qliqSOFT

# HIPAA STATEMENT

qliqSOFT provides a secure, HIPAA and HITECH compliant, messaging platform that connects healthcare professionals, their staff, patients, and ancillary service providers in realtime to facilitate communication and collaboration.

## WHAT IS HIPAA?

The Health Insurance Portability and Accountability Act (HIPAA), passed by Congress in 1996, was created to ensure the continuity of health benefits for all individuals.

Title II of the HIPAA regulations require healthcare providers to establish and follow procedures and practices that ensure the confidentiality and security of Protected Health Information (PHI) when it is transferred, received, handled, or shared.

## WHAT IS THE IMPACT OF HIPAA ON QLIQSOFT?

Since all PHI and other sensitive data is stored on your resources in a distributed model, it is 100% under your control just like the other systems that you are actively protecting from security breaches.

All PHI is only transiently stored in an encrypted form on our servers when the recipient's device is unavailable. All security keys are stored in an encrypted form on a completely separate server.

As such, qliqSOFT does not fit the definition of a Covered Entity or a Business Associate. When you partner with us, you will not need a Business Associate Agreement or invest in lengthy third-party validation procedures. We act merely as a conduit for the information and do not even access the information on a random or infrequent basis which exceeds the requirements as set out in the Federal Register, Vol. 75, No. 134, p. 40873.

qliqSOFT is dedicated to the privacy and security of its customers' information and we do our best to ensure that our applications exceed the current HIPAA and HITECH compliance requirements. We want to ensure that you are ready for a future that even the regulators have not anticipated yet. We are well-positioned to map every compliance requirement that might arise and can implement any changes in the law quickly. We are proactively monitoring the debated legal changes providing a level of due diligence that instills confidence in our healthcare customers that our secure messaging applications can be deployed on their network without risking non-compliance.

## DOES QLIQSOFT FACILITATE SUPPORT FOR HIPAA REQUIREMENTS?

HIPAA compliance is at the foundation of our secure messaging platform design. Built into all qliqSOFT applications are a full suite of features and security mechanisms that ensure healthcare organizations meet HIPAA compliance Security Standards.

qliqSOFT is committed to ensuring that our customers will meet or exceed all Privacy and Security rules.

## SUMMARY

The need for realtime, secure, HIPAA compliant messaging solutions is growing in importance due to anticipated decreases in the number of healthcare providers. Future healthcare providers will need to provide the same level and quality of care to more patients with fewer resources. This is already true in rural healthcare where patients have limited transportation and often live hundreds of miles from specialists. qliqSOFT solutions can bring that specialist to the patient.

There is also a demand among patients under 60 to have more access to their physicians and medical information. This demand is especially critical in times of a disaster where time sensitive communication between healthcare providers could affect a patient's outcome.

Our applications work in realtime across various platforms (iOS, Android, Windows, Mac) using strong data encryption protocols so the members of your healthcare organization know that the PHI being transmitted is secure no matter when or how they choose to access or transmit the data.

Whether you are a solo provider, provider on the go, part of a group, or member of a healthcare system, qliqSOFT has a solution that will exceed your expectations.

qliqSOFT is your preferred partner for secure HIPAA compliant communication of Protected Health Information.

