OceanMD Privacy Impact Assessment

Version 1.43

July 25, 2023

Document History

Version	Date	Author	Description
1.0	June 8, 2018	Greg Taylor	Initial draft
1.1	June 21, 2018	Jeff Kavanagh	Minor edits from SCA/TRA review
1.2	September 10, 2020	Yaron Derman Doug Kavanagh	draft updates to - reflect SMS communication modality, - expanded product offerings - changes to product names - Request submission process for TRA and privacy risk findings access Content changes in the following areas: - Section 7.1.3 expanded to describe SMS opt-out - IPC PIA Questionnaire Responses - reflecting SMS and OntarioMD Health Report Manager privacy considerations
1.3	October 28, 2020	Yaron Derman	Incorporated reviewer input
1.4	November 25, 2020	Yaron Derman	Added the final bullet to section 7.1.5 Incorporated feedback from Sylvia Carney, Privacy Lead, Ontario eServices Program
1.41	Apr 1, 2021	Doug Kavanagh	Updated to include optional new workflow from the SMART on FHIR launch with feedback from Sylvia Carney.
1.42	July 24, 2023	Doug Kavanagh Yaron Derman	Expanded Section 6 (Solution Overview) to include a privacy-focused description for each product and module. Revised section 7.1.2 to align with recent product updates Updated the privacy policy and EULA. Added description of data disposal methods and procedures. Updated hyperlinks for referenced articles.

			Updated CognisantMD references to OceanMD.
1.43	July 25, 2023	Doug Kavanagh Yaron Derman	Added Ontario eReferral Repository exception to section 7.1.2

Contents

1 Executive Summary

OceanMD's Ocean platform is used by thousands of clinicians across Canada to improve patient care with its patient engagement and provider networking technology. Ocean integrates with many healthcare systems and provides tools for patient messaging, reminders, online booking, secure website forms, studies, eReferrals, eConsults, eOrdering, eSubmissions, and secure report distribution.

This privacy assessment was conducted[1] in collaboration with MNP[2] to provide clinicians and other healthcare industry stakeholders visibility into OceanMD's privacy practices. It covers how OceanMD protects patient data: the procedures and policies in place to ensure appropriate safeguards are in full effect, and the processes that ensure incidents are handled appropriately.

2 Audience

This PIA is intended for stakeholders considering the implementation of the Ocean system for the purpose of patient engagement or eRequest management (eReferrals, eConsults, eOrders and eSubmissions), either in the context of a regional health network deployment or within a medical or health service clinic.

3 In Scope

The scope of this PIA is the core Ocean platform, including both patient engagement technology (such as tablets and patient messaging) as well as the provider network and eRequest management.

4 Out of Scope

This PIA does not include considerations relating to:

- EMR and EHR-specific implementations
- Specific third-party systems integrating with Ocean
- Ocean Studies

[1] The assessment has been updated since September 2020 to include new technology components and features of the Ocean platform, such as online booking and SMS messaging.
[2] https://www.mnp.ca/en

5 Privacy Principles

5.1 Overview

OceanMD operates as an Electronic Service Provider and, in some scenarios, as a Health Information Network Provider (HINP) under PHIPA/PIPEDA. The following sections discuss how Ocean adheres to the privacy principles of PHIPA/PIPEDA. OceanMD also presents and discusses these principles in the privacy section of its company website.

5.1.1 Electronic Service Provider

OceanMD, via the Ocean platform, acts as an Electronic Service Provider in normal operations. We provide services to Health Information Custodians (HICs) to allow them to handle personal health information with respect to the products and services provided by Ocean, except in those cases where we are acting as a HINP, as outlined below.

5.1.2 Health Information Network Provider

OceanMD, via the Ocean platform, acts as a HINP when it is administering its provider network and eRequest management services (such as eReferrals and eConsults). In some cases, these HINP responsibilities are carried out by a third party, such as the Ontario eServices program or its partner organizations in Nova Scotia.

5.2 Principles

5.2.1 Accountability

An organization is responsible for personal health information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles.

5.2.2 Identifying Purposes

The purposes for which personal health information is collected shall be identified by the organization at, or before, the time the information is collected.

5.2.3 Consent

The knowledge and consent of an individual are required for the collection, use, or disclosure of personal health information, except where appropriate.

5.2.4 Limiting Collection

The collection of personal health information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.

5.2.5 Limiting Use, Disclosure and Retention

Personal health information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal health information shall be retained for the minimum duration necessary for the fulfillment of those purposes.

5.2.6 Accuracy

Personal health information shall be as accurate, complete, and up to date as is necessary for the purpose for which it is used.

5.2.7 Safeguards

Personal health information shall be protected by security safeguards appropriate to the sensitivity of the information.

5.2.8 Openness

An organization shall make readily available to individuals' specific information about its policies and practices relating to the management of personal health information.

5.2.9 Individual Access

Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal health information, and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

5.2.10 Challenging Compliance

An individual shall be able to address a challenge concerning compliance with the above principles to the designate individuals accountable for the organization's compliance.

6 Description and Solution Overview

Ocean by OceanMD is a system that facilitates the sharing of data between patients and their healthcare providers ("Patient Engagement products") and between healthcare providers (e.g., eReferrals, eConsults, eOrdering and eSubmissions").

Ocean Patient Engagement products can be used by clinics to allow patients to complete forms on tablets (“Ocean Tablets”) or via a secure, private web link (“Patient Messaging & Reminders”). It can also be used to present forms on public websites, allowing patients to complete website forms (“Website Form Links”) and book appointments (“Online Booking”).

