HIMSS Maryland Chapter Meeting - "Protecting Maryland's Cyberspace"

December 2, 8:00am - 12:45pm, EST

Presenter: Greg Porter (info[at]alleghenydigital[dot]com)

Topic: Healthcare Cybersecurity Essentials

Presentation Resources

1. ***Center for Internet Security ("CIS") Critical Security Controls***: The CIS Critical Security Controls ("CIS Controls") are a concise, prioritized set of cyber practices created to stop today's most pervasive and dangerous cyber-attacks. The CIS Controls are developed, refined, and validated by a community of leading experts from around the world. The CIS Controls and additional information about them is available here: https://www.cisecurity.org/critical-controls.cfm

2. ***The CERT Resilience Management Model ("CERT-RMM")*** is the foundation for a process improvement approach to operational resilience management. It defines the essential organizational practices that are necessary to manage operational resilience. You can use CERT-RMM to determine your organization's capability to manage resilience, set goals and targets, and develop plans to close identified gaps. By using a process view, CERT-RMM can help your organization respond to stress with mature and predictable performance. Additional information about CERT-RMM is available here: https://www.cert.org/resilience/products-services/cert-rmm/

3. ***The U.S. Department of Health and Human Services ("HHS") Office of the Inspector General ("OIG")*** is the largest inspector general's office in the Federal Government, with approximately 1,600 employees dedicated to combating fraud, waste and abuse and to improving the efficiency of HHS programs. A majority of OIG's resources goes toward the oversight of Medicare and Medicaid — programs that represent a significant part of the Federal budget and that affect this country's most vulnerable citizens. Additional information regarding the OIG audits and electronic health records ("EHR") is available here: https://oig.hhs.gov/

4. ***Breaches Affecting 500 or More Individuals***. As required by section 13402(e)(4) of the HITECH Act, the Secretary must post a list of breaches of unsecured protected health information affecting 500 or more individuals. These breaches are now posted in a new, more accessible format that allows users to search and sort the posted breaches. Additionally, this new format includes brief summaries of the breach cases that OCR has investigated and closed, as well as the names of private practice providers who have reported breaches of unsecured protected health information to the Secretary. Please visit the following URL for additional information: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf