RF CODE
CRITICAL ASSET TRACKING & PROTECTION

WHITE PAPER

Healthcare at The Edge

Securing Edge Deployments and Ensuring Critical Service Availability for Patients and Providers

Introduction

The ongoing trend of pushing compute power closer to the patient is having significant impact in healthcare. Edge computing allows for clinicians and hospital administrators to deliver patient data in real-time. Any downtime causing an impact to the ability to access critical healthcare information can put patient's lives at risk, and can cost providers both financially and in reputation: It's estimated that 70% of hospitals have had a patient accidentally injured during unplanned downtime and that electronic medical records downtime can cost healthcare providers upwards of $8,662 per minute that the records system is unavailable.[1]

To ensure uptime and the delivery of real-time IT services for patient care, healthcare providers are moving from a centralized traditional enterprise data center to a distributed model across wholly owned, collocated, and edge data centers spaces. Not only is this changing user experience, but it's impacting the management of the infrastructure delivering these services. What challenges await and how can healthcare IT teams be prepared to deal with them? What do IT professionals need to keep in mind when making decisions related to operations management?

> *"By enabling edge computing, crucial data can be transmitted ... to the hospital in real time, saving time and arming emergency department teams with the knowledge they need to save lives."*
>
> *– Weisong Shi, Wayne State University in HealthTech: "Will Edge Compuitng Transform Healthcare?"*

Healthcare at The Edge

Healthcare IT is home to electronic health records (EHR), electronic medical records (EMR), patient billing information, and electronic protected health information (ePHI), accessible via:

- Centralized, on-precise, and cloud data centers

1 MedHost, "Infographic: The Hidden Costs of EHR Downtime" https://ont/infographics/infographic-hidden-costs-ehr-downtime/

- Large edge sites, including hospitals and call centers
- Smaller edge sites for individual practices and offices

As the technology stack gets closer to the patient, the business value of delivering secure, real-time patient data and analytics increases. Implementing edge technologies can mean fewer visits for the patient, increasing customer satisfaction and impacting decisions for future visits[2]. Delivering these services requires technology that clinicians and healthcare providers are not used to managing and supporting. The servers, routers, and infrastructure supporting the IT solutions are just as critical as the software running in the clinic. And ensuring that the underlying technology stack is properly accounted for, secured, and maintained is paramount for healthcare providers.

How Healthcare Providers are Using the Edge

Edge computing requires that clinicians and healthcare providers and their patients are located in close proximity to the IT equipment infrastructure. The real-time capabilities of edge computing enables patient-critical functions such as:

- **Accessing patient records in real-time via tablets:** Locally cached records and access to patient EMR/EHR prior to appointments allows providers to see more patients in a given time window'
- **Uploading health data from patient wearables and monitoring devices:** Data generated from patient devices can provide actionable results sooner than results collected during one appointment and reviewed during the next
- **Collaborative input:** Low latency connections at multiple offices as endpoints can provide a single point of service for input from multiple clinicians, and improve patient experience

2 HIT Infrastructure, "Healthcare Edge Computing Supports Increased Data Processing Needs" https://hitinfrastructure.com/news/healthcare-edge-computing-supports-increased-data-processing-needs

- **Shorter analytics compute time:** More computing power at the edge reduces network traffic back-and-forth for the analysis of tests or monitoring data and could mean fewer follow-ups for the patient

- **Viewing complex imaging results:** Local caching and digital transport of large imaging files alleviates the need for a patient to visit multiple provider locations and increases patient satisfaction

- **Verification of insurance and expedited check-ins and check-outs:** Digital patient records allow reception to focus on more complex tasks, and facilitates self-service for tasks like scheduling visits

All of these services are becoming less of a nice to have and more the basic requirements for providers to earn a patient's business. And delivering these services requires servers and storage connected to the enterprise network via reliable low-latency connections. No matter how far the endpoint is from the core data center, it has the same demands and accountability requirements – often more so – as enterprise IT infrastructure.

Yet, unlike a corporate data center that is staffed and monitored around the clock, edge computing infrastructure is installed in remote, often lights-out, environments, typically lacking appropriate staff and proper monitoring of equipment and environmental conditions. Addressing issues at these remote sites carries higher costs and takes longer to resolve – without IT staff on-site or even physically close to the location, it can take critical minutes or hours to service the equipment and meet computing demands if something goes wrong. Because of this, healthcare providers need to be vigilant in monitoring and responding to potential issues at their edge facilities.