Ocean includes thousands of different clinical forms that can be queued for patients at the physician’s discretion, covering a wide array of clinical presentations. It also includes a graphical form editor to enable clinics to build their own forms, which can be shared easily between clinics.

The Ocean Provider Network module is used by referring clinicians (“Referrers”, “requesters” or "source providers") to send patient data (including personal health information) to other healthcare providers ("health directory listings", “referral targets” or "receiving providers"), for clinical purposes, such as an eReferral, eConsult, or eOrder.

A primary feature of Ocean is the availability of modules that allow common electronic medical record systems (EMRs) used in many clinician offices to interface with Ocean. Integration modules are currently available for EMRs including TELUS Practice Solutions, TELUS Med Access, QHR Accuro and WELL EMR OSCAR Pro, as well as external communication systems such as OntarioMD’s Health Report Manager (HRM). Ocean uses a dedicated, private, and secure server called Cloud Connect to safely exchange personal health information while communicating with these external systems.

The Ocean system is built upon the principle of “Client-Side Encryption”, in which clinics receive a “shared encryption key” that is used to encrypt and decrypt data. The clinic is responsible for maintaining and safeguarding the shared encryption key. The strategy attempts to keep the knowledge of this key limited to just the health information custodian as a general safeguard, so that no other stakeholders can decrypt and view the personal health information, unless expressly permitted to do so. For this reason, the shared encryption key is not stored or logged on the Ocean server. It is not visible to OceanMD system administrators. As a policy, OceanMD employees will not request to see a client’s shared encryption key.

For pragmatic reasons, individual clinics may nonetheless choose to store their shared encryption key privately on a separate Ocean Cloud Connect server. This storage is used as a reliable backup mechanism for the shared encryption key. The storage of the shared encryption key in Cloud Connect also enables automated communication of personal health information with trusted third-party systems (such as the clinic’s EMR). OceanMD uses dedicated access restriction protocols and specific safeguards in Cloud Connect to keep the shared encryption key private for clinics.

6.1 eForms

Ocean Forms ("eForms") consist of a very large, customizable, open-source library of clinical and administrative patient forms.

The Ocean library has over 2000 patient-facing forms and questionnaires, including hundreds of standardized and clinically validated questionnaires with scoring and clinical decision support built in. It also includes a large variety of real-world specialist referral forms and order forms.

Users of the Ocean platform can create, edit, share, and maintain their own list of Ocean forms. Ocean provides an online graphical form editor (as well as an optional XML file format) which users can use to edit these forms. The forms are flexible in terms of their ability to hide, show, customize, and calculate content on the form, based on a variety of criteria, due to its embedded Javascript form scripting and templating engine. Many end users of the platform have independently used the form scripting engine to create regional and pathway-specific recommendations or implement customized clinical prediction rules based on patient criteria. Other sites may choose to incorporate forms built by these users in their own clinics, sometimes customizing them further for their own purposes.

6.2 Tablets and Kiosks

Patients use ocean tablets and kiosks to register at a clinic, complete Ocean forms, update their contact information, review clinic policies and consent, and provide a detailed patient history.

To use the kiosk, patients must provide their health number (or an alternate identifier such as a student number, if configured) and date of birth. Ocean checks in real-time to ensure that the patient has an appointment booked that day within a configurable time window. If so, the patient is permitted to register and proceed. If there is no pre-existing appointment, the kiosk will permit the patient to check-in only when it is configured to accept “walk-ins”; otherwise, the patient is instructed to present to reception. The kiosk may be configured at this time to show additional forms, such as a COVID-19 symptom screening questionnaire.

To use the tablet, a clinician must first enter the patient’s Ocean “reference number”, which is a random integer generated and displayed by Ocean used to link the tablet to this specific patient. To reduce the chance of an incorrect linkage, the clinician or patient must also confirm the patient’s birth date. Once linked, the tablet can proceed to optionally display the patient’s contact information for confirmation and update purposes, followed by a series of Ocean forms that have been either manually selected by the clinician or automatically queued based on heuristics.

Once linked, the kiosks and tablets have access to a limited set of personal health information from the patient’s chart. This PHI is used for clinical purposes as determined by the forms. For example, users may be prompted to review and confirm their current medications, or to review a flu shot reminder form, depending on the clinician’s preference and the presence of this information within the patient chart. To maximize privacy, this information cannot be viewed outside of the forms themselves; it is not stored on the device and is encrypted both at rest and in transit.

Once the patient finishes, the answers are automatically summarized and updated within the patient's chart in the EMR. The kiosk can additionally book a walk-in appointment or mark an existing appointment in the schedule as "arrived".

6.3 Patient Messaging

Ocean's Patient Messaging functionality allows clinicians to send secure messages and attachments to their patients and invite them to complete forms and questionnaires online. With Ocean's EMR integration, patient records are seamlessly updated without any scanning, typing, or manual staff involvement.

Clinicians may request an alert when your patient has read or responded to a message and receive notifications when a message is not viewed within a specified time.

These messages and forms are sent to patients with a customizable email containing a secure link. The link provides the patient with temporary access to the content via a hyperlink. For privacy reasons, the link is protected with a validation prompt, requiring the patient to enter either their birth date or some other combination of information such as the health number or an access password. Users can specify the lifespan of these secure links with a time period measured in days; once expired, the link can no longer be used to access the secure content.

The messages may be sent to individual patients on an ad hoc basis, or they can be triggered automatically based on an upcoming or recent appointment, or they can be sent to a group of patients.

