IntakeQ ePHI & HIPAA Compliance Overview

This document outlines how IntakeQ deals with ePHI (Electronic Protected Health Information) in order to remain HIPAA compliant and help customers achieve the same.

- Section 164.310(d)(2)(iv) "Create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment."
    - No equipment that stores data is moved. Nonetheless, database is replicated between Central US and West US Azure datacenters.

- Section 164.310(d)(2)(i) "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."
    - ePHI will be deleted and purged upon request. Data older than five years may be marked for purgation, although client will be notified before this occurs and this can be configured on an individual basis.

- Section 164.312(a)(2)(i) requires that you "Assign a unique username and/or number for identifying and tracking user identity."
    - IntakeQ addresses this by giving each user accessing the system a unique username specific to the identity of the employee or individual with access to the system.

- Section 164.312(a)(2)(ii) "Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency."
    - IntakeQ is available from any internet location. ePHI is only recoverable through a back-end portal protected by SSL connection.

- Section 164.312(a)(2)(iii) "Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity."
    - The patient facing application and the back-end portal containing patient data will become inactive after thirty minutes of inactivity.

- Section 164.312(a)(2)(iv) "Implement a mechanism to encrypt and decrypt electronic protected health information."
    - All communication between users and IntakeQs' servers is sent over SSL encrypted connections. Data at rest is encrypted by using AES and 3DES. Encryption certificates are rotated every 90 days.

- Section 164.312(b) "Implement hardware, software and/or procedural mechanisms that record and examine activity in information systems that contain or user electronic protected health information."
    - All activity on the secured back-end portal is tracked and recorded in a comprehensive audit log. Users with administrator, developer, or auditor privileges can view or search this log.

- Section 164.312(c)(1) “Implement policies and procedures to protect electronic protected health information from improper alteration or destruction. Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.”
    - In addition to requiring user authentication with password credentials over an SSL secure connection, ePHI submitted by patients cannot be altered modified without first contacting IntakeQ. When an authorized user deletes an intake form, IntakeQ deactivates the intake form and an automated process deletes the form after 10 days.
    - Regular network and application penetration tests performed by a third-party.

- Section 164.312(d) “Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.”
    - All users must provide correct authentication credentials to have access to ePHI. IntakeQ also offers 2-factor authentication, making it especially difficult for unauthorized people to have access to ePHI.
    - Repeated incorrect attempts to log in will result in a user lockout. IntakeQ will require validation of client identity through phone verification, including known details about the client, before unlocking users.

- Section 164.312(e)(2)(i) “Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network. Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.”
    - All data is sent solely over secure SSL encrypted connection, which securely prevents interception of ePHI.

- Section 164.312(e)(2)(ii) “Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.”
    - When transmitted, all data is sent over secure verified SSL encrypted connections.
    - SQL database containing ePHI is encrypted at the database level. Additionally, a second layer of encryption is applied to sensitive fields and decrypted at the application level.
    - ePHI is stored in Microsoft Azure and IntakeQ has obtained a Business Associate Agreement from Microsoft.

The Feb 17, 2010 HITECH Additions to HIPAA specify the obligations of vendors providing secure services. IntakeQ complies as follows:

- Know what information in your account is PHI.
    - IntakeQ defines ePHI in the context of the IntakeQ Intake Forms as any information provided by internet users onto the pre-specified secured, configured web forms that passes through or is stored on IntakeQ servers.

- Make sure that information is backed up, transmitted securely, and encrypted if needed.
    - All information is backed up weekly, and transmitted over a secure SSL encrypted connection.
    - Point-in-time restore is available for the last 35 days.
    - Backup files are also encrypted.

- Implement access controls to track who could have accessed that information — both from the public interfaces and through their back end systems.
    - IntakeQ provides a comprehensive audit log of ePHI data accessed by users in the system.
    - Application and database are hosted in a HIPAA compliant cloud service (Microsoft Azure) and they keep their own audit logs.

- Track uses and disclosures of that information.
    - While connected to the IntakeQ, all access to ePHI is recorded.

- Ensure that all staff that may be accessing your PHI in any way are trained and authorized.
    - Only IntakeQ's trained staff has access to ePHI. Access is restricted from regular support, sales and development members.

- Report unauthorized disclosures of PHI to Health and Human Services and possibly the media.
    - IntakeQ has specific breach protocol policies in place to purge compromised data and alert clients of all unauthorized disclosures detected.

Data Privacy & Responsibilities of Client

While IntakeQ does its best to secure all data, if the customer does not properly use the software, confidential medical information may be disclosed, violating HIPAA. Complete HIPAA compliance requires both users and software to work together.

For example, if a user discloses his or her password or login information to a third party, it may allow a user to bypass security measures. It is critically important that all users practice the following security measures.

- Logout immediately when walking away from a machine.
- Never disclose a password to anyone, including someone claiming to be from IntakeQ.
- Don't reuse your IntakeQ password on any other website (we recommend the use of password managers).
- Change your password at least every 90 days.
- Do not share login with another person. It is critical that each person access IntakeQ using their own username and password.

- Administrators must delete the user accounts of employees who no longer work within their organization.
- Do not write down a password anywhere.
- Make sure that the URL clearly displays both https and the domain name regularly used when logging in. IntakeQ cannot be held liable for organizations or individuals impersonating IntakeQ.
- Do not disclose PHI on emails or SMS messages sent through IntakeQ without the patient's consent.
- Never share access to e-mail accounts that are associated with your IntakeQ account.
- Review and adjust the Security Policy settings in your IntakeQ account to your organization requirements (they can be found under More > Team > Security Policies).
- We strongly recommend the use of 2-Factor Authentication (which can be configured in your Account page).
- Consider using the IP Restriction feature to restrict access to your account based on IP addresses.