HealthManagement
Promoting Management and Leadership

Infosec third-party risk management

Prominent CISOs from leading health systems and hospitals in the USA have launched a new initiative to better manage information security-related risks in their supply chains and to safeguard patient safety and information. A key part of this initiative was the establishment of the Provider Third Party Risk Management Council.

The founding member organisations for the Provider Third Party Risk Management Council include Allegheny Health Network, Cleveland Clinic, University of Rochester Medical Center, UPMC, Vanderbilt University Medical Center, and Wellforce/Tufts University.

Members of the Council observed their supply chains are filled with third parties who support the care delivery process and require access to patient information. Properly vetting and monitoring these third parties is a major challenge, and in some cases, insurmountable for many organisations who simply don't have the expertise or resources.

Through innovation and industry leadership, the Council is developing common vetting and oversight practices that will benefit health systems, hospitals and other providers in the U.S. and around the world.

"Health systems and other providers need to be more active in assessing and monitoring risks posed by third parties to protect patient information while delivering effective care," says Taylor Lehmann, CISO of Wellforce, parent organisation of a health system that includes Tufts Medical Center and Floating Hospital for Children. "The primary challenge is organisations can engage with vendors of various sizes, maturity and complexity without really knowing whether the vendor should be engaged in the first place based on their beliefs and investment in cybersecurity."

Third parties may have a small number of customers or possibly hundreds or thousands to serve, Lehmann points. For third parties, this challenge has resulted in lost time and resources in attempting to comply with each organisation's risk management requirements and ensure efficiency for both parties.

The Council is working with the HITRUST CSF and its assurance programmes for this initiative to better manage risk. The organisations on the Council have each independently decided to require their third-party vendors to become HITRUST CSF Certified within the next 24 months. The HITRUST CSF Certification will serve as their standard for third parties providing services that require access to patient or sensitive information and will be accepted by all the Council's organisations.

By choosing to adopt a single assessment and certification programme, healthcare organisations represented by the Council are prioritising the safety, care, and privacy of their patients by providing clarity and adopting best practices that their vendors can also adopt, while providing vendors the expectation of what it takes to do business with their organisations.

"We believe the healthcare industry as a whole, our organisations and our third parties will benefit from a common set of information security requirements with a standardised assessment and reporting process," says John Houston, Vice President, Privacy and Information Security & Associate Counsel, UPMC. "We are strongly encouraging other provider organisations to follow suit and adopt these principles."

Source: Help Net Security
Image Credit: Pixabay

Published on : Fri, 7 Sep 2018