Since these messages and forms are often re-used across many patients, Ocean has a template manager module within its user portal, where users can define the message template's email structure, secure message content, notification preferences, and so on.

Patient Group Messaging may be used to send the same templated message to a group or cohort of patients. To define the group of patients, health information custodians may run a query within their EMR to generate a list (cohort) of patients. This list may be exported in a variety of CSV (spreadsheet) file formats supported by Ocean, and subsequently uploaded into the Ocean portal. Once the full cohort of patients is uploaded to Ocean, users may proceed to select the cohort and a given template to send a batch of emails to the patients.

Despite the privacy protections used by Ocean for patient messaging as described above, due to the inherent privacy risks of email, health information custodians are strongly encouraged to collect and document email consent for participating patients prior to sending these patients any messaging.

6.4 Online Booking

Ocean's online appointment booking product may be configured by clinicians to offer real-time online booking for patients. Clinicians can choose from their set of EMR schedules to offer online via a "booking link" that can be hosted on the clinic's website. A large variety of booking rules may be configured for a schedule, specifying which types of appointments may be booked and when they may be booked. The online booking form is also configurable, allowing clinics to enforce clinic policies and consent prior to permitting the booking.

Patients typically access the online booking link on their provider's website. They proceed by signing in with their basic credentials, including their name, birth date, and health number (or equivalent identifier). Clinics may choose whether patients must have an existing chart in the system or whether new (previously unregistered) patients can book as well. Ocean checks the patient's credentials in real-time against the EMR system to ensure they match.

Once signed in, the patient completes the customizable booking form. Basic contact information may be shown on the form, such as the patient's email and address, for review and updates as needed. The available time slots are then shown based on a real-time query with the EMR's scheduling system, ensuring that the time slots are available even when manual secretary bookings are happening concurrently.

Ocean's online booking currently supports the following EMRs via proprietary implementations:

- TELUS PS Suite
- TELUS Med Access
- QHR Accuro
- WELL EMR OSCAR Pro

Authorized EMRs that adhere to Ocean's FHIR Cloud Connect Implementation Guide are also supported:

- Profile Intrahealth

6.5 Reminders

Ocean Reminders is an automated reminder, messaging, and form administration system. It connects to an EMR's scheduling system to determine a set of recent or upcoming appointments that meet configurable criteria. The patients with these matching appointments are notified with an Ocean message sent via email, SMS, or both.

Users can specify customizable templates for Ocean Reminders to use as the notification message. The templates allow users to customize the email subject, body, SMS options, validation requirements, and forms attached to the notification.

6.6 Website Forms

Ocean Website Forms allow healthcare providers to host Ocean forms on their website for patients to complete. The forms can be used for a variety of clinical and administrative purposes, including waitlisting, new patient registration and intake forms, prescription and other eRequests, health event and vaccine reporting.

The forms may be configured as open-access or “patient-authenticated”. The open-access forms may be completed and submitted by anyone accessing the website, without requiring authentication. The patient-authenticated forms require users to first sign in with the basic credentials in their chart (namely, their first name, last name, date of birth and health number or equivalent identifier), similar to the sign-in process required for Ocean’s online booking.

Patients may use the patient-authenticated website forms to submit a secure message to their health provider, as well as a set of attachments such as a photograph or health document. Standard formats such as PDF and JPEG are supported. The files are virus-scanned by Ocean prior to making them available for download.

The provider may access and download the website form submissions using the Ocean portal. To avoid the automatic import of inappropriate content, the provider must first review and accept the submission, after which it is automatically downloaded to the provider’s EMR.

6.7 Provider Network

The Ocean Provider Network is a comprehensive eRequest management and communication platform that securely connects providers and their patients for the provision of healthcare. It consists of a comprehensive, map-based searchable directory of health services, applications for managing requests such as eReferrals, eConsult, eOrders and eSubmissions, an analytics platform, and a notification system.

The Ocean Healthmap is a comprehensive, map-based directory that makes it easy to search and access health care services. In collaboration with provincial health care systems, the Healthmap is actively maintained and updated, empowering providers to make more informed care decisions. It assists providers in finding appropriate specialists and filter by subspecialties and health services. It allows providers to quickly view and sort services by calculated wait times and to select the most convenient location based on these wait times, or other criteria such as the distance from patient.

Clinics can easily claim, update, and customize their own directory listings. The directory listings are also pulled from regional repositories, such as the Provincial Provider Registry (PPR) in Ontario. To ensure these directory listings are accurate and legitimate, Ocean maintains validation status for individual listings, as provided by regionally authorized individuals using the system.

Ocean eReferrals replace fax-based referrals with the goal of improving privacy, reducing workloads, eliminating errors, and improve system wait times by assisting with the reallocation and optimization of services.

Ocean eConsults provide a secure, patient-specific communication channel directly between primary care providers and specialists, without requiring a formal referral, appointment booking and consultation between the specialist and the patient. They are primarily an aid for primary care providers to provide timely and effective care for their patients for specific issues under the guidance of a specialist. Unlike many platforms, Ocean allows the requesting or receiving provider to convert an eConsult to an eReferral or vice-versa, when appropriate.

Ocean eOrders allow providers to rapidly and accurately request diagnostic investigations and procedures for their patients directly from their EMR. They are typically used for diagnostic imaging (such as MRIs) or laboratory services. Like Ocean eReferrals, the eOrders can improve care over traditional fax-based communications with real-time, secure communication and notifications. They can also incorporate appropriateness criteria to ensure orders are accurate and appropriate.

