Securing Health Information Exchanges in a Modern Healthcare Network

By Perry Hutton, Regional Director – Africa at Fortinet

Healthcare providers are migrating from large, independent stand alone organizations into complex new ecosystems. Today Provider Organizations, affiliated physician groups, labs and others are involved in both the provisioning of care, and the collection of vast amounts of information from patients. Health Information Exchanges (HIEs) are evolving and are a more affordable means to transfer clinical information and other data.

Healthcare as we know it is changing quickly. Healthcare providers will soon be required to provide communication and collaboration platforms that allow seamless integration among the various stakeholders. These changes in information flows, along with an explosion of digital content that needs to be stored and shared, are driving the need for a secure, flexible and scalable IT platform through which Providers, Payers and Health sciences can support collaboration and information exchange.

The transition towards more patient-centric care and decentralized monitoring means providers, patients and payers need to access information that originates outside the hospital setting. The trends toward personalized medicine, prevention, and wellness means stakeholders need to connect information from various points within the healthcare value chain – including providers, laboratories, payers, and patients. The more this private information is opened to outside entities, the greater the chance that these systems can be compromised either intentionally or accidently.

Upcoming trends in a healthcare industries network

The major challenges to a healthcare provider's network arises from the different business functions increasingly taking place in their network.

- **Allowing Patient and Provider Access to the Network**

  As contradictory as it sounds, healthcare providers are now looking for ways to increase the access doctors, vendors, and patients have to applications and the Internet. With new guarantees for patients regarding access to information and a focus on lowering costs through new initiatives like telemedicine, the entire healthcare centre is driving towards a more collaborative environment where all parties have access to the information they need.

  The most obvious security concern with this approach is ensuring that sensitive information like protected health information (PHI) and payment information is kept separate and secured from general Internet and network traffic. This requires encryption and wireless management technology coupled with traffic shaping technology to ensure that the appropriate treatment information is accessible and is always the top priority.

- **Increased Use of Clinical Informatics to Improve Workflow**

  Along with the increased collection and flow of data, healthcare organizations are constantly striving to improve workflow, both physical and information. Improved workflows equal lowered costs, happy and productive caregivers and an environment that allows improved patient safety and quality care. The key challenge from a security perspective is ensuring that only the required pieces of data are transferred and nothing more.

- **Increasingly Stringent Compliance Mandates**

  As a result of the increasingly sensitive data handled by the healthcare industry, regulatory requirements have been implemented to help increase the security of healthcare providers and associates as well as the data they protect. HIPAA and HITECH set up standards around protecting PHI.

  Healthcare organizations also find themselves responsible

for complying with the Payment Card Industry Data Security Standard (PCI DSS). PCI DSS provides broad requirements for securing personal non public information used on digital technology in retail systems.

Towards a secure health architecture

All the challenges mentioned above require disparate functionality. Healthcare service providers need to evaluate their security needs at each of the following levels:

- **Management Level**
  Given the widely distributed nature of modern healthcare establishments, the ability to quickly modify and manage security appliances is essential.

- **Aggregation Level**
  The aggregation level is the destination for all data. Typically this is the hospital datacentre. Core security functions such as firewalling, application control and VPN termination take place at this level.

- **Business Associate Level**
  The individual clinic, lab, doctor's office, or any business associate requires security and connectivity for a wide variety of functions including WiFi, voice, and traditional network connectivity. With the addition of consumer connectivity, each associate much also be able to provide security functions such as antimalware and application control.

- **Access Level**
  As healthcare organizations extend access to providers using tablets and to patients using mobile devices, ensuring secure access is critical.

The entire healthcare industry is undergoing a dramatic shift designed to enhance the level of care provided to patients. The sensitivity of patient information has created the need for end-to-

end security solutions throughout the entire healthcare network – from doctor's offices all the way to the hospital data centre.

Healthcare providers can no longer afford to take security lightly. Only with security as the foundation can healthcare organizations build IT services and applications that meet the requirements of the business and healthcare mandates.
/Ends.