Distributed computing like the edge is all about increasing bandwidth and IT availability so users don't have to rely on central or regional data centers and the time it would take to send the data there and back. It gives healthcare providers the ability to handle computation locally and stream massive amounts of data without business interruption, and provides them with a level of resiliency for business continuity.

By using computing equipment physically close to the patient and practitioners, rather than at a distant enterprise data center, edge facilities protect patient experience and safeguard the provider's reputation and revenue by minimizing downtime and enabling providers to locally cache patient records for upcoming visits, and mitigating costs and the disruption caused by unforeseen downtime.

Challenges of Implementing Edge Computing

Healthcare providers face three major challenges with edge deployments in remote facilities:

- Managing the equipment
- Securing the space
- Assessing potential issues

Managing edge deployments requires planning beyond that for a traditional enterprise data center. Given the number of sites in many healthcare providers' portfolios, the scale alone makes management of these sites exponentially more complex to operate and monitor. For it to be an effective and efficient architecture, edge equipment has to work independently of network topology while remaining 100% reliable with uptime to match.

Security is a significant concern for healthcare providers because of the sensitive personal and medical information they house, and because of the need to comply with industry regulations like the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Edge services are enabled via connected devices that touch patient data, payment cards, and insurance records.

Threats to the safety of that information come from both the physical space housing the equipment and from physical access to those devices.

Environmental conditions can also threaten edge infrastructure, anything from a tenant upstairs with an overflowing drain, to storms creating power spikes and outages, to HVAC failures that can impact day-to-day operations and patient safety if allowed to impact server uptime.

Direct physical access can be an issue too. With edge equipment and servers in dispersed locations without oversight from dedicated IT or security staff, healthcare providers rarely know who accesses equipment or if those individuals are authorized to do so. Physical protection is critical, given that about a third of breaches can be attributed to direct physical access to IT equipment and infrastructure. HIPAA requires safeguarding physical access to IT infrastructure and electronic protected health information. The security rule defines physical safeguards as "physical measures, policies, and procedures to protect a covered entity's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion."[3]

3 Department of Health and Human Service, "HIPAA Security Series - Security Standards: Physical Safeguards " https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/physsafeguards.pdf

Healthcare providers accepting payment cards are subject to the security safeguard standards in the Payment Card Industry Data Security Standard (PCI DSS)[4]. This global standard applies to any organizations that handle credit and debit cards, to ensure that businesses that deal with publicly identifiable information take steps to prevent fraud and data theft. This standard requires physical security of IT equipment housing this type of information.

Even as edge deployments allow new opportunities to compete for patients' attention, the additional infrastructure complexity that edge deployments carry present additional challenges for providers. . In addition to the traditional enterprise data center, a true edge deployment requires a server closet or small computing facility on premises at the hospital or clinic. This adds several pieces of IT equipment to an already complex network and increases the workload of the IT team responsible for hundreds of geographically dispersed locations.

Because no two hospitals, clinics, or back-office locations are alike, IT teams do not get the benefit of a homogeneous infrastructure like what they're accustomed to with the enterprise data center. There is little consistency – each space in each location presents its own challenges and issues over time; things like HVAC and power, internet access, and bandwidth. Some locations may have dedicated space for servers and the associated IT infrastructure, while others may force the IT team to use less than ideal areas like a converted storage closet or a partially utilized stock room. Regardless, no matter what the physical location may look like, the corporate IT team has to choose the equipment, deploy it, connect it to the network, secure it, and then maintain the technology.

In most cases, it's simply not possible to secure non-traditional physical locations using the same security measures as in the

4 PCI Security Standards Council, "PCI Security" https://www.pcisecuritystandards.org/pci_security/

traditional data center. Further, healthcare staff – nurses, doctors, physicians assistants, receptionists, etc. – are not trained IT personnel. These individuals likely don't have awareness or training to secure and protect the IT equipment that enables their day-to-day workflow. Without on-site IT staff, the enterprise lacks critical insight as to what equipment is deployed, how well it is secured, and oversight of optimal operating conditions. This makes it difficult to identify, diagnose, and provide quick break/fix resolution in these critical patient-facing deployments.

Managing these edge locations is only feasible at scale with automated reporting, integrated alerts, and hands-off management. And as these servers and the associated connectivity equipment become more distributed and interconnected, it is becoming more and more important to be able to monitor and manage the technology stack from a centralized location to enable real-time patient solutions within each healthcare facility.