Ocean eSubmissions allow providers to access a centrally managed eForms library and securely submit patient health information to authorized organizations, with optional pre-population of fields from their EMR. They may be used for a variety of clinical, public health, and health administrative applications, such as: adverse event reporting, disease surveillance, study recruitment, and ministry of transport applications.

6.10 Cloud Connect

Cloud Connect is an optional, separate server tier within Ocean's infrastructure that serves as an integration bridge between Ocean's core server and its connected third-party systems, such as EMRs, EHRs, alternative provider networks, and government systems. Due to the requirements of these integrations, Cloud Connect must be able to decrypt and re-encrypt personal health information as part of its communications and business logic. Users may opt-in to store their site's encryption keys privately within Cloud Connect to enable this functionality (and as a back-up mechanism for the key itself).

Cloud Connect is implemented as a separate tier from the main Ocean server for several reasons:

- It allows sites to maintain their encryption keys privately outside of the core Ocean server, providing the privacy advantages of client-side encryption, while still enabling the server-side decryption features that are inherently necessary for system connectivity.
- It supports the enforcement of additional security, logging, and access constraints for users, particularly when accessing the site's shared encryption key, to ensure this information is kept highly confidential.
- The impact of third-party integrations is kept predominantly within Cloud Connect, isolated from the core Ocean server, mitigating the risk of cascading errors related to the integrations and their occasional service degradations.

6.11 API and FHIR Integrations

Authorized third-party systems may connect to Ocean for clinical, administrative, or analytic purposes. To provide this connectivity, Ocean offers inbound (RESTful), outbound ("webhook"),

and message exchanging interfaces with several standard protocols, particularly HL7 FHIR as the health industry standard.

To connect, the integrator must first authorize their system with Ocean using their Ocean user account's administrator-level access to a particular Ocean site, using the Ocean portal to obtain a set of site-specific access credentials (namely, a “client ID” and “client secret”). These credentials are used to receive time-limited access to the Ocean site via Ocean's APIs.

When a request is made by a third-party system via the API, the credentials are first validated using a standard OAuth2 authorization protocol. If the credentials are valid, they may be used for any authorized API call to read or write certain types of data from Ocean. The validation and subsequent API calls are logged and, when necessary for auditing purposes, can be traced back to the original authorizing user. Credentials can be revoked at any time, either by the site administrator or by Ocean’s own administration team.

Ocean's Open API protocol is provided directly with the Ocean server using a set of RESTful connection endpoints. Clients may use their credentials to issue HTTPS "POST”, “GET” and “PUT” calls against the Ocean server to send or retrieve specific data sets. Some of these data sets involve PHI and some do not. The API itself does not encrypt or decrypt PHI, so clients must do the encryption and decryption themselves when working with PHI, using their site’s shared encryption key.

In contrast, Ocean’s FHIR API involves the exchange of unencrypted PHI between systems; this exchange of unencrypted PHI is necessary to adhere to the FHIR standard. Since this API therefore involves the decryption of PHI, clients must activate Ocean’s Cloud Connect server and store their shared encryption key within Cloud Connect. This activation enables Cloud Connect to handle the encryption and decryption of PHI on the client’s behalf while fulfilling API requests.

Ocean also implements several of its own proprietary API implementations as a client to connect to legacy EMR systems. For example, to connect to TELUS, QHR, or WELL EMR OSCAR Pro systems, Ocean’s Cloud Connect server issues a series of calls via REST to send and retrieve data from these systems. Ocean site administrators may configure their site to connect to a specific EMR server using these protocols. Since the proprietary APIs offered by these systems also work with decrypted PHI, Ocean’s Cloud Connect handles the encryption and decryption as needed to communicate.

7 Privacy Analysis

7.1 Principles Analysis

7.1.1 Accountability

- OceanMD has a publicly designated privacy officer to provide leadership on compliance with privacy accountability. Dr. Doug Kavanagh is the OceanMD Privacy Officer. The Privacy Officer can be reached at privacy.officer@oceanmd.com, or by phone at 1-888-864-8655 x701.

- All OceanMD employees and representatives are provided with resources to learn the fundamentals of privacy. an Employees must also successfully complete an online privacy training module annually.

7.1.2 Identifying Purposes

- OceanMD / Ocean does not collect personal health information without providing a clear explanation of the intent in the system's user interface.

- Health information custodians may use Ocean to collect personal health information for the sole purpose of providing their patients relevant clinical services. Ocean collects this information as an electronic service provide on behalf of the custodian, but OceanMD or its partners do not use or disclose the information for any other purpose.

    - ⊄ An exception to OceanMD's PHI usage policy was implemented in Ontario, beginning March 31, 2023, under the mandate of the Ontario Health government. eReferrals sent within Ontario under the Ontario eServices Program, including some personal health information, may be shared with the Ontario Health eReferral Repository for use by authorized Ontario Health personnel for several purposes, including to support broader health system planning. For more information, see this article: ehealthce.ca/eReferral-Repository-.htm (current July 25, 2023)

- Some personal health information such as the patient's email or mobile phone number, may be used to notify the patient of specific events or communications related to the platform, under the direction of the health information custodian. Health information custodians are encouraged by OceanMD to obtain consent from patients prior to using any communication service such as email.

- Health information custodians may also occasionally use Ocean as an electronic service provider to collect information for patients for research and clinical studies ("Ocean Studies"), which may include information beyond the direct provision of healthcare. In

these circumstances, the HIC is expected to obtain informed consent from patients prior to the collection of any information. OceanMD does not use or disclose any information within these Ocean Studies to third parties.

