Qpath E Cloud Technology and Security White Paper

Implementing and Securing Qpath E at Your Organization

Contents

Introduction

This document is intended for existing and potential customers who are interested in, or currently integrating Qpath E Cloud into their hospital IT environment.

The document describes Qpath E Cloud connection architecture and security controls used to communicate with a client's hospital system, securely transmit and store their data in MS Azure Cloud

The document targets to answer potential security questions on Qpath E connection with a hospital network, data transmission, data protection and recovery plan to ensure that the required security compliance is achieved in the cloud.

MS Azure – Approach to Security and Data Protection

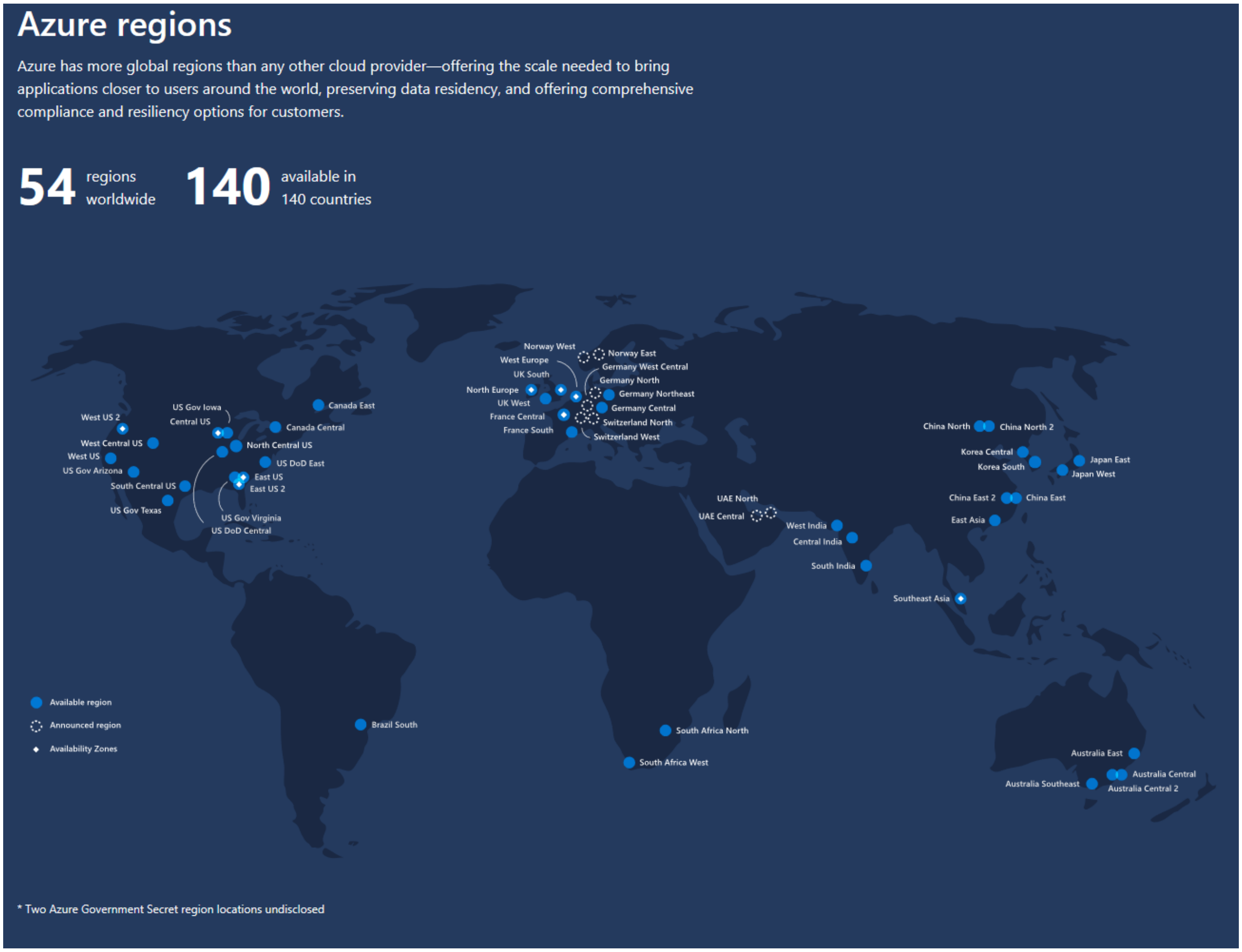
Why Azure

MS Azure Cloud platform is the choice for millions of customers as it provides a trustworthy foundation upon which businesses can meet their solution needs and security requirements.

Qpath E runs on MS Azure because of its:

- unlimited storage and capacity
- reliability and security
- quick and easy deployment and maintenance
- flexibility, scalability and redundancy.

