

Safeguarding Health Information: Building Assurance through HIPAA Security Hosted by the HHS Office for Civil Rights (OCR) and the National Institute of Standards and Technology (NIST) Ronald Reagan Building and International Trade Center May 21-22, 2013 – FINAL AGENDA	
Time	Day 1 - Plenary Sessions - Atrium Hall
9:00-9:15	Welcoming Remarks
9:15-10:00	Keynote Eric Dishman, Intel Fellow and General Manager of the Health Strategy & Solutions Group
10:00-10:15	Break
10:15-11:15	Provider and Patient Identity Management in HIE Deven McGraw (Center for Democracy and Technology) , Walter Suarez (Kaiser Permanente) , Peter Tippet (Verizon) , & Elizabeth Franchi (Veterans Affairs)
11:15-12:15	HIPAA Requirements and Mobile Apps Adam Greene (Davis Wright Tremaine)
12:15-1:15	Lunch - Atrium Hall Included with In-Person Registration
1:15-2:15	HITECH & The Cloud: Control and Accessibility of Data Downstream Moderator: David Holtzman (OCR) Panelists: James Koenig (PWC) & Ted LeSueur (McKesson) Abstract The session will first provide an overview of the new HIPAA/HITECH requirements around business associates and the unique issues/complexities to consider that healthcare organizations are addressing in various ways. The session will also discuss the key cloud issues organizations are trying to solve and what are the industry trends to manage risk and compliance. Highlights will include an overview of vendor/BAA programs being put in place, including pre-contract assessments, enhanced BAAs and periodic vendor post-contract compliance/risk audits as well as examples of what organizations are doing in connection with moves to the cloud and risks and obstacles encountered. The session will close with a look at what companies are doing around post-contract audits of their cloud service providers including the processes to put into place, the scope of the audit protocol and testing, and best practices from the perspective of an enterprise-sized purchaser of cloud services.
2:15-3:00	Report on the OCR Privacy, Security, and Breach Notification Rule Compliance Audit Program Verne Rinker (OCR)
3:00-3:15	Break

<p>Safeguarding Health Information: Building Assurance through HIPAA Security Hosted by the HHS Office for Civil Rights (OCR) and the National Institute of Standards and Technology (NIST) Ronald Reagan Building and International Trade Center May 21-22, 2013 – FINAL AGENDA</p>	
3:15-4:15	<p>Leveraging Social Media While Mitigating the Risk David Etue (SafeNet)</p>
4:15-5:00	<p style="text-align: center;">HIPAA Security Awareness Tools Rachel Seeger (OCR), Laura Rosas (ONC)</p> <p style="text-align: center;">Abstract</p> <p>HIPAA covered entities and their business associates care deeply about patient trust and the importance of keeping health information secure and confidential. This session will include an overview and discussion of the multiple tools and resources developed by the U.S. Department of Health and Human Services' Office for Civil Rights and the Office of the National Coordinator for Health Information Technology to help organizations create a culture of privacy and security across their organizations to safeguard patients' protected health information.</p>
<p>End Conference Day 1</p>	

Safeguarding Health Information: Building Assurance through HIPAA Security
 Hosted by the HHS Office for Civil Rights (OCR) and the National Institute of Standards and Technology (NIST)
 Ronald Reagan Building and International Trade Center
 May 21-22, 2013 – **FINAL AGENDA**