7.1.3 Consent

- Based on Ocean's end-user license agreement (EULA), providers are required to obtain the appropriate consent from patients prior to using these services, unless implicit consent is deemed appropriate by the accountable health information custodian.
- Ocean can be used as a mechanism for collecting consent from patients (for example, sending a consent eForm via email or secure messaging service) and documenting evidence of this consent in the client's EMR. It should not be used as the client's system of record for consent because Ocean regularly purges PHI from its databases.
- When Ocean's email and/or text message services are used to send information to patients, the health service providers are reminded that they have a responsibility to obtain informed consent from patients.
- Each initial communication sent to patients via a text message includes instructions on how to opt-out of text message delivery. OceanMD will treat this as a global text message opt-out such that the relevant phone number will no longer receive any Ocean communication from any Ocean site.

7.1.4 Limiting Collection

- OceanMD / Ocean never collects personal health information beyond what is necessary to fulfill its primary use cases (such as the completion of a designated clinical questionnaire by a patient's health service provider).
- All personal health information is encrypted with private encryption keys prior to leaving the clinic. Since OceanMD personnel do not have these keys, it provides a strong safeguard against unauthorized use.
- All collection and processing of information is in accordance with Canada's and Ontario's privacy laws.

7.1.5 Limiting Use, Disclosure and Retention

- OceanMD / Ocean does not use personal health information for purposes other than those for which the information is collected.
- These purposes are limited to the use cases of its patient engagement and provider network products, such as the completion of an Ocean tablet questionnaire or an Ocean secure patient message sent to the patient via email or SMS.

- The actual uses and disclosures by the system are directed by the health service providers to fulfill these use cases in accordance with our EULA. OceanMD acts as an electronic service provider for these uses in accordance with PIPEDA / PHIPA[3].

- Individual HICs may choose to authorize and activate third-party integrations with their Ocean site by configuring their site administration settings in the Ocean portal. In this scenario, the HIC is choosing to enlist the third party as an agent or electronic service provider under PIPEDA/PHIPA to act for or on behalf of the custodian. The agent may use PHI from the HIC as necessary to provide additional services, such as the completion of an eReferral or ancillary patient support services. In this context, OceanMD/Ocean is acting as an electronic service provider under PIPEDA/PHIPA (as opposed to an agent) to enable the agent's connectivity to the HIC, without using or disclosing any PHI itself.

- Details on our data retention and disposal procedures are discussed in Exhibit 8.6.

7.1.6 Accuracy

- The Ocean system interfaces with the healthcare practitioner's EMR, which is the system of record, to obtain comprehensive and up-to-date clinical information for patients. It is the healthcare practitioner's responsibility to ensure the accuracy of PHI collected in/stored/accessed from the EMR.

- Ocean synchronizes with the EMR nightly to ensure it is up to date regarding the email address, mobile phone number and other relevant information.

- Safeguards are placed in the user interface to ensure important personal health information is periodically confirmed by patients for accuracy. For example, patients may review their contact information for accuracy each visit on an Ocean tablet. Validation checks are conducted for birth dates, phone numbers and health numbers to reduce the likelihood of error.

7.1.7 Safeguards

- As a general safeguard, Ocean's end-to-end public-private key encryption ensures that all personal health information is inaccessible to third parties, including OceanMD employees, unless these third parties have been specifically authorized by the HIC to access this PHI.

- Ocean provides the individual HICs' site administrators the ability to run audit reports of user activity associated with their site to monitor appropriate PHI collection, use, access, and disclosure (see Exhibit 8.3).

---

[3] See OntarioMD's Privacy Frequently Asked Questions for Physicians and Staff for more information. Last accessed: Sept 10, 2020

- Industry-standard techniques such as 256-bit encryption, strong password policy management, two-factor authentication and user access restrictions are universally used within OceanMD systems and are strictly enforced by the development and operations team.

- Source code reviews are regularly performed to limit the risk of unintentional disclosures of personal health information.

- Third-party provider network integrations with Ocean have limited access to personal health information only within sites designated by the applicable health information network provider (HINP). These integrations are only permitted by OceanMD in contexts where the HINP has explicitly authorized such integrations with and on behalf of participating HICs.

- A threat-risk assessment (TRA) was performed by MNP of the Ocean platform and Cloud Connect. It deemed that the safeguards put in place result in an overall "low" risk to personal health data.

7.1.8 Openness

- OceanMD endeavours to publish its policies and procedures openly on our support portal, which is publicly available.

- OceanMD also provides a simplified patient-friendly summary of our privacy policy and public links to our existing PIAs. Many other articles that discuss privacy and security are available in our support portal.

7.1.9 Individual Access

- Individuals may consult our patient-facing support articles to learn more about the company's policies on personal health information usage.

- Since Ocean does not store unencrypted personal health information, OceanMD is unable to provide patients with direct access to their personal health information. If a patient makes a personal health information request from Ocean, OceanMD will take steps to connect the individual with the applicable health service providers to facilitate access and review in a timely manner. (Note: Since Ocean typically pulls data from third-party EMRs as its primary information source for personal health information, individuals are likely to first request access to their electronic patient chart within these systems at their clinician's office. They may request corrections or annotations for their chart in these systems as necessary, whereupon the changes will be automatically updated in Ocean as well.)

