


**(Agenda Subject to Change)**

## WEDNESDAY, DECEMBER 16, 2020



### The Best Defense is a Good Offense; Embracing Change in Order to Protect the Industry

**Time: 11:00am- 11:30am EST**

**Jeanette Manfra, Director of Government Security and Compliance**
*Google Cloud*

Jeanette Manfra is the Director for Government Security and Compliance within the Google Cloud Office of the CISO. Jeanette is focusing on helping customers, particularly those in regulated industries, build and maintain the highest levels of security and trust into their technical infrastructure and services. Prior to joining Google, Jeanette was the Assistant Secretary for Cybersecurity and the Cyber and Infrastructure Agency within the US Federal Government. In that role she was responsible for driving security modernization across Federal civilian agencies as well as enabling the security of critical infrastructure across the US. Jeanette spent more than a decade serving in various roles at the Department of Homeland Security and the White House focused on establishing the nation's first civilian cyber defense agency.



### OCR Ransomware Guidance and HIPAA Security Rule Provisions

**Time: 11:30am- 12:00pm EST**

**Nicholas Heesters, Senior Advisor for Cybersecurity**
*HHS Office of Civil Rights (OCR)*

Nicholas Heesters is a certified information privacy professional with over 25 years of experience supporting technology and information security across many diverse industries. Mr. Heesters earned his Master of Engineering in Computer and Software Engineering from Widener University and Juris Doctor from the Widener University School of Law. Currently, Mr. Heesters leads a team of security professionals supporting OCR's HIPAA Security Rule compliance and enforcement activities for the U.S. Department of Health and Human Services Office for Civil Rights.





## Incident Response Guidance; How to Respond Practically and Legally

**Time: 12:00pm – 12:30pm EST**

**Lee Kim, Director of Privacy & Security**
*HIMSS*
**Iliana Peters, Shareholder**
*Polsinelli*

Lee Kim is the director of privacy and security at the Healthcare Information and Management Systems Society (HIMSS) North America. Lee's roles include subject matter expert, public policy professional, and analyst. Lee authors domestic and international works on topics that include information privacy, cybersecurity, law, and public policy. Her publication credits include GCN, ABA, Digital Health Legal, Nursing Management, and the California Continuing Education of the Bar.

Iliana L. Peters believes good data privacy and security is fundamental to ensuring patients' trust in the health care system, and to helping health care clients succeed in an ever-changing landscape of threats to data security. She is recognized by the health care industry as a preeminent thinker and speaker on data privacy and security, particularly with regard to HIPAA, the HITECH Act, the 21st Century Cures Act, the Genetic Information Nondiscrimination Act (GINA), the Privacy Act, and emerging cyber threats to health data.

## Lunch Break

**Time: 12:30pm- 1:00pm EST**

## Understanding the Threat- Ransomware and the Healthcare Industry



**Time: 1:00pm- 1:30pm EST**

**Greg Singleton, Director, Health Sector Cybersecurity Coordination Center (HC3)**
*HHS*

The Health Sector Cybersecurity Coordination Center (HC3) is a U.S. HHS group working to improve cybersecurity in the healthcare and public health sector. Greg previously worked at the Department of Energy as a Senior Advisor on power grid cybersecurity, critical infrastructure protection, and grid resilience. He holds a BS in Systems Engineering from the University of Virginia, and MS degrees in Political Science and Technology & Policy from the Massachusetts Institute of Technology.



## Invest in Your Security; Best Practices for Cybersecurity Planning and Infrastructure

**Time: 1:30pm – 2:00pm EST**

**Kevin Charest, Senior VP, Chief Information Security Office**
*Health Care Service Corporation*

Dr. Kevin Charest serves as the divisional senior vice president and Chief Information Security Officer for Health Care Service Corporation (HCSC). He is responsible for all aspects of IT security operations across HCSC's five health plan states, including

actively monitoring and mitigating current cyber-threats and overseeing the governance, risk and compliance program.