Azure Cloud is a globally used platform with the regions added world wide. More and more regions are being added regularly



Azure regions

Azure has more global regions than any other cloud provider—offering the scale needed to bring applications closer to users around the world, preserving data residency, and offering comprehensive compliance and resiliency options for customers.

54 regions worldwide **140** available in 140 countries

* Two Azure Government Secret region locations undisclosed

Azure Security and Compliance

Microsoft helps reduce the security and compliance burden for customers by providing trustworthy enterprise cloud services, while also offering the security capabilities and flexibility customers need to use the services in accordance with their own standards.

Data security and protection on MS Azure Cloud is achieved through the main approaches:

- **Protecting data at rest**

  Azure offers a wide range of encryption capabilities, giving customers the flexibility to choose the solution that best meets their needs. Azure Disk Encryption leverages the industry-standard BitLocker feature of Windows and the DMCrypt feature of Linux to provide volume encryption for the OS and the data disks. The solution is integrated with Azure Key Vault to help users control and manage the disk encryption keys and secrets in their key vault subscription, while ensuring that all data in the virtual machine disks are encrypted at rest in your Azure storage. SQL Database TDE is based on SQL Server's TDE technology, which encrypts the storage of an entire database by using an industry-standard AES-256 symmetric key called the database encryption key. SQL Database protects this database encryption key with a service-managed certificate. All key management for database copying, GeoReplication, and database restores anywhere in SQL Database is handled by the service.

- **Protecting data in transit**

  For data in transit, customers can enable encryption for traffic between their own VMs and end users. Azure protects data in transit, such as between two virtual networks. Azure uses industry-standard transport protocols such as TLS between devices and Microsoft datacenters, and within datacenters themselves.

- **Data redundancy**

  Customers may opt for in-country storage for compliance or latency considerations or out-of-country storage for security or disaster recovery purposes. Data may be replicated within a selected geographic area for redundancy to ensure data recovery and high availability.

- **Data destruction**

  When customers delete data or leave Azure, Microsoft follows strict standards for overwriting storage resources before reuse. As part of our agreements for cloud services such as Azure Storage, Azure VMs, and Azure Active Directory, we contractually commit to specific processes for the deletion of data.

- **Data segregation**
  Customer data is kept logically separate on each component throughout the OMS service. All data is tagged per organization. This tagging persists throughout the data lifecycle, and it is enforced at each layer of the service. Each customer has a dedicated Azure blob that houses the long-term data.

- **Physical security**
  The OMS service is manned by Microsoft personnel, and all activities are logged and can be audited. The OMS service runs completely in Azure and complies with the Azure common engineering criteria.

- **Compliance and certifications**
  Microsoft cloud services and platforms meet rigorous security standards and are trusted. Azure conforms to a large number of global standards such as ISO 27001, HIPAA/HITECH, FedRAMP, SOC 1 and SOC 2, as well as country-specific standards.

MS Azure – Disaster Recovery Strategy

Azure provides disaster recovery (BCDR) strategy that keeps users data safe, and their apps and workloads up and running, when planned and unplanned outages occur:

- **Site Recovery service**
  Site Recovery helps ensure business continuity by keeping business apps and workloads running during outages. Site Recovery replicates workloads running on physical and virtual machines (VMs) from a primary site to a secondary location. When an outage occurs at the customer’s primary site, it fails over to secondary location, and accesses apps from there. After the primary location is running again, user can fail back to it.

- **Backup service**
  The Azure Backup service keeps customers’ data safe and recoverable by backing it up to Azure.

Related links

All Azure compliance and certification offerings.

Azure Security Documentation

Disaster Recovery for Azure Applications

Qpath E Use of MS Azure Services

The following MS Azure services are used to facilitate Qpath E work in the cloud:

Compute – App Service

App Service is a fully managed and scalable platform compatible with any OS. Qpath E running on Azure App Service requires minimum maintenance support and is fully self-managed in load balance.

Azure SQL Database

Azure SQL Database is the intelligent, fully managed relational cloud database service that provides the broadest SQL Server engine compatibility. Each Qpath E client has a separate DB with control access and multifactor authentication. All data is kept encrypted while in use (encryption at-rest). SQL Database meets stringent compliance standards, such as GDPR, ISO/IEC 27001/27002, FedRAMP/FISMA, SOC, HIPAA, and PCI DSS. Long term backup retention and backup restore can be configured per client's requirements. The default Qpath E DB auto backup is set to the last 35days. To ensure durability, high availability and protection from planned / unplanned outages or natural disasters, all data is replicated across the data centers in geographically separated regions (georedundancy)

Azure Blob Storage

Blob storage is a massively-scalable object storage for unstructured data. A separate storage account is created for each Qpath E customer. The storage is comprised of the three main containers per Qpath E instance:

- DICOM Storage
- Cache - includes Images Data and Video streams data cache storage
- Attachments

The data in Azure Storage is always replicated and is at least 99.9% available in the face of any failures as per Azure Service Level Agreement for Storage. Qpath E storage is georedundant which means the storage data is replicated in the data centers across geographical regions.