- OceanMD can also, upon request, provide individuals with a full audit log of the use and disclosure of their personal information by its systems, with the constraint that the

patient's identifying information be provided to enable these queries, such as a health number or an EMR chart ID[4].

7.1.10 Challenging Compliance

- OceanMD's senior leadership and its privacy officer pledge to create an open, supportive environment for individuals who have any concerns about the company's compliance to the above principles.
- Health information network providers (HINPs) interacting with OceanMD as an electronic service provider are encouraged to contact OceanMD with any concerns as they arise.
- Individuals are also encouraged to contact OceanMD's privacy officer with any concerns.
- The company commits to providing a timely and fully considered response in these circumstances, including the provision of any organizational and technological changes deemed necessary to correct gaps in this compliance.

7.2 Privacy Risks and Recommendations

OceanMD maintains a list of privacy risks. The list is updated as risks are identified, and risk mitigation recommendations are developed. Open risks are maintained in the Privacy Risk Dashboard and reviewed at least monthly in a standing meeting attended by the Privacy Officer and relevant department personnel.

7.2.1 Privacy Risk Review Process

1. Privacy risk is identified.
2. Privacy risk is added to the Privacy Risk Dashboard. The following information is tracked:
    a. A description of the privacy risk
    b. Initial recommendations
3. Privacy risks are reviewed monthly.
    a. Recommendations are reviewed and updated.
    b. Remediating actions taken since the last meeting are reviewed and updated.
    c. New remediating actions are added, and work scheduled.

[4] Because all PHI within Ocean is encrypted, OceanMD cannot generate a patient-specific report across all sites. Each site's audit log is protected by site-unique encryption (called a private hashing algorithm). The private hashing algorithm must be used in conjunction with the patient-specific identifiers from the corresponding EMR to cross-link the patient's information to existing audit records. While this delivers superior PHI protection, it does result in a more labour-intensive audit review process.

7.3 IPC PIA Questionnaire Responses

Question	Response	Comment
A1. Is there an organizational strategic plan or business plan that addresses privacy protection?	Y	
A2. Does your organization have a written privacy policy or statement of information practices?	Y	
A3. Have privacy policies or procedures been developed for various aspects of the organization's operations?	Y	
A4. Do the privacy policies or procedures that you identified in response to questions A2 and A3 ensure the following: • Personal health information is collected in accordance with PHIPA and other applicable legislation; • Individual consent is obtained in accordance with sections 18 of PHIPA where consent is required; • A written public statement about the organization's information practices, who to contact with privacy questions or complaints, and how to obtain access or request correction of a record of personal health information is readily available to individuals, as outlined in section 16 of PHIPA; • Individuals are entitled to request access to and correction of their own personal health information as provided for under sections 52-55 of PHIPA, subject to certain exceptions; • There is a record retention schedule for records of personal health information that outlines the minimum and maximum lengths of time personal health information may be retained as well as procedures outlining how personal health information will be securely destroyed.	Y	Yes, as per OceanMD's privacy policy (https://www.oceanmd.com/privacy-policy), OceanMD has policies and procedures consistent with its obligations under PHIPA. Consent is generally implied consent at the discretion of the HIC (e.g., for tablets or referrals to other HICs), and Ocean prompts users to remind them of the need to collect consent where applicable (e.g., email consent). Requests to correct or access data by patients are redirected to the clinic because OceanMD does not have access to the PHI due to client-side encryption technology. Data retention policies can be found on the OceanMD support site, and a copy is attached as Exhibit 8.7.
A5. Are administrative, technical, and physical safeguards in place at the organization to protect personal health information against theft, loss, unauthorized use or disclosure and unauthorized copying, modification, or disposal pursuant to section 12 of PHIPA?	Y	See MNP Threat Risk Analysis.
A6. Is there an appointed privacy contact person in the organization?	Y	Dr. Doug Kavanagh, who can be reached at privacy.officer@oceanmd.com.
A7. Does a reporting process exist to ensure that the organization's management is informed of any privacy compliance issues?	Y	OceanMD has a Privacy Breach Management Policy, which is attached as Exhibit 8.1.

A8. Are senior executives actively involved in the development, implementation and/or promotion of your organization's privacy program?	Y	
A9. Are employees or agents with access to personal health information in your organization provided training related to privacy protection?	Y	Yes. Employees also sign an agreement as a condition of employment that confirms their PHIPA obligations. Employees must also complete an online privacy training module annually.
A10. Have policies and procedures been developed concerning the management of privacy breaches, including the notification of individuals when the confidentiality of their personal health information has been breached?	Y	See Exhibit 8.1.
B1. Has a summary of the proposed or existing information system, technology or program been prepared, including a description of the requirements for the system, technology or program and a description of how the information system, technology or program will or does meet those needs?	Y	
B2. Has a listing of all personal health information or data elements that will be or are collected, used, or disclosed in the proposed or existing information system, technology or program been prepared?	Y	See Exhibit 8.2.
B3. Have diagrams been prepared depicting the flow of personal health information in the proposed or existing information system, technology, or program	Y	See Exhibit 8.13 and Exhibit 8.14.
B4. Have documents been prepared showing which persons, positions, or employee categories will have access to which elements or records of personal health information	Y	Personal health information is not available to OceanMD personnel due to a combination of safeguards, such as the client-side encryption as documented in TRA. The decryption of this information requires the shared encryption key, which is not known to administrators. Access to the system is logged throughout. See Exhibit 8.3 for a list of all actions audited in Ocean. This can be used by the user site administrators to perform audit event reviews.
B5. Does consent from the individual or an authorized substitute decision-maker provide the primary basis for the collection, use and disclosure of personal health information for the proposed or existing information system, technology, or program?	Y	In general, patient consent is considered "implied" for most use cases, including Ocean tablets, with patients being able to opt-out through notification to the HIC. eReferrals to other HICs inherit the same "implied consent" requirement, and OceanMD has added "patient consent required" warnings to the product where applicable. For example, when sending referrals to health service providers that are not considered HICs under PHIPA, the referrer is reminded to obtain consent.
B6. Have you documented the purposes for which personal health information will be or is collected, used, or disclosed in	Y	See website Privacy Policy: https://www.oceanmd.com/privacy-policy