**END-TO-END ENCRYPTION. CENTRALIZED CONTROL OF DEVICES. CUSTOMER OWNED MESSAGE ARCHIVAL.**


**CONTACT US FOR MORE INFORMATION:**

qliqSOFT Three Galleria Tower, 13155 Noel Road, Suite 900, Dallas, Texas 75240

**Phone:** (866) 295-0451 **Email:** sales@qliqsoft.com **Website:** www.qliqsoft.com

# HOW qliq TECHNOLOGY WORKS

qliqSOFT

## DATA FLOW OF MESSAGES THROUGH THE QLIQ NETWORK:

**1** Senders sends a message.

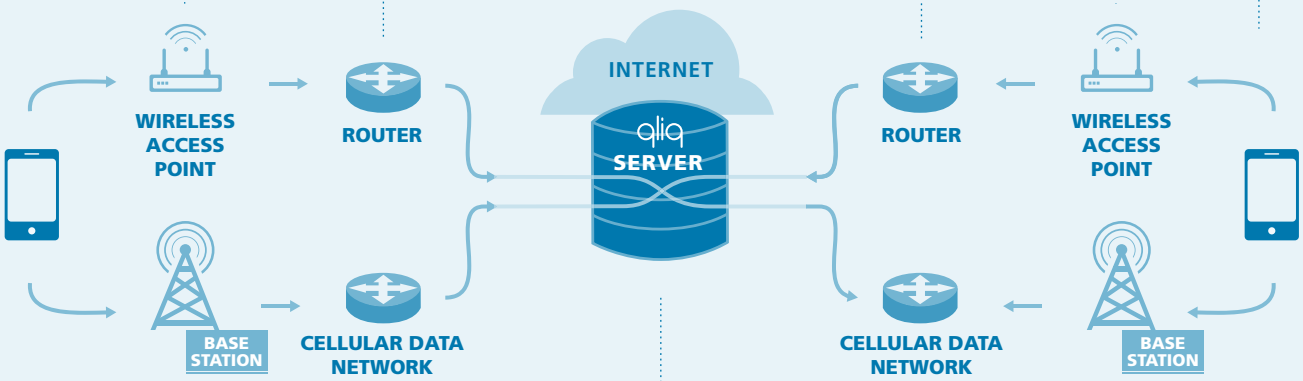
**2a** If the sender has a WiFi connection, the phone will preferentially transmit the message to the wireless access point (WAP), which will then forward the message to the network router. [The WAP and router may or may not be integrated into a single piece of hardware.]

**3a** The Network router forwards the message to the qliqServer.

**5a** If the recipient's IP address is associated with a network address, the network router will receive the message and forward it to the WAP.

**6a** The WAP processes the message and transmits it to the recipient's device over WiFi.

**7** Recipient receives the message.



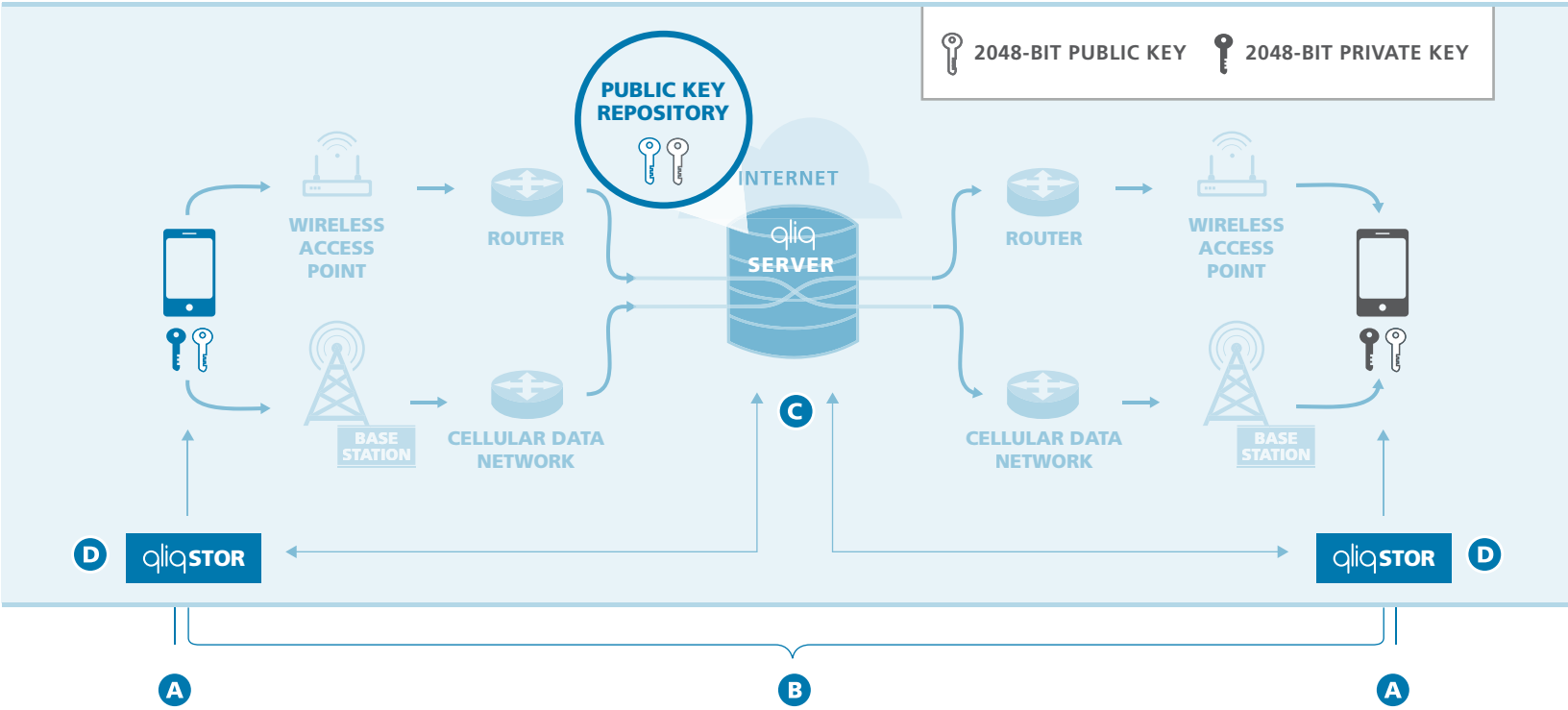

**2b** If the sender has a 3G/4G data connection with no active WiFi connection, the message is transmitted to the cell tower and processed by the base station (BS). It is then sent to the cellular data network (CDN).