Time	Day 2 - Plenary Sessions - Atrium Hall
9:00-9:45	<p align="center">Dialogue on HIPAA/HITECH Compliance Leon Rodriguez, Director, OCR</p> <p align="center">Abstract</p> <p>Director Rodriguez will provide an overview to the new impact of the Omnibus HIPAA Rulemaking and highlight OCR's commitment to enforcement, audit and education initiatives in the coming year.</p>
9:45-10:15	<p align="center">Looking Over the Rainbow: What's Next in Legislation and Policy Impacting Health Privacy & Security Kirk Nahra (Wiley Rein)</p> <p align="center">Abstract</p> <p>Now that the Omnibus regulation is out, what's next for health care privacy and security? This session will review what's left on the HITECH agenda and, more significantly, the future of health care privacy and security law as it evolves to meet the changes in the health care industry and in privacy regulation overall.</p>
10:15-10:30	<p align="center">Break</p>
10:30-11:15	<p align="center">HIPAA/HITECH Rule Changes Affecting Breach Notification & HIPAA Security Kathleen Kenney and David Holtzman (OCR)</p> <p align="center">Abstract</p> <p>This session will include an overview of the enforcement statistics associated with OCR's Breach Notification submissions. Additionally, the session will touch upon the Omnibus Final Rule's modification to the definition of breach. Finally, a portion of the presentation will include OCR's experience with breach reports deriving at the business associate and a discussion of BA's liability under the Final Rule.</p>
11:15-12:15	<p align="center">Health Information Security Assurance in HIE and Interoperable EHRs Moderator: Sue Miller (WEDI Security and Privacy Workgroup) Panelists: Mike Zegar (NJ-HITEC) Joseph McClure, JD (Siemens) Doreen Espinosa (Utah Health Information Network) Ruth Carr, JD (Statewide Coordinator, Georgia HIE)</p> <p align="center">Abstract</p> <p>The healthcare industry is becoming more and more electronically interoperable. The four (4) panelists will outline the stages of interoperability in 2013. They will outline not only how HIPAA Security assists interoperability, but also the risks and problems.</p>
12:15-1:15	<p align="center">Lunch - Atrium Hall Included with In-Person Registration</p>

1:15-2:00	<p style="text-align: center;">Healthcare Threat Briefing Debra Kobza (National Health Information Sharing and Analysis Center [NH-ISAC])</p> <p style="text-align: center;">Abstract</p> <p>Cyber threats aimed at healthcare organizations are on the rise. The risks are staggering. The number of global data breaches reached 2,644 last year, more than doubling the number of incidents in 2011. They accounted for the exposure of 267 million records. This session will touch upon the reasons that healthcare records have become targeted and outline some of the most common threats.</p>
2:00-2:30	<p style="text-align: center;">Framework for Improving Critical Infrastructure Cybersecurity: Executive Order 13636 Kevin Stine (NIST)</p> <p style="text-align: center;">Abstract</p> <p>Executive Order (EO) 13636, Improving Critical Infrastructure Cybersecurity, was issued by the President in February 2013 and requires NIST to develop a Cybersecurity Framework to reduce cybersecurity risks to critical infrastructure. This session will provide an overview of the EO, and will discuss NIST's implementation plan for developing the Cybersecurity Framework.</p>
2:30-3:00	<p style="text-align: center;">Health IT and the National Cybersecurity Center of Excellence (NCCoE) Nate Lesser (NCCoE)</p>
3:00-3:15	<p>Break</p>
3:15-4:15	<p style="text-align: center;">Managing the Insider Threat: Real-time Monitoring of Access Patterns to e-PHI Mac McMillan (HIMSS), Jennings Aske (Partners Healthcare), Daniel Fabbri (U. Michigan) & Mike Terra (Oracle)</p> <p style="text-align: center;">Abstract</p> <p>Managing the Insider Threat: Real-time Monitoring of Access Patterns to e-PHI - This session will explore the use of real-time monitoring to detect inappropriate access to sensitive data maintained in electronic health record systems (EHRs). Mac McMillan (HIMSS) will discuss the use of real-time monitoring techniques in other industry verticals. Jennings Aske (Partners Healthcare) will discuss his institution's attempt at implementing real-time monitoring of its electronic health record system. Mike Terra (Oracle) will discuss Oracle's products which facilitate real-time EHR monitoring, and are being implemented at Partners HealthCare. Daniel Fabbri (U. Michigan) will discuss his research into approaches to secure EHRs through audit log analysis and mining.</p>
4:15-5:00	<p style="text-align: center;">New Tools to Manage Security Settings of End-User Devices Operating MS Windows Vince Johnson & Hector Rodriguez (Microsoft)</p> <p style="text-align: center;">Abstract</p> <p>In today's world of healthcare, change is the only constant. Reform is ushering a new era of systems and technology that will push the barriers of traditional information security. During this session, Microsoft will explore how organizations can embrace change and apply best practices that allow innovation to continue without sacrificing security and privacy standards. The session will provide in depth scenarios that can cause compromised security and also outline the best practices to mitigate these problems. Microsoft will also outline how the HIPAA Security Rule affects these scenarios and the challenges to implementing the proper controls in today's resource constrained market. Microsoft will also introduce a new set of HIPAA Group Policy Objects produced that will continuously re-apply the necessary security settings to server and client operating systems throughout your environment.</p>
<p>End Conference</p>	