the information system, technology, or program?		
B7. Is personal health information collected, used, disclosed, or retained exclusively for the identified purposes and for purposes that an individual would reasonably consider consistent with those purposes?	Y	
B8. Will personal health information in the proposed or existing information system, technology or program be linked or cross referenced to other information in other information systems, technologies, or programs	Y	Yes, via the EMR ID and the referral reference, which is not personally identifying and meaningless without access to EMR. These are used to ensure that patient data can be linked for clinical purposes. The Provider Message / Health Report Manager feature does used the patient health insurance number to enable the recipient's EMR to identify the correct patient and deposit records in his chart
B9. Will personal health information collected or used in the information system, technology or program be disclosed to any persons who are not employees or agents of the responsible organization?	Y	For Patient Engagement technology (tablets, forms), patient data is restricted to the responsible organization. For eReferrals and eConsults, data may be disclosed to the intended recipient as directed by the referring HIC.
B10. Have you made arrangements to provide full disclosure of all purposes for which the information system, technology or program will collect personal health information?	Y	
B11. Have communications products and/or a communications plan been developed to fully explain the information system, technology, or program to individuals and how their personal health information will be protected	Y	This is done in two places: the Privacy Policy on the OceanMD website, as well as the OceanEReferralNetwork.ca site under the Patients tab.
B12. Does the proposed or existing information system, technology or program involve the collection, use or disclosure of any personal health information beyond Ontario's borders?	Y	Data is maintained within Canada and stored within our primary data centre in Montreal. The Ocean platform is available to all Canadian provinces and territories, which consequently requires the exchange of data that includes personal health information. The one exception is Ocean's SMS service provider, which is based in the United States of America. The only personal health information that will be passed to the SMS service provider is the patient's phone number. Privacy safeguards include: ● Ocean users can only use (a) 'canned' text message that does not contain any personal health information beyond the phone number used for the text message". ● Ocean users (as HICs) must 'opt in' to using text messages (it is not a default feature) ● Ocean users are instructed that patients must consent ('opt-in') to receiving text messages.

B13. Has an assessment been completed to identify potential risks to the privacy of individuals whose personal health information is collected, used, retained, or disclosed by the proposed or existing information system, technology, or program	Y	Open privacy risks are maintained in the Risk Register spreadsheet and reviewed at least monthly in a standing meeting.
B14. If potential risks to privacy have been identified, have means to avert or mitigate those risks been incorporated into the design and/or implementation of the proposed or existing information system, technology, or program	Y	See Exhibit 8.4.
B15. Has an assessment been completed to identify whether other health information custodians have implemented the same or a similar information system, technology or program, the risks to privacy experienced by other health information custodians and the means implemented by these other health information custodians to avert or mitigate these risks	Y	Our TRA confirms that Ocean meets industry-standard protections regarding privacy and security for Canadian health information technology, with numerous documented safeguards that avert or mitigate these risks. In addition, its "client-side encryption" architecture is beyond standard encryption models and provides a strong safeguard against breaches. See Exhibit 8.5 for recommendations for secure handling of the clinic encryption key.
B16. Have key stakeholders been provided with an opportunity to comment on the sufficiency of privacy protections and their implications on the proposed or existing information system, technology, or program?	Y	This privacy assessment has been reviewed by the System Coordinated Access program on behalf of the Ontario Ministry of Health and hundreds of HICs.
B17. Will users be trained in the requirements for protecting personal health information and will they be made aware of the relevant notification procedures if personal health information is stolen, lost, or accessed by unauthorized persons?	Y	The core users of Ocean are HIC clinicians, who have a pre-existing duty to be familiar with the standard notification procedures. In 2017, OceanMD and the SCA created an interactive "Privacy Primer" pop-up that is shown to all new users to introduce PHIPA and important obligations of users. As well, eReferral users must sign an appropriate HINP agreement which discusses these procedures
B18. Have security policies and procedures to protect personal health information against theft, loss, unauthorized use or disclosure and unauthorized copying, modification or disposal been documented?	Y	See Exhibit 8.6.
B19. Have privacy policies or procedures been developed for various aspects of the operations for the proposed or existing information system, technology, or program?	Y	See Exhibit 8.6.
B20. There is a record retention schedule for records of personal health information that outlines the minimum and maximum lengths of time personal health information may be retained in the proposed or existing information system, technology, or program, as well as procedures outlining the	Y	Documented on OceanMD Support site. See Exhibit 8.7.

manner by which personal health information in the proposed or existing information system, technology or program may be securely destroyed		
B21. Does the proposed or existing information system, technology or program provide functionality for the logging of the insertion, access, modification, or disclosure of personal health information as well as an interface to audit those logs for unauthorized activities?	Y	See Exhibit 8.3.
B22. Have policies and procedures been developed for the enforcement of privacy rules relating to the proposed or existing information system, technology, or program, including fulfilment of the commitments made in the PIA	Y	See Exhibit 8.8 for a summary of OceanMD's privacy policy as it relates to the Canadian Standards Association Model of Privacy Principles.