**3b** The Packet Router GGSN/PDSN forwards the message to the qliqServer.

**4** The qliqServer determines a recipient's availability, including their current IP address. If the recipient is available, the qliqServer will forward the message. If the recipient is not available, the qliqServer will send a notice to the recipient's device via a push notification informing them that they have a new qliqConnect message. Once the recipient logs into the application, the qliqServer will send the message to the recipient's IP address.

**5b** If the recipient's IP address is associated with a CDN, the CDN will receive the message and forward it to the correct base station (BS).

**6b** The BS processes the message and transmits it via the cell tower to the recipient's device over 3G or 4G.




## SECURITY FEATURES

### A PHYSICAL SECURITY

- User authentication is required before smartphone or desktop users can send or receive messages. Users must log in using authorized credentials.
  - Convenient four-digit PIN authentication access is available.
  - Group administrators can set password strength requirements.
  - Application data is encrypted on the device to protect against USB copying.

### B TRANSMISSION SECURITY

- All data is encrypted end-to-end, both in transit and at rest.
  - 2048-bit end-to-end message encryption (running across port 443).
  - 256-bit AES encryption for message attachments (image, audio, and various document formats).
- Messages are encrypted by the sending device and then decrypted by the receiving device, using a combination of public and private keys. Only the intended recipient can decrypt the message.
- qliqSoft cloud-based servers route messages, which are then stored on end-user devices in an encrypted file. No unencrypted messages are stored in the cloud.

### C qliqSERVER

- qliqSoft does not store or access the information that flows through the qliq network. Rather, storage is distributed and information is controlled by the end-users and their organizations.
- The message server routes message traffic and the information in the cloud only long enough to complete the message delivery. When deliver occurs, the user information is deleted from the qliqServers.
- Hosted on an SSAE-16 compliant Cloud Virtual Data Center.

### D qliqSTOR

With the optional qliqStor feature, organizations can store all of the message traffic exchanged between the users of a qliq group on a group-controlled virtual server that can be queried by the group administrator or authorized designees for auditing purposes.

### ACCOUNT MANAGEMENT

Through the qliqWeb console, the group administrator can:

- Add, remove, and edit a user's access
- Monitor usage activity
- Enforce group policy for password strength, inactivity timeout, and other security settings
- Lock and wipe application data remotely from a lost or stolen device (group and individual management to provide BYOD support)

# HIPAA SECURITY STANDARDS MATRIX

qliqSOFT

| ADMINISTRATIVE SAFEGUARDS | IMPLEMENTATION SPECIFICATION<br>*(R) = Required*<br>*(A) = Addressable* | DESCRIPTION | qliqSOFT FULFILLMENT |
|---|---|---|---|
| Security Management Process 164.308(a)(1) | Risk analysis (R) | Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity. | qliqSOFT's applications are built around breach prevention. We continuously review our internal and external security protocols and procedures. |
| | Risk management (R) | Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a). | qliqSOFT's applications are built around security. We continuously implement the latest security measures regardless of the industry that they were designed for. |
| | Sanction policy (R) | Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity. | qliqSOFT's infrastructure is designed to minimize security breaches. However, if it were to happen and the few messages that might be accessible were accessed, that individual would be terminated immediately and all appropriate breach notifications sent. |
| | Information system activity review (R) | Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports. | qliqSOFT monitors the general activity on its servers and it has designed a detailed audit and logging report for its customers. |
| Assigned Security Responsibility 164.308(a)(2) | Security Official (R) | Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the entity. | Krishna Kurapati, our CEO, is also head of security as he has 18 years of experience in designing and implementing highly secure IT systems. |
| Workforce security 164.308(a)(3) | Authorization and/or supervision (A) | Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed. | qliqSOFT thoroughly screens all employees that might be able to remotely access one of our secure servers. Only designated employees can access qliqSOFT servers. |
| | Workforce clearance procedure (A) | Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate. | qliqSOFT only allows a few of the most senior employees to access our cloud servers. No other employee or contractor is permitted to access these servers. |
| | Termination procedure (A) | Implement procedures for terminating access to electronic protected health information when the employment of a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(B) of this section. | As qliqSOFT does not store PHI, we do not need to have a procedure for terminating access. We do have a policy in place to change access codes to our cloud servers should one of our Senior employees leave. |