Related Links

MS Azure App Service
MS Azure SQL Database Service
MS Azure SQL Database automated backups
Azure Service Level Agreement for Storage

Qpath E Cloud Connector – secure connection to hospital systems

What is Qpath E Cloud Connector

To ensure the secure connection with a hospital network, Qpath E cloud does not communicate with hospital systems directly. This communication is performed through Cloud Connector application implemented by Telexy specially for this purpose.

Cloud Connector is a TCP relay-based application used to facilitate the connection between on-premises and the cloud environment without having to open a firewall or any other intrusive changes to a corporate network infrastructure. Cloud Connector runs on a basic hospital server or VM.

Connections and ports

The data in transit through Cloud Connector is encrypted with TLS 1.2 protocol over HTTPS connection.

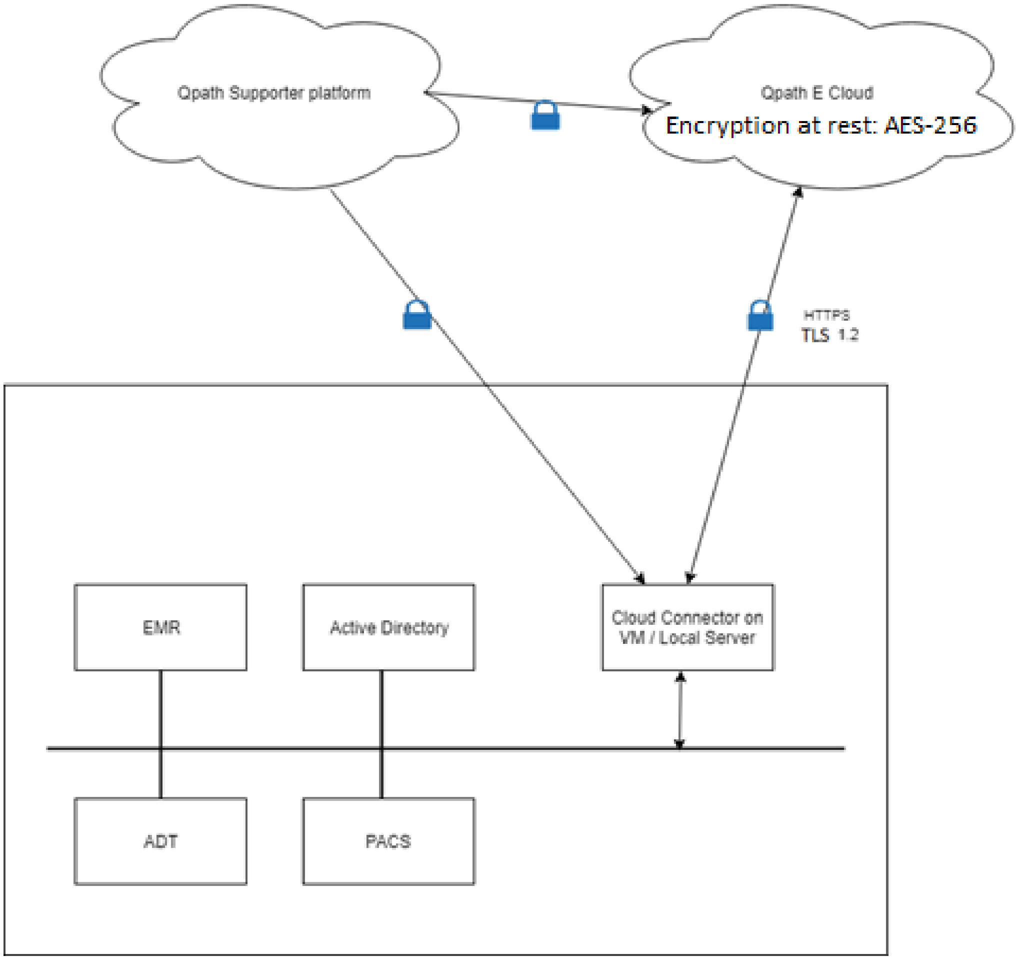
The communication is usually established through the following ports configured in Cloud Connector and Qpath E:

- DICOM to Qpath E (PACS system, Modality Worklist)
- HL7 to Qpath E (EMR / ADT interfaces)
- Qpath E to DICOM
- Qpath E to HL7
- LDAP to Qpath E(Active Directory interface)

Telexy uses Qpath E Supporter platform for the application installation and configuration.

The below diagram shows how the connection between Qpath E and Hospital network is set up.

Qpath E Cloud connection to Hospital internal network



Telexy Security Policies and Procedures

At Telexy, we understand that building a healthy security culture starts with the company security policies and related security procedures.

Telexy conducts comprehensive background checks for all new hires. In addition, Telexy all staff are trained and tested in principles pertaining to security, confidentiality and ethics through our Security Awareness program.