Ocean Security FAQ

1. How is Personal Health Information (PHI) kept secure in Ocean?

- All patient data stored in Ocean is encrypted end-to-end using the industry-standard 128-bit AES (Advanced Encryption Standard) or better.
- Ocean stores its data in highly secure, 100% Canadian-based data centres. The data centres utilize superior data center infrastructure including environmental controls, fire suppression systems, redundant power sources and UPS backup, multi-homed Tier 1 bandwidth, 24/7 security including card entry, video monitoring, as well as technical and monitoring capabilities. All Ocean data centres have multiple security and compliance certifications, including ISO 27001.
- Administrative access requires an SSH connection with individual keys held only by CognisantMD system administrators plus a second factor. Production server access is further protected by a separately secured VPN and access is fully audited.
- Database access is limited to the application server cluster via a private subnet, meaning the servers are inaccessible from any external source. The database is secured with a password known only to CognisantMD system administrators.

2. How is PHI kept secure in transit?

- All Ocean Application Programming Interface (API) calls are made via HTTPS (TLS 1.2 or above) between Processing Service and Ocean System, and between Web Service Endpoint and the Ocean System. This helps in preventing visibility of data to potential intruders by providing confidentiality and integrity of data.
- All patient data that is transmitted to/from Ocean is encrypted using a unique one-time key which is further encrypted with a site-specific Shared Encryption Key. CognisantMD staff do not have access to any keys used to encrypt PHI.

3. What is the Shared Encryption Key (SEK), and how does it work?

- The SEK is a secure key used by Ocean to exchange patient data safely and securely. It *must* be at least 16-characters long. (24- and 32-character keys are optional.) It *must* contain at least one digit, one uppercase letter, one lowercase letter and one punctuation mark (e.g.!,., _, @, etc.).
- Each clinic or organization designates an Ocean site administrator. This administrator sets up the SEK and only shares it with authorized personnel within your organization.
- Any device (workstation, laptop, tablet etc.) using Ocean will require this SEK to view patient data.
- No one at CognisantMD or outside of your organization has access to your SEK. This ensures no one can view any of your patient data held within Ocean.
- The shared encryption key (SEK) provides an extra layer of security for patient health data stored temporarily in Ocean beyond industry standard safeguards.

- All patient data that is transmitted to/from Ocean is encrypted using a unique one-time key which is further encrypted with a site-specific Shared Encryption Key. This one-time key is never stored in Ocean in an unencrypted form. This enhances confidentiality and integrity of PHI being transmitted by making decryption of bulk patient data a lot harder. Access to a one-time key only grants access to a single encrypted patient.

4. How do you protect against password guessing and brute force attacks?

- We have the following password requirements implemented in Ocean today:
  - Minimum 8-character length passwords
  - At least 3 of the following of the following kinds of characters must be used:
    - Uppercase characters
    - Lowercase characters
    - Numbers
    - Special characters (%, *, $, etc.)
- Two-factor authentication can be set up to provide an additional level of security for Ocean users. Once enabled, the user will be prompted to enter a 6-digit code generated by an authenticator app each time they sign into Ocean.
- Ocean site admins can generate a report of users who belong to a site and are not using 2 factor authentication and can follow up with those users as part of a regular audit process.
- After 5 failed login attempts, a user must wait 30s before trying to login again.
- After 10 failed login attempts a user must wait 1hr before they may try to login again. There can be at most 10 failed login attempts in an hour.

5. What security measures are in place to guard against cyber threats?

- Ocean is monitored continuously (24 hours a day, seven days a week) for security, privacy and other events that could impact system reliability and availability.
- CognisantMD leverages several third party platforms to detect and mitigate threats to the system i.e., AWS, Cloudflare, Datadog, SumoLogic, Azure etc.
- The monitoring system incorporates signals from VPC flow logs (network traffic logs), AWS dashboard + API use logs, AWS CloudTrail, operating system logs and application logs
- Operating system, application, and server logs are collected centrally
- Log events are analyzed automatically, and alerts sent to the Operations team when unusual behaviour is detected.
- AWS GuardDuty detects new attacks that involve anomalous network traffic entering or leaving the system.
- Web application firewall (WAF) protects against a variety of application layer attacks. Rate based rules are continually fine tuned specifically to Ocean.

In 2021, CognisantMD engaged Cycura (https://www.cycura.com/) to provide a comprehensive technical Threat and Risk Assessment (TRA) against the Ocean eReferral platform, and its associated APIs. The assessment consisted of:

- A Grey and White Box Penetration Test conducted to ascertain the potential number of technical vulnerabilities within the platform itself, its associated infrastructure, or its operational management.
- A formal TRA review of both the technical output of the Penetration Test, as well as the governance and controls in place at CognisantMD to support the platform.

Stakeholders who have a legitimate need to review the full TRA document may do so after signing a non-disclosure agreement with CognisantMD and the Ontario eServices Program.