| ADMINISTRATIVE SAFEGUARDS | IMPLEMENTATION SPECIFICATION<br>*(R) = Required*<br>*(A) = Addressable* | DESCRIPTION | qliqSOFT FULFILLMENT |
|---|---|---|---|
| Information access management 164.308(a)(4) | Isolating healthcare clearinghouse function (R) | If a healthcare clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization. | qliqSOFT has no clearinghouse functions. |
| | Access authorization (A) | Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism. | As qliqSOFT does not store PHI, the control of this function is at the level of the administrator for that practice, group, or healthsystem. |
| | Access establishment and modification (A) | Implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process. | As qliqSOFT does not store PHI, the control of this function is at the level of the administrator for that practice, group, or healthsystem. |
| Security awareness and training 164.308(a)(5) | Security reminders (A) | Procedures for guarding against, detecting, and reporting malicious software. | At qliqSOFT, we are intently focused on security and implement new security features on a regular basis. |
| | Protection from malicious software (A) | Procedures for guarding against, detecting, and reporting malicious software. | As qliqSOFT only provides secure messaging applications, there is no threat of any malicious software or viruses affecting our closed system. |
| | Log-in monitoring (A) | Procedures for monitoring log-in attempts and reporting discrepancies. | At qliqSOFT, we provide the tools so that the administrator for that practice, group, or healthsystem can set this policy. |
| | Password management (A) | Procedures for creating, changing, and safeguarding passwords. | At qliqSOFT, we provide the tools so that the administrator for that practice, group, or healthsystem can set this policy. |
| Security incident procedures 164.308(a)(6) | Response and reporting (R) | Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes. | At qliqSOFT, security is our primary focus and expertise. We have implemented a distributed solution that lowers the risk of a potential breach while minimizing its impact. If there were to be a breach, appropriate reports would be made. |
| Contingency plan 164.308(a)(7) | Data back-up plan (R) | Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information. | At qliqSOFT, we have created qliqStor so that the administrator for that practice, group, or healthsystem can back up their data. Our basic application allows the user to create a pdf and/or print conversations for inclusion in the patient's health record. |
| | Disaster recovery plan (R) | Establish (and implement as needed) procedures to restore any loss of data. | As qliqSOFT does not store any PHI, we do not need to recover any lost data. Our qliqStor application is designed to help our customers recover lost data sent through our system. qliqSOFT has a backup and recovery process for our cloud servers. |

| ADMINISTRATIVE SAFEGUARDS | IMPLEMENTATION SPECIFICATION<br>*(R) = Required*<br>*(A) = Addressable* | DESCRIPTION | qliqSOFT FULFILLMENT |
|---|---|---|---|
| | Emergency mode operation plan (R) | Establish (and implement as needed) procedures to enable the continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode. | As all data that passes through our qliqSOFT servers is secure, we do not need to make any operational changes for an emergency. |
| | Testing and revision procedure (A) | Implement procedures for periodic testing and revision of contingency plans. | qliqSOFT has a continuous process to improve the availability of our service. |
| | Applications and data criticality analysis (A) | Assess the relative criticality of specific applications and data in support of other contingency plan components. | qliqSOFT provides secure messaging applications. We constantly assess various components of the system and make contingency plans. |
| Evaluation 164.308(a)(8) | Technical and non-technical evaluation (R) | Perform a periodic technical and non-technical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, that establishes the extent to which an entity's security policies and procedures meet the requirements of this subpart. | At qliqSOFT, security is our primary focus and expertise. We are constantly evaluating all security procedures. |
| Business associate contracts and other arrangements 164.308(b)(1) | Written contract or other arrangement (R) | Document the satisfactory assurances required by paragraph (b)(1) of this section through a written contract or other arrangement with the business associate that meets the applicable requirements of § 164.314(a). | As qliqSOFT is strictly a **conduit** and we do not even access the information that passes through our servers on a random or infrequent basis, we do not even meet the minimum requirements (as noted in the Federal Register, Vol. 75, No. 134, p. 40873) to be considered a Business Associate. |

