Leveraging the Cloud to Meet Security Requirements for Telemedicine

KURT HAGERMAN   CISO, ARMOR
Kurt Hagerman
Chief Information Security Officer, Armor

As Chief Information Security Officer for Armor, Kurt is responsible for the governance, risk and compliance side of the security mission for customer facing products and issues. He regularly consults with Armor prospects and customers on PCI, HIPAA and financial services regulations and helps them understand how these regulations impact their business and how Armor can help them meet their regulatory responsibilities. Mr. Hagerman regularly speaks and writes on information security topics in the payments and health care spaces as well as on cloud security.
Agenda

01 Early challenges of telemedicine
02 Telemedicine today
03 Challenges for the health care industry
04 Why the cloud makes it easier
05 How to move to a secure cloud
06 Armor use cases
Early Challenges of Telemedicine
Growing Pains

- Bandwidth deficiencies (especially in rural areas)
- Technology challenges
- Slow adoption
Telemedicine Today
The Right Stuff

Luckily, the technology landscape has changed and telemedicine can thrive thanks to:

- Reliable bandwidth
- IoT devices
- Mobile technology
Paradigm Shift

Improving technology and demands for mobility have made telemedicine convenient – and available.

The use of telemedicine is expected to increase by 18% through 2020.

29 states and the District of Columbia require health insurers to cover telemedicine.

Challenges for the Healthcare Industry
Time for a Check Up

Despite the interest and enthusiasm, telemedicine creates challenges for the healthcare industry, including:

- Stretching already stretched budgets
- Having to manage security beyond an organization’s four walls
Why Securing in the Cloud Is Easier
Simplifying Security

Regardless of the challenges for healthcare organizations, there are many, many benefits to embracing the cloud – especially since it simplifies the challenge of security.

- Access Control
- Isolation
- Encryption
Access Control

- Limited to patient and care provider
- Multi-factor authentication
Isolation

- Easier and less complex than bolting onto existing environment because the cloud environment can be isolated
- Easier to defend
- You define the environment and know where the data is
- It was designed for the purpose of telemedicine
Encryption

- Secured communication between devices
- Logical (role-based) encryption of data at rest
Shared Responsibility in the Cloud
That means the biggest threat to your cloud is “you don’t know what you don’t know.”

95% of cloud security failures through 2020 will be the customer's fault.

Top Strategic Predictions for 2016 and Beyond – Gartner 2016
Armor Use Case
CASE STUDY – ARMOR COMPLETE

Worldwide provider of IT, technology and enterprise products and solutions

CUSTOMER NEED

- Required flexibility of the cloud for distribution
- Managed security for data captured by remote stethoscope application

SITUATION

- Large corporation seeking to secure their remote stethoscope application outside of their environment

WHY ARMOR

- Strength of security operations team
- 24/7/365 monitoring of cloud data
- Expertise in managing HIPAA environments

SOLUTION & RESULT

- Application monitored, secured and managed by people who know how rather than overburden a small IT group
Questions

KURT HAGERMAN  CISO, ARMOR