Dr. Charest comes to HCSC from UnitedHealth Group, where he served as VP, IT Security and Cyber Defense Operations. Prior to joining UnitedHealth Group, he served as the Chief Information Security Officer for the Department of Health and Human Services (HHS) and was directly responsible for the HHS cybersecurity technology portfolio.





## After the Storm; Lessons Learned from Ransomware Attacks

**Time: 2:00pm- 3:15pm EST**

**John Klimek, Senior VP Industry Information Technology**
*NCPDP*
**Andrew Fitzpatrick, Operations and Licensing**
*X12*
**Adam Dean, Senior Security Specialist**
*GreyCastle Security*

John Klimek R.Ph. is Senior Vice President, Industry Information Technology with the National Council for Prescription Drug Programs (NCPDP). His main objective in this current position at NCPDP is to work with industry leaders in healthcare to achieve interoperability amongst the healthcare standards, which will ultimately increase healthcare efficiencies and safety.

Andrew Fitzpatrick has more than 25 years of experience successfully leading the development and delivery of technology solutions for health care providers, payers, and government agencies in North America. In addition to supporting X12's standards development and publishing technologies, he is a strong advocate for collaborative stakeholder initiatives.

Adam Dean is a Senior Security Specialist at GreyCastle Security with over 5 years of experience as a digital forensics and security incident response professional. As GreyCastle Security's Incident Response Subject Matter Expert, Adam consults with clients nationwide specializing in healthcare, higher education, critical infrastructure, and other prominent industries who are experiencing security incidents ranging from malicious infections to data breaches. Adam notably lead the successful response and forensic investigation involving a security incident at a level 1 trauma center which fell victim to a ransomware attack, compromising over 6,000 systems and causing the hospital to temporarily revert to paper charting.

.







## Get Your Playbook Ready; Preparation and Protection for the Future

**Time: 3:15pm- 4:00pm EST**

**Julie Chua, Risk Management Branch Chief**
*HHS*
**Lee Barrett, Executive Director and CEO**
*EHNAC*
**Erik Decker, Chief Security and Privacy Officer**
*University of Chicago Medicine*

Julie Chua is the Director of the Governance, Risk Management, and Compliance (GRC) Division within the HHS Office of Information Security (OIS). Julie established a Department-wide cybersecurity risk management program and spearheaded the integration into HHS' Enterprise Risk Management framework. She is responsible for high-priority, high-visibility initiatives including the establishment of the HHS High Value Asset (HVA) Program for the identification, protection, and prioritization of HHS' most critical high value assets and oversees the HHS FedRAMP and Cloud Security Program. Julie is also the Federal Lead for the implementation of the Cybersecurity Act (CSA) of 2015, Section 405(d): *Aligning Health Care Security Approaches*.

Lee Barrett has been recognized as a top HIT national leader. Mr. Barrett serves as the Executive Director of Electronic Healthcare Network Accreditation Commission (EHNAC), a national 501c6 non-profit nationally recognized accreditation organization focused on providing stakeholder trust regarding managing risk mitigation strategies around reducing risk of HIPAA breach, incident and Cybersecurity/Ransomware attacks and Organizational Readiness Plans. EHNAC is nationally recognized for its focus on risk mitigation for organizations as it provides a framework for review of privacy, security including cybersecurity/ransomware, technical/operational infrastructure, best practices, and resources.

Erik Decker is the Chief Security and Privacy Officer for the University of Chicago Medicine, and is responsible for its Cybersecurity, Identity and Access Management and Privacy Program. Erik has 20 years of experience within Information Technology, with 14 years focused on Information Security. The majority of his career has been focused on Academic Medical Centers; establishing two information security programs and an identity and access management program.

He is currently Co-Leading a Department of Health and Human Services (HHS) task group of more than 250 industry and government experts across the country for implementing the Cybersecurity Act of 2015, 405D legislation within the Healthcare sector.



## Closing Remarks

**Time: 4:00pm EST**

**Charles Stellar, President and CEO**
*WEDI*

**Thank You to our Sponsor Axway.**
**Click on their logo to learn more about their products and solutions**