AHIMA Privacy and Security Institute Agenda

AHIMA19 Health Data and Information Conference

McCormick Place—Lakeside Center, Chicago, IL

Saturday, September 14, 2019

This is a highly interactive meeting in which attendees are encouraged to engage in discussion and networking with the faculty and other attendees. Please review presentations prior to the meeting and bring any questions, scenarios, and challenges related to any of the topics to be discussed throughout the Privacy and Security Institute.

Time	Agenda Outline	
7:30–8:15 a.m.	**Continental Breakfast**	
8:15–8:30 a.m.	**Welcome and Introductions**	
8:30–10:15 a.m.	***Updates from HHS OCR—What's Your Favorite Regulator Done for You Lately?*** *Iliana Peters, JD, LLM, CISSP, Health Care Services, Polsinelli, Washington, DC* Are you up to date on the latest developments from the HHS Office for Civil Rights? Learn about all the recent developments in HIPAA Privacy, Security, and Breach Notification, essential for privacy and compliance professionals that work with protected health information on a daily basis.	
10:15–10:30 a.m.	**Networking Break with Vendors in Exhibit Hall**	
Morning Tracks	***Privacy***	***Security/Cybersecurity***
10:30–11:45 a.m.	***Employer Data Breach Liability: The Employee as Threat Vector***. Barry Herrin, JD, CHPS, FAHIMA, FACHE Worried about insider threats? You should be! Insider threats now account for the majority of all cyber incidents. Should organizations consider their employees as threat vectors in cybercrime? Find out the six big decisions that healthcare organizations must make to reduce the known threat from insiders and employees.	***Medical Device Security Risk Management Automation/Tooling***. Jongbum Keum, Product Safety and Security, Deloitte, Boston, MA (*invited)* Medical device manufacturers and healthcare delivery organizations (HDOs) are increasingly using connected devices to remotely monitor patients, transfer medical information, and connect patients and doctors in remote locations. This trend increases the potential risks around patient safety, patient

AHIMA Privacy and Security Institute Agenda

AHIMA19 Health Data and Information Conference

McCormick Place—Lakeside Center, Chicago, IL

		information, and raises questions around medical device security risk management. Learn about a comprehensive solution using an asset inventory to aid in the identification, triaging, and assessment of potential vulnerabilities.
11:45 a.m.–12:30 p.m.	**Networking Lunch**	
Afternoon Tracks	***Privacy***	***Security/Cybersecurity***
12:30–1:30 p.m.	***Privacy Breach Investigation and Response.*** T. Andrew Reeder, MPA, CISSP, CHPC, CISA, CISM, HCISPP Every day organizations work with sensitive patient information with the potential to be misdirected, lost, stolen, or simply mishandled—leading to an improper disclosure. The cost of noncompliance exists (i.e., trust, image, and cost of breech response). Explore these issues, regulatory compliance obligations, and what covered entities can do to improve their compliance, investigation, and breech response.	***What Are Vendors Doing with Data?*** Daniel Fabbri, PhD, Maize Analytics, Inc. Nashville, TN With the increased adoption of cloud solutions and machine learning applications, healthcare organizations must understand how vendors store data, what controls are used to protect the data, and how the vendors use their data and the associated risks. Learn how to formulate business associate agreements in the era of "Big Data" to manage data re-purposing, data mixing, and machine learning model mixing to limit how your data is being used. And examine different legal and technological processes to ensure vendors compliance with BAAs, even if the vendor application is managed in the cloud.
1:30–2:30 p.m.	***NIST Privacy Framework***. Karen Greenhalgh, HCISPP, Cyber Tygr, Virginia, Beach, VA Do you know about the new NIST Privacy Framework? The security of Personally Identifiable Information (PII) plays an important role in the protection of privacy- individual privacy cannot be achieved by solely securing PII.	***NIST CsF = Standard for HIPAA Compliance + Cybersecurity.*** Uday Ali Pabari, MSEE, HITRUST (CCSFP), CISSP (ISSAP, ISSMP), ecfirst, Waukee, IA NIST CsF is the framework that executives can trust as a basis for their HIPAA compliance program. It can be used by organizations of all sizes, including business associates, physician

	This session will reveal the most impactful and challenging attributes of a privacy risk-based program and how the NIST Privacy Framework addresses them. Learn how to incorporate privacy risk management standards, guidelines, and best practices, into your healthcare organizations policies and practices.	practices, hospitals, IT firms, government agencies, and other healthcare entities.
2:30– 3 p.m.	**Networking Break**	
3–4:30 p.m.	***Compliance Analytics: A Framework for Integrating Governance, Security, and Privacy.*** Robert Lord, Protenus, Baltimore, MD *(invited) and* Ashley McArthur, Yale New Haven Health System, New Haven, CT *(invited)*	
4:30–4:45 p.m.	**Closing Day 1**	

CEUs: 7 (plus additional 1 CEU for networking in the Exhibit Hall)

