# TELMEDIQ

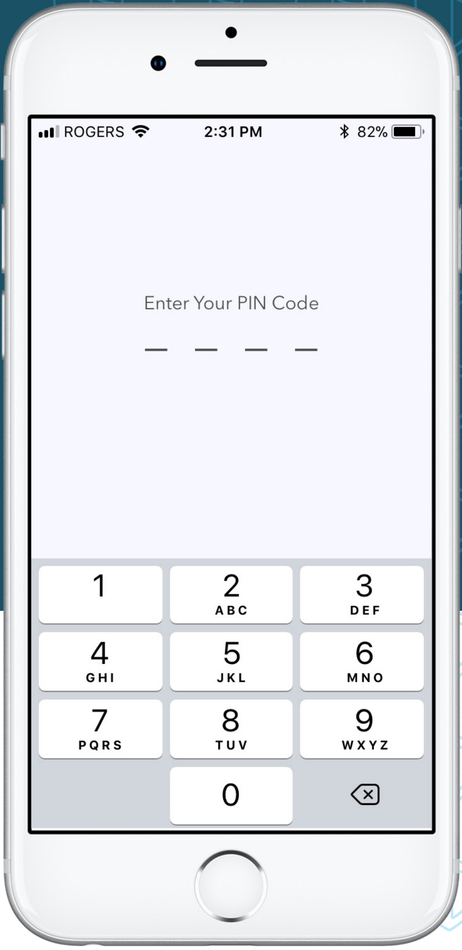
# Data Security Overview

KLAS
CATEGORY LEADER
SECURE COMMUNICATIONS
2019
2018

In order to meet CMS HIPAA compliance requirements and the standards set out under the Joint Commission, secure communication platforms must include:

- Encryption of all data in transit and at rest
- The ability to authenticate the user, preferably with 2-factor authentication
- Safeguards to guard against unauthorized access
- Ability to keep a discoverable archive of messages for 7 years, or longer
- Administrative ability to lock users from the system when they leave the organization
- Administrative ability to wipe all texting data from a user's device

Telmediq offers a unified healthcare communication platform that meets the most stringent levels of security under HIPAA and Joint Commission standards. In order to provide leadership in security and privacy, Telmediq's own risk program ensures regular audits, employee training, near real-time third-party intrusion and threat detection monitoring and third-party penetration testing.



Enter Your PIN Code

## Application Level Security

Password protection and integration with LDAP/AD and OAuth integrations, data encrypted in-transport and at-rest, customizable data retention policy (download and purge), with full auditing and monitoring. Biometric authentication for iOS and Samsung Android devices; Face ID authentication for iPhone X devices.

## Account Security

All access to instances delegated through a bastion host with fine-grained security policies for access to infrastructure (user or group roles), supported by 2-factor authentication. Messages cannot be sent to users until they download and register the mobile application in order to validate the user against the Active Directory. Separate accounts for staging, development, and production environments provide additional levels of account security. All access is audit logged.

HIPAA Compliant

**Better Communication. Better Care.**

2018-2019 Best in KLAS: Software and Services, Secure Communications, (C) KLAS 2019

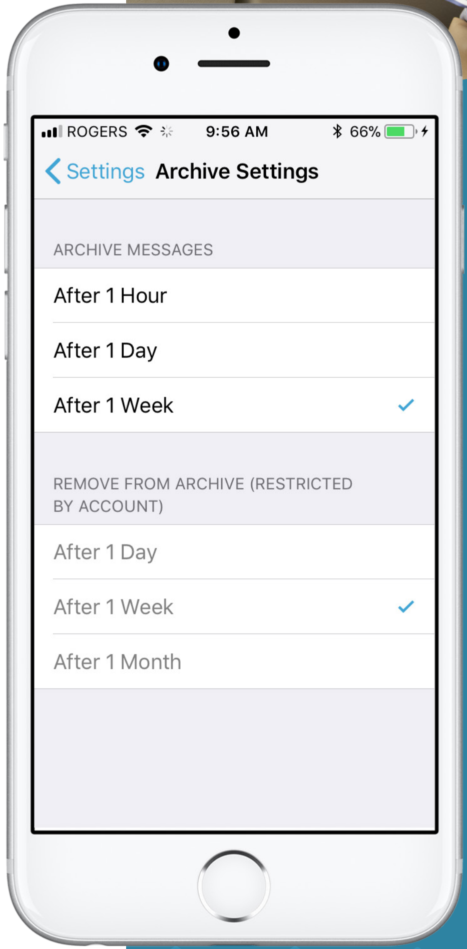
## Network Security

The Telmediq platform is a closed system running inside an isolated network (VPC). All Egress and Ingress is controlled by firewall rules between every subnet. All traffic to the Internet runs through a private internet gateway. Transport security uses TLS 1.2 and modern cipher suites between nodes (ex. App to DB Server). AES-256-bit encryption is used for data at rest with block-level encryption on all storage volumes, including back-ups.

All customer data is segregated from other clients using a customer Account ID on all transactions at the most granular level or can be further segregated utilizing a private cloud deployment. Telmediq utilizes Amazon AWS for cloud services.

## Data Layer Security

AES-256 bit encryption, block-level encryption on all storage volumes (including backups) meets with the Federal Information Processing Standards (FIPS) 140-2 approved cryptographic algorithms and key management.



ROGERS 9:56 AM 66%

Settings **Archive Settings**

ARCHIVE MESSAGES

- After 1 Hour
- After 1 Day
- After 1 Week ✓

REMOVE FROM ARCHIVE (RESTRICTED BY ACCOUNT)

- After 1 Day
- After 1 Week ✓
- After 1 Month

## BYOD Security

2-factor authentication and configurable password protection protect application access, further supported with end-to-end data encryption, message lifespan controls, and remote lock and wipe. Compliant with all leading MDM market solutions to ease deployment and add additional security protection. Active Directory integration automatically controls user access for entering and exiting employees.

## Auditing

Audit account security and data use with the ability to keep a discoverable archive of messages for 7 years. Further, the platform allows the sender to see if/when a message is delivered and read and gives clinicians the option to save conversations to the health record.

## Critical Message Delivery

Provides alternate delivery paths and routing paths for messages and a way to escalate non-delivered or unread messages to minimize patient risk when time sensitive or critical information is being sent.