



National Committee on Vital and Health Statistics

Virtual Hearing on Security in Healthcare and Public Health

Speaker Bios

July 14, 2021

Panel I – Addressing Healthcare Security Challenges

- **Erik Decker; Assistant Vice President/Chief Information Security Officer, Intermountain Healthcare**
Erik is the Assistant Vice President – Chief Information Security Officer at Intermountain Healthcare. Previously Erik was the Chief Security and Privacy Officer for the University of Chicago Medicine, where he was responsible for its Cybersecurity, Identity and Access Management and Privacy 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. Additionally, he led the development of the Health Industry Cybersecurity Tactical Crisis Response guide (HIC-TCR) under the same working group. He is also a member of the Executive Council of the Healthcare Sector Coordinating Council's Joint Cybersecurity Work, which is a public-private workgroup formed under the National Infrastructure Protection Plan. Erik earned his Master of Science in Information Technology from Loyola University in Chicago and bachelor's degree from the University of Illinois in Champaign/Urbana in Cell and Structural Biology.
- **Jane Wong, Vice President and Associate Chief Information Officer of UCSF Health**
Jane Wong is the Vice President and Associate CIO for enterprise applications in the UCSF information technology department. She joined UCSF from the commercial sector, and she has brought with her the culture of innovation and creativity. Jane continues to serve as WIT@UCSF's executive sponsor and mentor.
- **Sabrina Kidd, MD, FACS, FASCRS, Chief Medical Officer, UCSF Health**
Dr. Sabrina Kidd is the Chief Medical Officer and UCSF Medical Director for Sonoma Valley Hospital and is a dual board certified colorectal and general surgeon. Her practice includes the surgical treatment of colorectal cancer, benign colon and rectal disorders, anorectal disorders, colonoscopy, gallbladder disease, and much more. Dr. Kidd is a volunteer with Operation Access, a not-for-profit that enables Bay Area health care providers to donate vital surgical and specialty care to people in need. Outside of the operating room, she enjoys being active outdoors and spending time with family and friends.
- **Denise Anderson, President of H-ISAC**
Denise Anderson is President of the Health Information Sharing and Analysis Center (H-ISAC). Prior to H-ISAC, she was a Vice President of FS-ISAC where for almost nine years she helped the ISAC grow and achieve its successful status in the information sharing community. She has over 25 years of executive management level experience in the private sector. Denise currently serves as Chair of the National Council of ISACs (NCI). She was instrumental in implementing a CI/KR industry initiative to establish a private sector liaison seat at the National Infrastructure Coordinating Center (NICC) to enhance information sharing between the private sector, CI/KR community and the federal government and serves as one of the liaisons. She is a health sector representative to the National Cybersecurity and Communications Integration Center (NCCIC) — a Department of Homeland Security-led coordinated watch and warning center that improves national efforts to address threats and incidents affecting the nation's critical information technology and cyber infrastructure. Denise was certified as an EMT (B), and Firefighter I/II for twenty years and as an Instructor I/II and state EMT evaluator in Virginia for over ten years. Denise holds an MBA in International Business and is a graduate of the Executive

Leaders Program at the Naval Postgraduate School Center for Homeland Defense and Security.

Panel II – State, Tribal, and other Perspectives on Healthcare Security

- **John Guerriero, Cybersecurity Program Director - Acting, National Governors Association**
John Guerriero serves as a cybersecurity policy analyst on the Homeland Security & Public Safety team of NGA's Center for Best Practices, where he supports Governors' staff and state policymakers on issues related to cybersecurity, including governance, workforce development, and election security. Prior to joining the homeland security team at NGA, John focused on workforce development, including registered apprenticeship and occupational licensing, as a part of NGA's Economic Opportunity team. John holds a master's degree in public policy and a bachelor's degree in political science from the University of Michigan.

