OCEAN PRIVACY IMPACT ASSESSMENT FAQ

This FAQ document was created to assist in Privacy Impact Assessments (PIA) involving CognisantMD's Ocean Platform and associated products.

Has CognisantMD completed any privacy audits, security audits or Privacy Impact Assessments for Ocean?

Yes, CognisantMD has completed the following privacy/security reviews for Ocean:

1. Assessment done and passed by St. Michael's Hospital July 2013.
2. Assessment done and passed by Sunnybrook Health Sciences, April 2014.

Three other major Ontario healthcare institutions have conducted privacy/security reviews more recently and proceeded to deploy Ocean. To date, every privacy/security audit has resulted in a pass.

Has CognisantMD completed a Treat Risk Assessment?

Yes. MNP conducted a TRA on the Ocean platform in May 2016. A summary is available upon request. Two threat risk actors and vectors were analyzed, "individual hacker" and "rogue employee". Both were assessed as "low risk".

Who is using the Ocean Platform?

The Ocean platform has updated over 1M patient records at over 300 primary care clinics including over 65% of Family Health Teams in Ontario to date (Oct 2017). Our earliest customers started using the Platform in 2013.

How do your customers avoid privacy and/or security risks when using Ocean?

All PHI is fully encrypted using an encryption key that never leaves the customer site. As a result, even CognisantMD employees are unable to see PHI persisted or even in transit, providing much better security than server-side encryption.

What kinds of PHI are collected, used, modified, disclosed and/or stored through Ocean?

Unencrypted: Nothing except the EMR ID, which is meaningless outside the EMR context.

Encrypted using the clinic's private encryption key (again, never even sent off premises): Most of the patient's demographics (name, phone, email) and conditions of the patient as stored in the EMR.

Can you provide a diagram of how PHI will flow into, out of, and through the Ocean Platform?

The Ocean system moves data between three systems over the Internet:

- the Ocean Android tablet app
- the Ocean server
- the Electronic Medical Records (EMR) package

A fourth system, available for EMRs such as QHR Accuro and TELUS PS Suite, is OceanConnect. OceanConnect is an Android app that brokers communication between an EMR server (local or ASP) and the Ocean server. It must run on a secure network with access to the EMR server.

In order to prevent eavesdropping, the Ocean system uses HTTPS, which is the global standard for secure data transmission used by governments and banks around the world. It would take millions of years to "brute force" hack the current standard of SSL encryption. CognisantMD uses a signed, registered, publicly-trusted SSL certificate to protect against "man in the middle" attacks.

A network flow diagram is available upon request.

Do CognisantMD employees have access to PHI?

CognisantMD never sees a client's encryption key and therefore has no ability to see PHI. Individual users in the system have "roles" that are enforced using the industry-standard "Spring Security" framework.

Where is PHI data stored on Ocean?

No patient or clinical data is stored on the Ocean tablet. This guards against any privacy breaches in the event of theft or loss of the tablet. The Tablet is also equipped with “tamper proofing” technology that ensures that the installed packages is unchanged. If other apps are installed or uninstalled, the Ocean Tablet app will delete authentication and encryption data immediately.

All Ocean data, including PHI, is stored in our primary storage facility located in Toronto, with additional copies of the data kept in a warm failover disaster recovery facility in Vancouver. Our data centers are SSAE 16 certified: this means they are locked, guarded, and monitored through closed-circuit television systems, with onsite security teams, military-grade pass card access, and biometric finger scan units providing additional security. You can read about the security measures in place at our data storage facilities here: http://ssae16.com/SSAE16_overview.html.

Administrative access requires an SSH connection with a key held only by CognisantMD system administrators. Database access is limited to the application server cluster via IP whitelisting, meaning external computers are blocked from accessing the database directly. The database is secured with a password known only to CognisantMD system administrators. Patient data is held in the Ocean server only as long as required and automatically at scheduled intervals.

Is PHI processed, disclosed, or retained outside of Canada?

All Ocean data, including PHI, is stored in our primary storage facility located in Toronto, with additional copies of the data kept in a warm failover disaster recovery facility in Vancouver, BC. Long-term backups are stored in the Amazon datacenter in Montreal. For more details on our data storage, see “Where is PHI data stored on Ocean?”.

Do you have any plans for quality assurance and audit programs to assess the ongoing state of the safeguards applicable to the Ocean Platform?

The fundamental safeguard of the system is client-side encryption of PHI. This is protected by the senior members of the CognisantMD team who have an extensive background in enterprise security architecture. We also perform regular reviews of our Threat Risk Assessment.

What contingency plans and documented procedures are in place to identify and respond to security breaches or disclosures of PHI in error?

In accordance with PHIPA, all CognisantMD staff are trained to notify the PHI custodian immediately. CognisantMD is a small team with decades of experience in highly sensitive data management software, including EMR software. All CognisantMD staff been trained in requirements and ethics for protecting personal health information.

CognisantMD keeps a corporate wiki that describes the operational steps of handling PHI data, such as using SSH for all database access, reporting breaches, etc.

In the case of an audit requiring a patient report or a user report, what information can CognisantMD provide?

Ocean maintains an audit log of user access and time to the system. Audit records contain necessary information to identify the nature and details of the action, including the EMR ID of the patient. Upon request, CognisantMD can produce audit records in JSON format (which supports the "ragged" data captured in our audit log), which could be converted to CSV if required.

How does CognisantMD maintain a test system/environment?

CognisantMD maintains a staging server and a test server in Amazon AWS. It also maintains a continuous build/test cycle in its Toronto head office. No ‘live data’ (patient PHI, user information, etc.) is ever included in any test environment (“demo data” is used).

How is the Ocean Platform maintained and how is PHI protected during maintenance?

System maintenance is normally done Monday between 9pm and 11pm ET. Most of this time the system is available. There is never any impact on patient privacy as all PHI is encrypted using private keys not known to CognisantMD staff.

ress
5 Yonge Street Suite 304
nto ON, M4N 2M1