DATA FUELS INTELLIGENCE & IMPROVED OUTCOMES. **BE SURE IT'S PROTECTED.**

Digitized health data has enormous potential to drive intelligence and improved outcomes. As data grows in volume and complexity, organizations are looking for ways to effectively manage and protect information, derive actionable insights and scale decision support tools.

Below are five security considerations driving the adoption of wavelength encryption technologies to better secure and optimize in-flight data across the healthcare continuum.

The Proliferation of IoT:

The Internet of Things (IoT) can deliver groundbreaking contextual insights, real-time visibility and granular data points painting a more holistic picture of patient activities and hospital operations. While this intelligence has countless applications and use cases, there are complex and serious security implications to consider. IoT-enabled devices can generate tremendous amounts of sensitive data that may be shared across the care continuum. Encrypted Layer 1 connectivity enhances the security of data travelling outside data centers and core locations to protect in-flight information across multiple protocols and all upper network layers.

Technology Should Help, Not Hinder, Care:

Decision support tools, patient enablement applications and M2M learning are just a few technologies that have exciting potential to improve outcomes. However, network infrastructure must be both scalable and secure to ensure optimal performance. Existing in-flight encryption options at the application layer (e.g. HTTPS/SSL) and Layer 3 (IPSec) can seriously impact latency and stifle/limit scalability. In fact, 74% of enterprises cite system performance and latency as the most critical feature when considering encryption technology solutions.[1] Encrypted waves connectivity is a secure solution that better supports a high-performing, low-latency networking environment.

Protect PHI and Care Continuity:

Healthcare IT leaders cite "dealing with security threats" as a top challenge[2], and one third of respondents in a 2017 study expressed a high level of concern that a breach could impact care at their organization within 12 months.[3] As a result, players are developing security strategies that better protect PHI and care continuity. According to Gartner, "through 2020, driven by the increasing risk of a data breach, more than 50% of enterprises will purchase enterprisewide encryption products, which is a significant increase from fewer than 20% today."[4] You can better protect confidential information and help ensure uninterrupted care delivery by supporting key applications with in-transit Layer 1 encryption across your interconnected data center and key locations.

Overcome Compliance Challenges:

While HIPAA compliance is an important piece of a comprehensive security strategy, it's not exhaustive. Today's providers must deploy secure networking solutions that evolve and respond to the cyber-crime landscape. In a recent report, "55 percent of respondents see compliance with privacy and data security requirements as the main driver to using encryption technologies."[5] With vast amounts of PHI data traversing the network, wavelength encryption can help providers ensure security compliance, while creating an additional layer of defense. Building security into networking solutions will help healthcare organizations strengthen their security postures beyond HIPAA to stay ahead.

Cut Down on Complexity:

Healthcare organizations operate within large and rapidly evolving ecosystems, creating complex security architectures and networks to manage and control. As a result, healthcare organizations have one of the highest industry rates of encryption usage.[6] Today's IT leaders must design agile networks that ensure business continuity while also protecting critical information. Optical transport encryption through the network provider helps organizations move away from on-premises hardware models to "encryption as a service," which can reduce overhead and management complexity. And with no need to buy or manage DWDM Encryption equipment or Key Management Service tools, IT teams can free up resources and budgets to focus on core initiatives.

LEVEL 3® ENCRYPTED WAVELENGTH SERVICE: SECURE, EFFICIENT and HIGH PERFORMING

Contact Level 3 to learn more about implementing highly scalable, encrypted network connectivity to better protect your company and customer data.

[1]Ponemon, Global Encryption Trends Study, April 2017
[2]Frost & Sullivan, Digital Transformation in Healthcare, September 2016
[3]Level 3 & HIMSS Analytics, Security Study, Feb 2017
[4]Gartner, Prioritize Enterprise-Wide Encryption for Critical Datasets, 28 June 2017
[5]Ponemon, 2017 Global Encryption Trends Study, 2017
[6]Ponemon, 2017 Global Encryption Trends Study, 2017

17508717

Level 3® COMMUNICATIONS
Connecting and Protecting the Networked World℠