ATELCOR®

Everything, Everywhere Point of Care®

TELCOR QML® Data Protection, Security, and Continuity

A Comprehensive Approach to Safeguarding Point of Care Data in Healthcare Environments

Executive Summary

Point of care testing systems operate within a healthcare technology landscape where cybersecurity threats, evolving data protection standards, and complex network environments are a growing consideration for organizations. TELCOR designed QML as an on-premise, highly configurable system that protects sensitive information, maintains operational uptime, and supports compliance with security expectations across healthcare IT.

This paper describes the technical safeguards, operational controls, and continuity mechanisms built into QML. These include AES-256 database encryption, TLS-secured network communication, IP whitelisting, annual independent penetration testing, high availability database options, application failover strategies, and structured backup and recovery workflows.

Encryption At Rest

The commercial Sybase SQL Anywhere (Sybase) database(s) used by QML accommodates FIPS 256-bit AES encryption, a commercial option that can be purchased from and installed on the QML database(s) by TELCOR. All new QML implementations starting in 2020 have included this protection with the purchase and installation.

However, it can be purchased and installed on any QML database, including those implemented before 2020. This protects all QML database tables and data at rest. All backup files created from a production encrypted database will also be automatically encrypted. Once installed, the encryption key is stored within the Microsoft Dynamics CRM product utilized by TELCOR for customer management and provided to the customer, whose contact information along with the date and time provided, are also recorded in the CRM.

Encryption In Motion

Though QML is not intended to send data outside of your environment, we have all heard and some have sadly experienced internal networks being compromised.

To minimize risk without encryption in transit, TELCOR requests the ADT host to limit HL7 messages to the MSH, PID, PV1 and MRG segments. The demographic elements stored in QML database include only those elements required to confirm the patient encounter and include Enterprise ID (if available), MRN, Account Number, Name, DOB, Sex, Patient Class and Type, Assigned Facility/Room/Bed, Admitting and Attending Provider information and Admit/Discharge Dates.

To further protect this data, we completed projects to enable Transport Layer Security (TLS) 1.2 certificated encryption for in-transit QML data as defined below. Certainly, implementation of this encryption with Devices and Host systems is dependent on the system to which QML is connected.

- HL7 Solicited and Unsolicited Results via TCP socket to socket communication.
- HL7 ADT and Orders via TCP socket to socket communication.
- Sybase database connections, meaning all QML user traffic, which requires FIPS encryption of the Sybase database.
- Device interfaces will be updated as device vendors provide encryption.

Whitelist

Whitelisting is also a security strategy available for the ADT, Orders, Solicited and Unsolicited Result interfaces. This denies access to everything by default and only allows connection to/from the IP addresses explicitly defined. This provides controlled interface access and reduces exposure to lateral movement threats inside a network.

External Penetration Testing

As a best practice, TELCOR conducts annual external penetration testing through independent third-party security organizations. Penetration testing results feed into TELCOR's software development lifecycle, patching, and roadmap.

Data Continuity

The QML database can be configured with a High Availability (HA) option. This option includes two (2) Sybase databases each on a dedicated server and one (1) Sybase arbiter also on a dedicated server.

QML is configured to connect to both Sybase database servers. All three servers talk to each other. If the Primary server goes down, the Arbiter server and the Mirror server detect the disconnect from the Primary. The Mirror server then becomes the Primary server when the Mirror server and the Arbiter server reach quorum. When the original Primary server comes back up, it will then be the Mirror server. (The Primary and Mirror servers may also be referred to as Partner servers.) This switching is automatic and instantaneous and could be caused simply from a network delay to the primary or by the server itself being unavailable. The two Sybase HA database servers can be installed in different data centers. The HA Arbiter server should be installed in the same data center as one of the Sybase HA database servers.

The QML Interface/Application Server typically includes device connectivity and host system interfaces (e.g., result, ADT, orders). Occasionally, host system interfaces may be configured on their own server depending on volume. Whether a single or multiple interface servers, an option for a Production Ready (PReady) server(s) can be purchased from TELCOR. Host system interfaces can be defined using the actual server IP(s) or a virtual IP address(es).

Recovery of QML to a PReady server within the production site can be accomplished utilizing a virtual IP address that can be redirected to the PReady server in the event the primary server is unavailable. A network device with IP address persistence can be used to facilitate recovery within the production site by preserving the IP address of clients. This recovery option is a manual process requiring TELCOR to enable services and recover unprocessed data to the PReady server from the primary server.

Recovery of QML to a remote site can be accomplished by routing the production IP address(es) to the remote site. A network device with IP address persistence can be used to facilitate the remote site recovery by preserving the IP address of clients. This capability would be used in conjunction with migration of the production application server to the remote site via use of a PReady server or a virtual machine replication solution. This recovery option is a manual process requiring TELCOR to enable services and recover unprocessed data to the remote site. In addition, customer involvement is required to reroute the production IP address(es) to the remote site.

Most devices connected directly to QML

accommodate entry of a single IP address only. This could be the actual IP address of the QML production application/interface server or a virtual IP. The intention of a virtual IP is to automatically route data to a new production application/interface server in the same data center. A network device with IP address persistence can eliminate the need to update the IP address in each device when the QML application/interface is replaced.

Backup and Recovery

Backups of the QML Sybase database are by default scheduled daily for a full backup on Saturday and incremental daily backups Sunday through Friday to occur automatically at 2 a.m. local time. Each daily file is stored in the QML database (db) backup folder on the database server. The customer is responsible for copying this folder to network storage after the daily backup completes. The QML dashboard also includes a backup tile with the date, time, storage location, and status of the daily backup. If the tile states the backup has “Failed,” the customer is directed to contact the TELCOR POC support hotline for triggering of a manual backup and then troubleshooting the cause of the failure.

This backup event can be customized by TELCOR for more frequent and/or all full rather than incremental backups depending on customer request. These files will still be written to the database (db) backup folder on the database server and the customer is still responsible for copying this folder to network storage.

In the event of a database error, TELCOR is responsible for restoring the database to current date. This could include restoring the previous full backup and then applying the current log or restoring the previous full backup, applying a previous log and then needing to re-process files from devices to return to current state.

If deploying the Sybase HA option, both the Primary server and the Mirror server maintain a copy of the database and transaction logs.

Conclusion

TELCOR QML provides precise, structured, and technically validated security and continuity controls that protect point of care program data. These include AES-256 encryption, TLS network protection, IP whitelisting, independent penetration testing, database high availability, structured failover strategies, and defined backup and recovery procedures.