The Solution

This distributed healthcare environment requires a secure, manageable edge that can deployed in remote locations without the overhead of on-site IT support. The only way to effectively accomplish this is the ability to monitor each edge deployment from afar – in a network operations center, security operations center, at the enterprise data center, or even from an on-call employee's mobile device. Visibility into these distributed and disparate spaces is required for IT to diagnose and fix problems quickly and to enable uninterrupted operation.

Real-time monitoring with sensors and video, alerts when unexpected events occur, and reporting on changes over time enable actionable responses to minimize and even completely avoid downtime.

Asset Management

Monitoring critical assets means using sensors to understand their use state (provisioned, idle, newly received, disposed, etc.) and their physical location (storage room, loading dock, network closet 1, clinic rack 3, and so on). This becomes increasingly more complex as assets are deployed across potentially hundreds or thousands of edge locations.

For example, if you need to take a specific type of server out of service because a maintenance update is required for HIPAA compliance, real-time data generated by the asset management sensor network allows your IT staff to do so in a cost effective and time sensitive manner. Rather than having to send full-time employees or third-party technicians to every hospital, clinic, and office in the enterprise to verify what devices are in which locations, a real-time report to locate the equipment in question enables staff to begin their roll-out accordingly. It also makes the job easier when you know what devices you have in inventory to deploy as replacements, preventing over-provisioning of costly capital infrastructure.

Physical Security

Sensors can alert IT staff of unauthorized access to remote facilities and attempts to access sensitive equipment or even attempts to remove a device from the premises. The last thing any chief information security officer wants is to see their name in news article about fines for a regulatory non-compliance or a data breach containing sensitive patient information. Proper monitoring with sensors and video protects healthcare companies from additional regulatory risk associated with data theft caused by a physical security breach by providing proof that equipment was protected to an acceptable level.

Environmental Conditions

Monitoring the environment housing your IT equipment means deploying a sensor network that can track the atmosphere of the physical space – temperature, humidity, air pressure, fluid activity, etc. Monitoring the environmental conditions across many facilities is equally as complicated as tracking physical location – different weather conditions in disparate geographical locations require unique understanding of climate, seasonal fluctuations, and how all these factors impact sensitive IT devices.

Tracking the location and conditions of IT assets is only part of the reason that monitoring matters. Using that information to make informed decisions with real-time data gives your IT team the insight they need to reduce time to resolution for servicing equipment failures or addressing environmental hazards.

RF Code for Edge: CenterScape Edge Manager

CenterScape Edge Manager, part of RF Code's CenterScape software suite, thoughtfully addresses healthcare providers' edge deployment needs. The solution monitors the environment (power and cooling, access and activity) and the assets (servers, networking devices, storage, and peripherals) holistically and at scale. This combined hardware/software approach provides value beyond monitoring just the enterprise data center by bringing visibility into all locations to single pane. It's designed to address the unique challenges and complexity of edge computing environments, increase operation efficiency, improve the organization's security posture, reduce the costs of managing equipment, and deliver the simplicity, savings, and visibility needed to effectively operate at the edge.

If you're a healthcare provider with data on the edge, a likely scenario given the 35% growth rate[5] in the industry, you need a comprehensive edge management strategy for these highly distributed facilities and their complex monitoring requirements. RF Code for Edge is a key element of that strategy, tracking all your assets' current locations to the rack level and monitoring the environmental conditions and facility access.

Specifically designed with the unique requirements of edge deployments, CenterScape provides real-time insight and control over operations risks, costs, and compliance. This quick-to-deploy and easy-to-manage solution, accurate to the rack level and collecting data 24x7, provides reporting and accountability for compliance, regulatory requirements, and service level agreements. As an open platform, the solution is designed to easily integrate with your existing software deployments like IT systems management tools (ITSM), building management systems (BMS), and data center infrastructure management (DCIM) platforms.

Edge facilities only bring that value when they're working efficiently, effectively, and at scale. To do so requires granular, real-time intelligence and alerts for each of your hospitals, clinics, and back-office staff locations. As edge computing is impacting more and more business operations, RF Code empowers healthcare enterprises to leverage the edge effectively and make informed decisions faster.

5 HIT Infrastructure, "Healthcare Edge Computing Supports Increased Data Processing Needs " https://hitinfrastructure.com/news/healthcare-edge-computing-supports-increased-data-processing-needs