DATA SHEET

CenturyLink® Encrypted Wavelength Service

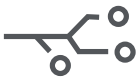
5 reasons for wavelength encryption in the healthcare industry

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.

The following are five security considerations driving the adoption of wavelength encryption technologies to secure and optimize healthcare data in flight.

1. Taking advantage 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 traveling outside data centers and core locations to protect in-flight information across multiple protocols and all upper network layers.



2. Scaling patient enablement app performance

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. According to consolidated findings, enforcement of policy, system performance and latency and support for both cloud and on-premise deployment are the three most important features.[1] Encrypted waves connectivity is a secure solution that supports a high-performing, low-latency networking environment.

CenturyLink®

3. Protecting PHI and care continuity

Healthcare IT leaders now know that data breaches have the potential to disrupt healthcare delivery.[2] In fact, according to the 2020 Frost & Sullivan Global Digital Health Outlook Report, at least 96 reports of healthcare provider data breaches or compromises involving more than 3 million records were reported to the U.S. Department of Health and Human Services Office of Civil Rights from Jan. 1 to May 1, 2019.[2] As a result, players are developing security strategies that better protect PHI and care continuity. 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.

4. Overcoming 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 cybercrime landscape. In a recent report, "46 percent of respondents see compliance with privacy and data security requirements as the main driver to using encryption technologies."[1] 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.

5. Cutting down 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 are responsible for encrypting a variety of data sets. The most common include payment, HR and customer-related data.[1] 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.

Turn to CenturyLink® Encrypted Wavelength Service to protect your customer data. Encrypted Wavelength Service is a secure, efficient and high-performing solution to meet the cycbersecurity concerns of evoloving heathcare systems. Secure, efficient and high performing.

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

[1]Ponemon Institute, *2019 Global Encryption Trends Study* 2019
[2]Frost & Sullivan Global, *Digital Health Outlook Report, 2020,* Aug. 23 2019

CenturyLink®