CLINICAL CYBERSECURITY – BEATING THE CYBER VIRUS LIKE A HUMAN VIRUS

By Erik Decker – 405(d) Industry Task Group Lead

Doctors and nurses know that washing their hands is critical to prevent the spread of viruses. However, that does not mean health care workers wash up as often as they should. Similarly, we know that cybersecurity practices reduce the risk of cyber-attacks and data breaches. Just like washing your hands before caring for patients can reduce infections, good cybersecurity practices can reduce the impact of cybersecurity threats and vulnerabilities. Given the increasingly sophisticated and widespread nature of cyber-attacks, the health care industry must make cybersecurity a priority and make the investments needed to protect its patients. Like combatting a deadly infection, cybersecurity requires mobilization and coordination of resources across a myriad of public and private stakeholders, including hospitals, IT vendors, medical device manufacturers, and governments (state, local, tribal, territorial, and federal) to mitigate the risks and minimize the impacts of a cyber-attack.

Cyber Safety is Patient Safety. To aid organizations and to improve approaches and coordination across the sector, the U.S. Department of Health and Human Services and the Health Industry formed a joint Task Group called 405(d), and released the *Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients (HICP).*

The HICP publication aims to raise awareness, provide vetted cybersecurity practices, and move towards consistency in mitigating the current most pertinent cybersecurity threats to the sector. It seeks to aid Healthcare and Public Health organizations to develop meaningful cybersecurity objectives and outcomes. Recognizing that cybersecurity recommendations are rarely one-size-fits-all solutions, the document, which is available to the public, compiles practices specific to healthcare organizations of varying sizes, ranging from small physician practices to large hospital systems. Various audiences can leverage the publication to raise awareness for executives, healthcare practitioners, and hospital employees. Additionally, it provides detailed technical implementation recommendations for IT and information security professionals. Your organization's vigilance against cyber-attacks will increase concurrently with your workforce's knowledge of cybersecurity. This knowledge will enable you to advance to the next series of cybersecurity practices, expanding your organization's awareness of and ability to thwart cyber threats.

Health care organizations must practice good "cyber hygiene" in today's digital world, including it as a part of the daily universal precautions. Like the simple act of washing your hands, a culture of cyber-awareness does not have to be complicated or expensive. Just as we can protect our patients from infections by washing our hands, we should all work towards protecting patient data to allow physicians and caregivers the ability to trust the data and the systems that enable quality health care. In

summary, every member of a health care organization must remember that cyber safety is patient safety.