IntakeQ's Security FAQ

Version 1.14 (March 2020)

1) Where is my data hosted?
IntakeQ databases are exclusively hosted on Microsoft Azure, which meets several compliance standards, such as ISO 27001, HIPAA, GDPR, PIPEDA, FedRAMP, SOC 1 and SOC 2.

2) Where is my data physically located?
It depends on your location.

- Data from USA customers are physically located within US borders.
- Data from customers outside of the USA are located in Canada.

3) Is my data encrypted?

- All data transferred between our servers and the browser is encrypted via SSL.
- All internal data transfers (database replication, automated backups) are encrypted in transit and performed via secure channels.
- All communication between IntakeQ and 3rd party APIs are encrypted via SSL.
- All customer data is encrypted at rest at the database level.
- An additional layer of encryption is added at the application level to more sensitive data types, such as intake forms and treatment notes.
- All backups are encrypted at rest.

4) Do you have an audit log?
IntakeQ provides the account administrator with a detailed audit trail containing user activity. The audit trail tracks events and allows admins to view who opened, created, altered or deleted any sensitive data, such as intake forms, treatment notes, appointments, client profiles, etc.

5) Is IntakeQ HIPAA compliant?
No products can be labeled as HIPAA compliant, however, IntakeQ Inc., as a Business Associate, is HIPAA compliant in the sense that it follows the Privacy, Security and Breach Notification Rules.

6) Is IntakeQ HIPAA Certified?

There is no such thing as a HIPAA Certification, however, every year, IntakeQ's HIPAA Compliance Program is verified by a third party (Compliancy Group) to ensure that we are following the latest requirements.

We also receive coaching by a former HHS auditor to help us meet HIPAA standards and implement requirements.

7) Do you provide a HIPAA Business Associate?
If you are subject to HIPAA as a Covered Entity or Business Associate (as defined in HIPAA) and employs our services in a manner that causes IntakeQ to create, receive, maintain, or transmit Protected Health Information (PHI) on your behalf, then you are subject to our HIPAA Business Associate Agreement.

8) Is my data behind a firewall?
All IntakeQ servers and databases use IP whitelist policies, meaning that we only open specific firewall ports that are necessary (e.g. web servers are only open to load-balancers, databases are only open to web servers, etc.).
A Web Application Firewall (WAF) is also used in our public-facing load-balancer, employing a positive security model against the most common 15 attack vectors.

9) Do you perform Penetration Tests?
Yes. We perform automated and manual penetration tests against our infrastructure and web application.

- Weekly tests are performed via a crowd-sourced platform (Detectify).
- Every six months we employ an OWASP expert to retest our web application and APIs for vulnerabilities .
- Continuous automated functional tests built into our deployment process.

10) Does IntakeQ perform Risk Assessments?
Yes. At least once a year, IntakeQ performs an internal risk assessment using an adaptation of NIST SP 800-30, as recommended by HHS.

11) Does IntakeQ have a Disaster Recovery Plan?
Yes. Disaster Recovery and Business Continuity have been built into our infrastructure since day one. We review and test our recovery plans every year.

12) Do you have an SLA?

Yes, we have a 99.95% SLA provided upon request. Historically, our uptime has been above 99.99%, with the exception of September of 2016. For current system status, visit http://status.intakeq.com.

13) Can IntakeQ provide SOC 1 and SOC 2 reports?
We haven't gone through SOC audits. As a small team with limited resources, our compliance efforts have been mostly dedicated to HIPAA. That doesn't mean we compromise on any aspect of our security and availability. We plan to dedicate more resources to regulatory compliance as we grow and enter the enterprise market.

14) Who owns the data that I enter into IntakeQ?
There are 2 different sets of data.

- The data that we collect from IntakeQ users in order to provide the service (name, email, billing information, IP addresses, account settings) is governed by our privacy policy.
- Patient data (intake forms, charts, appointments, invoices, etc.) is owed by you, or your account owner.

15) Is 2-Factor Authentication available?
Yes, IntakeQ provides 2FA to its customers and allows account administrators to enforce 2FA for all account users.

2FA is also available to patients who have access to the client portal, and can be made mandatory by the account administrator.

16) Can I configure custom security policies?
Yes. The account owner has access to the Security Policy section, where they can configure several security-related settings, such as session timeout, password policy, 2FA policy, IP restriction, etc.

17) Are IntakeQ Telehealth sessions encrypted?
Our Telehealth feature works over webRTC in a peer-to-peer fashion. Media shared in our Telehealth peer-to-peer rooms is encrypted end-to-end and can never be accessed by IntakeQ or underlying providers. Each participant in a peer-to-peer room negotiates a separate DTLS/SRTP connection to every other participant. All media published to or subscribed from the room is sent over these secure connections, and is encrypted only at the sender and decrypted only at the receiver.