| PHYSICAL SAFEGUARDS | IMPLEMENTATION SPECIFICATION<br>*(R) = Required*<br>*(A) = Addressable* | DESCRIPTION | qliqSOFT FULFILLMENT |
|---|---|---|---|
| Facility access controls 164.310(a)(1) | Contingency operations (A) | Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency. | At qliqSOFT, our cloud servers are under an SSAE-16 Compliant cloud service provider. |
| | Facility security plan (A) | Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft. | qliqSOFT does not keep or store PHI in our office. All data is securely routed and passes directly through our SSAE-16 Compliant cloud servers. |
| | Access control and validation procedures (A) | Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision. | Since there are no paper or digital PHI records stored in qliqSOFT's office, we do not need to enforce these stringent policies; front desk based controls are implemented. Data Center access controls follow SSAE-16 standards and procedures as well as industry best practices. |
| | Maintenance records (A) | Implement policies and procedures to document repairs and modifications to the physical components of a facility, which are related to security (for example, hardware, walls, doors, and locks). | Since there are no paper or digital PHI records stored in qliqSOFT's office, this standard does not apply to us. |
| Workstation use 164.310(b) | Function and attributes (R) | Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information. | At qliqSOFT, we only provide the application and not the hardware so this standard does not apply to us. |
| Workstation security 164.310(c) | Restrict access (R) | Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users. | At qliqSOFT, we provide the tools so that the administrator for that practice, group, or healthsystem can implement appropriate password protection and automatic system logoff. |
| Device and media controls 164.310(d)(1) | Disposal (R) | Implement policies and procedures to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored. | As qliqSOFT does not store PHI, this standard does not apply to us. However, we are able to advise our customers on how to do this. |
| | Media re-use (R) | Implement procedures for removal of electronic protected health information from electronic media before the media are made available for re-use. | As qliqSOFT does not store PHI, this standard does not apply to us. However, we are able to advise our customers on how to do this. |

| PHYSICAL SAFEGUARDS | IMPLEMENTATION SPECIFICATION<br>*(R) = Required*<br>*(A) = Addressable* | DESCRIPTION | qliqSOFT FULFILLMENT |
|---|---|---|---|
| | Accountability (A) | Maintain a record of the movements of hardware and electronic media and any person responsible. | As qliqSOFT does not store PHI, this standard does not apply to us. However, we are able to advise our customers on how to do this. |
| | Data back-up and storage (A) | Create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment. | As qliqSOFT does not store PHI, this standard does not apply to us. However, we have created qliqStor that allows our customers to fulfill this requirement. |

| TECHNICAL SAFEGUARDS | IMPLEMENTATION SPECIFICATION<br>*(R) = Required*<br>*(A) = Addressable* | DESCRIPTION | qliqSOFT FULFILLMENT |
|---|---|---|---|
| Access control 164.312(a)(1) | Unique user identification (R) | Assign a unique name and/or number for identifying and tracking user identity. | qliqSOFT's secure messaging applications assign a unique password and PIN code to each user so that they are the only ones who can decrypt the messages received. |
| | Emergency access procedure (R) | Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency. | qliqSOFT's secure messaging applications are realtime and allows physicians to access data no matter where they are located. qliqSOFT provides a local device login in the event there is a sustained loss of network connectivity. |
| | Automatic log-off (A) | Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity. | qliqSOFT's secure messaging applications allow the administrator for that practice, group, or healthsystem to set the time of inactivity before the application logs off or locks. |
| | Encryption and decryption (A) | Implement a mechanism to encrypt and decrypt electronic protected health information. | qliqSOFT's secure messaging applications provide true end-to-end encryption. Message traffic is encrypted with 2048 bit RSA keys and the attachments and data at rest are encrypted with a 256 bit AES-CBC. The sender encrypts the message and only the intended receiver can decrypt the message. |
| Audit controls 164.312(b) | (R) | Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information. | At qliqSOFT, we provide the tools so that the administrator for that practice, group, or healthsystem can monitor system usage. |

| TECHNICAL SAFEGUARDS | IMPLEMENTATION SPECIFICATION<br>*(R) = Required*<br>*(A) = Addressable* | DESCRIPTION | qliqSOFT FULFILLMENT |
|---|---|---|---|
| Integrity<br>164.312(c) | Mechanism to authenticate electronic protected health information (A) | Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner. | As qliqSOFT does not have access to PHI, this standard does not apply to us. |
| Person or entity authentication<br>164.312(d) | (R) | Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed. | At qliqSOFT, we provide the tools so that the administrator for that practice, group, or healthsystem can control access to the PHI stored in the group's location. |
| Transmission security<br>164.312(e)(1) | Integrity controls (A) | Implement security measure to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of. | The integrity of the PHI transmitted within our secure messages is automatically maintained due to their end-to-end encryption. |
| | Encryption (A) | Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate. | All data sent using a qliqSOFT application is end-to-end encrypted and uses SSL/TLS between the client and our cloud server. |