30	**Lunch**		
1:30-2:15	HIE Security Architecture	This session will present Harvard Pilgrim HealthCare's experience with using health information exchange and related business practices and operating principles to improve efficiencies and to facilitate electronic communications with health care providers. Ultimately, these electronic processes can benefit consumers when health information becomes more available and accessible when needed for treatment and care decisions. The presentation will use a case study of how Harvard Pilgrim HealthCare has participated in a working Health Information Exchange, the New England Health Exchange Network (NEHEN), and will discuss the pertinent operating principles, the technology infrastructure, and the results and positive outcomes. In particular, the session will focus on the various approaches taken to address the ethical and legal requirements to protect privacy and confidentiality, while providing a technically secure information exchange network, and how these approaches can be leveraged for national models and efforts.	John Kelly – Director, eBusiness Architecture, Harvard Pilgrim Healthcare
2:15-3:00	Security Implementation Considerations for Mobile and Wireless Technologies	The distributed use of mobile and wireless technologies across the Federal government requires solutions that leverage industry standards to provide secure, scalable, and interoperable communication architectures. Key elements to consider when approaching wireless security include areas where networks are most vulnerable, wireless technology's built-in security protocols, wireless and wired intrusion detection, access controls, and mobile device protection. Wireless technologies can offer extremely secure communications when properly implemented. This presentation will introduce the audience to the unique security requirements, threats, countermeasures, and resources to select and implement secure mobile and wireless communications.	Matt Sexton – Booz Allen

Safeguarding Health Information: Building Assurance through HIPAA Security

An OCR & NIST HIPAA Security Rule Conference

Agenda

Conference Day 2: Wednesday May 12, 2010			
Time	**Session**	**Abstract**	**Speaker(s)**
3:00-3:15	**Break**		
3:15-4:15	Encryption Standards	Encryption is one technology that can be used protect sensitive health information. This session will provide a management-level discussion of the encryption standards, guidelines, and functional capabilities cited in various HIT rules and regulations. Cryptographic technologies, validations, and transition timelines for common cryptographic algorithms will also be discussed.	Matt Scholl – Group Manager, Security Management and Assurance, Computer Security Division, NIST