Healthcare & Public Health Sector Coordinating Councils

PUBLIC PRIVATE PARTNERSHIP

The Healthcare Cyber Circulatory System – Supply Chain Security

October 16 - Just like the human body itself, the healthcare industry is a circulatory system, not of blood but a complex chain of medical procedures, device manufacturing and management, data recording and transmittal, and payment processing. This circulatory system is our supply chain – the supply of services, products and data. And the suppliers make up a complex eco-system of interdependent organizations of all sizes, spanning patient care, payment and data management systems, pharmaceutical and technology research and manufacturing, and public health administration. These interdependencies mean that a cybersecurity event in one organization is likely to have ripple-effects on multiple other links within the supply chain.

This October we observe National Cyber Security Awareness Month, and we in the health sector are taking stock of the many ways this sector has become subject to myriad cyber threats that jeopardize the delivery of care and patient safety. The effects of a cyber incident or disruption can include loss of patient data and payment information; theft of intellectual property; or exploitation of medical device vulnerabilities that lead to disruption of functionality or patient harm. The growth of ransomware in recent years, by which hackers are able to encrypt entire systems of data in a hospital or clinical environment and demand ransom for its release, threatens the availability of critical health systems, leaving organizations unable to provide services or distribute the products relied upon by patients and health professionals.

In response, larger organizations have dedicated resources to improve their resiliency through rigorous attention to ensuring that the products and services they procure – and the suppliers they procure them from – are hardened against the many cyber threats and vulnerabilities that afflict the healthcare system. Many small-to-medium sized organizations, however, lack the scale or the budget to staff dedicated teams of cybersecurity experts.

To that end, the Health Sector Coordinating Council has produced a toolkit for the sector, called the Health Industry Cybersecurity Supply Chain Risk Management Guide (HIC-SCRiM). It is intended primarily for leadership in small-to-medium sized organizations, providing actionable guidance and practical tools to enable those organizations to manage the cybersecurity risks they face through their dependencies within the health system supply chain. The imperative is that healthcare organizations – from health providers to device and pharmaceutical manufacturers, labs and payers – step up their demands for secure products and services from their suppliers, which in turn will leverage market forces to raise the bar across the healthcare supply chain to the benefit of all.

While the guidance and tools presented are aimed primarily at small and medium sized organizations, the call to action is for larger organizations to:

- Use their reach within the supply chain to disseminate this document to their suppliers and recommend that they incorporate these practices into their own organizations, encouraging their suppliers to do the same in turn.
- Review their own supplier risk management program against the best practices laid out in this document.
- Join the Health Sector Coordinating Council's Joint Cybersecurity Working Group to actively shape health-sector supplier risk management.

All through this circulatory system called the supply chain, there are too many cyber security points of failure that often leave the health care provider unaware of the vulnerabilities and unable to deal with them either in an urgent care situation or in routine treatment, putting the patient at risk. So it is during this National Cyber Security Awareness Month that we must inject a dose of reality into our supply chain operations and recognize that patient safety depends on supply chain cyber safety.