Panel III — Emerging Security Threats and Preparedness Across the Healthcare Industry

- **Suzanne Widup; Senior Analyst, Verizon Enterprise Solutions**
Suzanne Widup is a co-author of the Verizon Data Breach Investigations Report, and lead author for the Verizon PHI Data Breach Report. She spends quality time hunting for publicly disclosed data breaches for the VERIS Community Database (vcdb.org). Suzanne has 20 years of IT experience, including unix system administration, information security engineering and digital forensics in large enterprise environments. She holds a B.S. in Computer Information Systems and an M.S. in Information Assurance. Suzanne is the author of Computer Forensics and Digital Investigation with EnCase Forensic v.7, published by McGraw-Hill.
- **Kevin Stine; Chief of the Applied Cybersecurity Division in the National Institute of Standards and Technology's Information Technology Laboratory (ITL)**
Kevin Stine is the Chief of the Applied Cybersecurity Division in the National Institute of Standards and Technology's Information Technology Laboratory (ITL). He is also NIST's Acting Chief Cybersecurity Advisor and Acting Associate Director for Cybersecurity in NIST's ITL. In these roles, he leads NIST collaborations with industry, academia, and government to improve cybersecurity and privacy risk management through the effective application of standards, best practices, and technologies. The Applied Cybersecurity Division develops cybersecurity and privacy guidelines, tools, and reference architectures in diverse areas such as public safety communications; health information technology; smart grid, cyber physical, and industrial control systems; and programs focused on outreach to small businesses and federal agencies. The Division is home to several priority programs including the National Cybersecurity Center of Excellence, Cybersecurity Framework, Cybersecurity for IoT, Identity and Access Management, Privacy Engineering and Risk Management, and the National Initiative for Cybersecurity Education.

Panel IV – Federal Perspectives on Security Infrastructure and Enterprise-wide Risk Management in Healthcare

- **Julie Chua; HHS Security Risk Management Division Manager, Office of Information Security (OIS) and Government Co-Lead of the 405(d) Task Group**
Julie Chua is the Director of Governance, Risk Management and Compliance (GRC) Division within the U.S. Department of Health and Human Services (HHS) Office of Information Security (OIS). Julie is also the Federal Lead for the implementation of the Cybersecurity Act (CISA) of 2015, Section 405(d): Aligning Healthcare Cybersecurity Approaches. This public-private partnership effort is one of many HHS cybersecurity initiatives to help push forward the cybersecurity and resiliency of the HPH sector.
- **Kevin Fu; Acting Director of Medical Device Cybersecurity, FDA's Center for Devices and Radiological Health**
Kevin Fu is Acting Director of Medical Device Cybersecurity in the FDA's Center for Devices and Radiological Health. Kevin is Associate Professor of EECS at the University of Michigan where he

directs the Security and Privacy Research Group (SPQR.eecs.umich.edu). His research focuses on analog cybersecurity—how to model and defend against threats to the physics of computation and sensing. His embedded security research interests span from the physics of cybersecurity through the operating system to human factors. Past research projects include MEMS sensor security, pacemaker/defibrillator security, cryptographic file systems, web authentication, RFID security and privacy, wirelessly powered sensors, medical device safety, and public policy for information security & privacy. Kevin received his B.S., M.Eng., and Ph.D. from MIT. He earned a certificate of artisanal bread making from the French Culinary Institute and is an intermediate level salsa dancer.

- **Timothy Noonan, Deputy Director; Health Information Privacy Division; HHS Office for Civil Rights**
Timothy Noonan is the Deputy Director for Health Information Privacy, at the Office for Civil Rights (OCR), United States Department of Health and Human Services. The Health Information Privacy Division administers and enforces the Health Insurance Portability and Accountability Act (HIPAA) Privacy, Security and Breach Notification Rules and the Patient Safety and Quality Improvement Act and Rule through investigations, rule-making, guidance, and outreach. Previously, Tim served in OCR headquarters as the Acting Associate Deputy Director for Operations and the Acting Director for Centralized Case Management Operations. Tim joined OCR as the Southeast Regional Manager in November 2013. Prior to joining OCR, Tim was a Supervisory General Attorney for the U.S. Department of Education, Office for Civil Rights, and a shareholder in a Michigan law firm. Tim is a graduate of Michigan State University and Wayne State University Law School.