AHIMA Privacy and Security Institute Agenda

AHIMA19 Health Data and Information Conference

McCormick Place—Lakeside Center, Chicago, IL

Sunday, September 15, 2019

Time	Agenda Outline	
7:30–8:15 a.m.	**Continental Breakfast**	
8:15–8:30 a.m.	**Welcome and Introductions**	
8:30– 10:15 a.m.	Keynote Address - ***Healthcare Cybersecurity: Top Threats and Best Practices.*** Ty Greenhalgh, HCISPP, Cyber Tygr, Virginia Beach, VA and *Erik Decker, Cybersecurity and Privacy, University of Chicago Medicine, Chicago (invited)* Audiences gain insight into healthcare's "Top 5 Cybersecurity Threats" and "10 Best Practices", created by the HHS led Health and Public Health Sector 405(d) Task Group. This congressionally mandated 405(d) Task Group focus has focused on building voluntary, consensus-based principles, and best practices to ensure cybersecurity in the Health Sector. Ensure your organization focuses on the highest risk threats with appropriate control techniques, as well as policies and procedures. Templates and toolkits will help integrate this knowledge into a plan that can establish targeted policies and coordinate departmental workflow, cybersecurity education and compliance.	
10:15– 10:30 a.m.	**Networking Break with Vendors in Exhibit Hall**	
Morning Tracks	***Privacy***	***Security/Cybersecurity***
10:30–11:45 a.m.	***Assessing Privacy and Security Compliance***. Kelly McLendon, PHIA, CHPS, CompliancePro Solutions, Titusville, FL and Rita Bowen, MA, RHIA, CHPS, CHPC, SSGB, Privacy, Compliance and HIM Policy, MRO Participants will benefit from learning about the different requirements for privacy and security assessments, beyond just HIPAA. They will also be exposed to methodologies, real	***Biomedical Device Breach.*** Keith Fricke, MBA, PMP, Healthcare Security Operations, tw-Security, Overland Park, KS The most important step in incident response is knowing what needs to be done and in which order. A security incident requires much more than finding a solution and fixing it. Carefully

	world examples, scoring, reporting and creation of remediation plans. New rules such as GDPR and CCPA will be discussed in the context of what should be assessed and when, along with their application into healthcare.	orchestrating the response, steps can reduce penalties, fees and judgments. When data breaches involve patient safety, proper incident response may mean the difference between life and death. This exercise will challenge all participants to think about critical actions and timelines, legal and compliance requirements, and outcomes, as the details of this important biomedical device tabletop exercise unfold live.
11:45 a.m.–12:30 p.m.	**Networking Lunch**	
Afternoon Tracks	***Privacy***	***Security/Cybersecurity***
12:30–1:30 p.m.	***Identify Privacy Strengths and Weaknesses by Using Data Analytics and Data Integration Strategies.*** Jill Burrington-Brown, MS, RHIA, FAHIMA, Information Services, Skagit Regional Health, Mt. Vernon, WA **and** Brienne Gahan, Information Services, Skagit Regional Health, Mt. Vernon, WA The HIPAA Security Rule requires that covered entities are not only required to ensure confidentiality, but to protect**,** detect**,** contain and correct privacy and security violations. Detecting inappropriate access or use of any PHI is difficult in most systems, and often is not proactive, but reactive to complaints. Acquire insight from this organization's year-long experience with applying a commercially available solution and the effect on its privacy compliance.	***Dealing with New Technologies*****.** Ronald Hedges, JD, Dentons US LLP, New York **and** Gail Gottehrer, JD, Law Office of Gail Gottehrer, Stamford, CT Do you understand the potential healthcare benefits of wearable devices and medical apps, as well as the privacy, cybersecurity, and other legal implications of these technologies? Be better prepared to evaluate whether a healthcare provider should use wearables and healthcare apps, and which ones are the best choice for the healthcare provider.

AHIMA Privacy and Security Institute Agenda

AHIMA19 Health Data and Information Conference

McCormick Place—Lakeside Center, Chicago, IL

1:30–2:30 p.m.	***Into the Breach: Successfully Coming Out on the Other Side.*** Daniel Sergile **and** Scott Ruthe, Ciox Health, Alpharetta, GA Want to hear what is needed to be successful during a breach? What to learn what key elements are required in every organization, and when and how to leverage those elements? Presenters use several mock scenarios taken from real world breaches and show how missing an element could be devastating for an organization. They work through timelines, when to engage and deploy departments, and assets along the timeline.	***Phishing, Shoulder Surfing, Drafting–Avoiding Social Engineering Exploits.*** Chris Apgar, CISSP, Apgar & Associates, LLC, Tigard, OR Social engineering has been around longer than computers and continues to represent a significant risk to healthcare organizations in the US and globally. This session will include covering real life examples of social engineering and what can go wrong. Participants receive tools they can use in their work and personal lives to protect PHI and other sensitive information as well as technologies and training that will, if understood and used properly, reduce risks significantly.
2:30–3 p.m.	**Networking Break**	
3–4:30 p.m.	Closing Session Address - ***Catholic Health Initiatives and Dignity*** – Ram Ramadoss, MBA, CISA, CISM, CISSP, CRISC, CIPP, Catholic Health Initiatives, Englewood, CO	
4:30–4:45 p.m.	**Institute Wrap-up and Feedback**	

CEUs: 7.5

Premier Sponsors:

Sponsors: