

## APPLICATION NOTE

# End-to-End Network Encryption for Secure Healthcare

Despite billions of dollars spent on data security in the healthcare industry, cyber attacks and data breaches continue at epidemic levels. Nearly 90 percent of healthcare providers have been hit by data breaches in the last two years, according to a 2016 Ponemon Institute study. Healthcare CIOs have realized it's no longer a matter of *if* you will be attacked, it's *when* you will be attacked. The cost of these data breaches is also rising, to nearly \$4.1 million per incident.<sup>1</sup> In addition, patients are now beginning to include cyber security as a factor when choosing their healthcare providers. These potential business impacts and the continuing onslaught of attacks is an increasingly frequent topic in covered entity and business associate board-level discussions.

Traditionally, healthcare data security strategy has focused on shoring up the perimeter. Over the past couple of years, CIOs began focusing more attention on encrypting patient data at rest, mainly due to HIPAA recommendations. But many CIOs are neglecting to encrypt data as it traverses their networks. In the aforementioned Ponemon study, 40 percent of hospitals indicated that they do not encrypt data in transit. This is an alarming statistic, given the trend toward greater sharing of Patient Health Information (PHI) between non-affiliated covered entities and business associates that need to collaborate along the continuum of a patient's treatment. For example, PHI can travel between primary care physicians, specialists, surgeons, imaging centers, home health agencies, accountants, insurance companies, and family members. In an era of analytics and big data, so much new, unstructured data is generated every day that it can be difficult for IT administrators to know where it all resides and how and by whom it is being used.

### Benefits

- Safeguards protected electronic patient information from data breach and keeps critical systems secure
- Protects valued reputations and avoids costly fines, public media exposure, and patient churn by meeting expectations for information protection
- Provides a 'safe harbor' exemption under HIPAA requirements for reporting a data breach; contributes to compliance with regulations such as PIPEDA, EUDPD, JPIPA, UKNHS

<sup>1</sup> Ponemon Institute: "Sixth Annual Benchmark Study on Privacy & Security of Healthcare"; May, 2016; by Dr. Larry Ponemon