8 Exhibits

8.1 OceanMD Privacy Breach Management Policy

See OceanMD Privacy Breach Management Policy document.

8.2 What Personal Health Information is Stored in Ocean?

See https://cognisantmd.zendesk.com/hc/en-us/articles/360004387832

8.3 Audited Actions in Ocean

The support articles Guide for Reviewing Your Site's Audit Logs and Documentation for Ocean Audit Log Entries provides guidance to site administrators on how to download and interpret the audit log for their sites. Note that the list of audit events and descriptions is an ongoing work in progress. Contact OceanMD if you require additional information.

8.4 How do I protect the privacy of my site's shared encryption key?

See How do I protect the privacy of my site's shared encryption key?

8.5 Security Precautions and Privacy Controls Policy

See Security Precautions and Privacy Controls document. All OceanMD employees are required to view and acknowledge this document.

8.6 How long are patient records (with personal health information) kept in Ocean?

See How long are patient records (with personal health information) kept in Ocean?

8.7 Privacy Policy: How does OceanMD adhere to the 10 Privacy Principles of PHIPA?

See Privacy Policy: How does OceanMD adhere to the 10 Privacy Principles of PHIPA?

8.8 What is OceanMD's Role Under PHIPA?

See What is OceanMD's Role Under PHIPA?

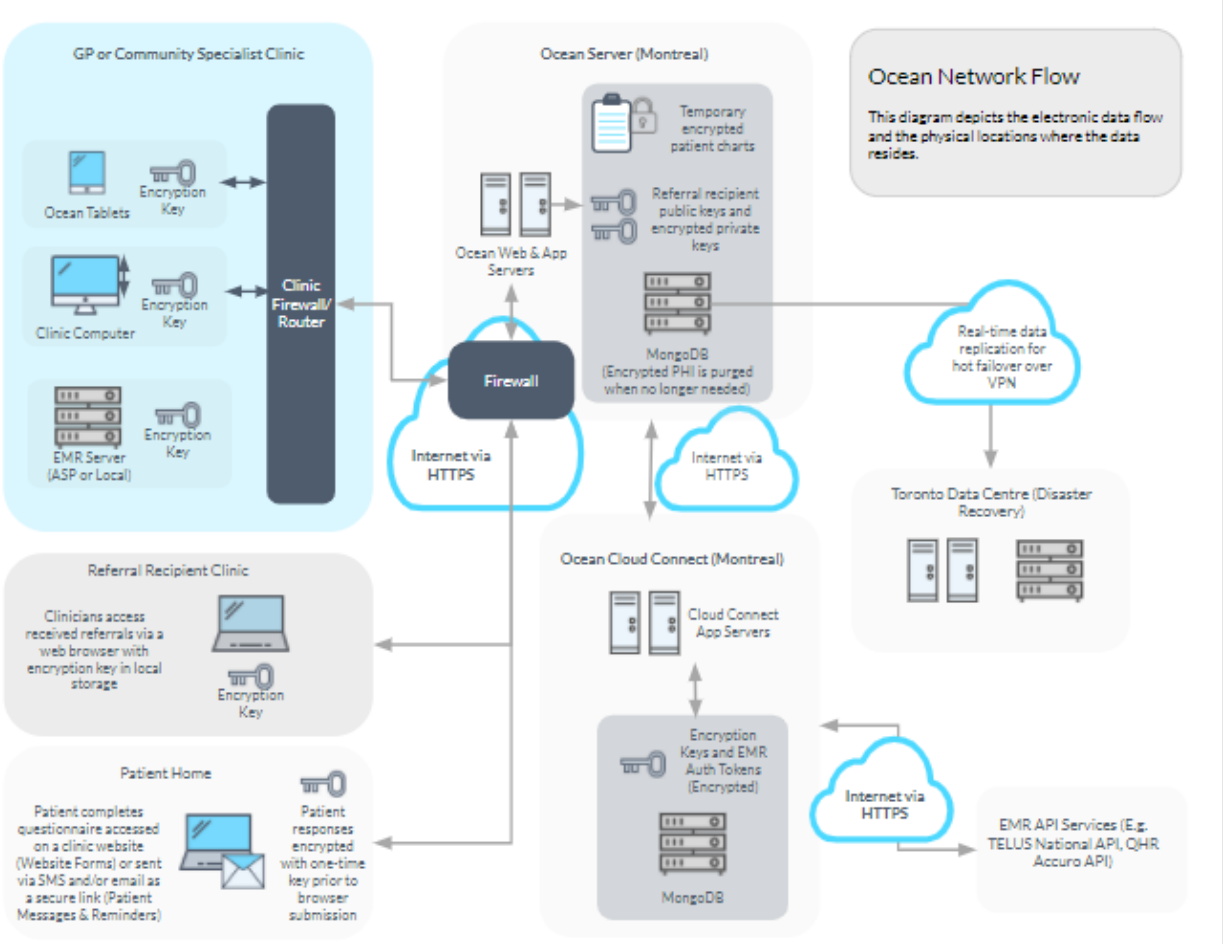
8.9 How does OceanMD validate health service directory listings as legitimate health information custodians (HICs)?

See How does OceanMD validate health service directory listings as legitimate health information custodians (HICs)?

8.10 How does OceanMD validate referrers as legitimate health service providers (HSPs)?

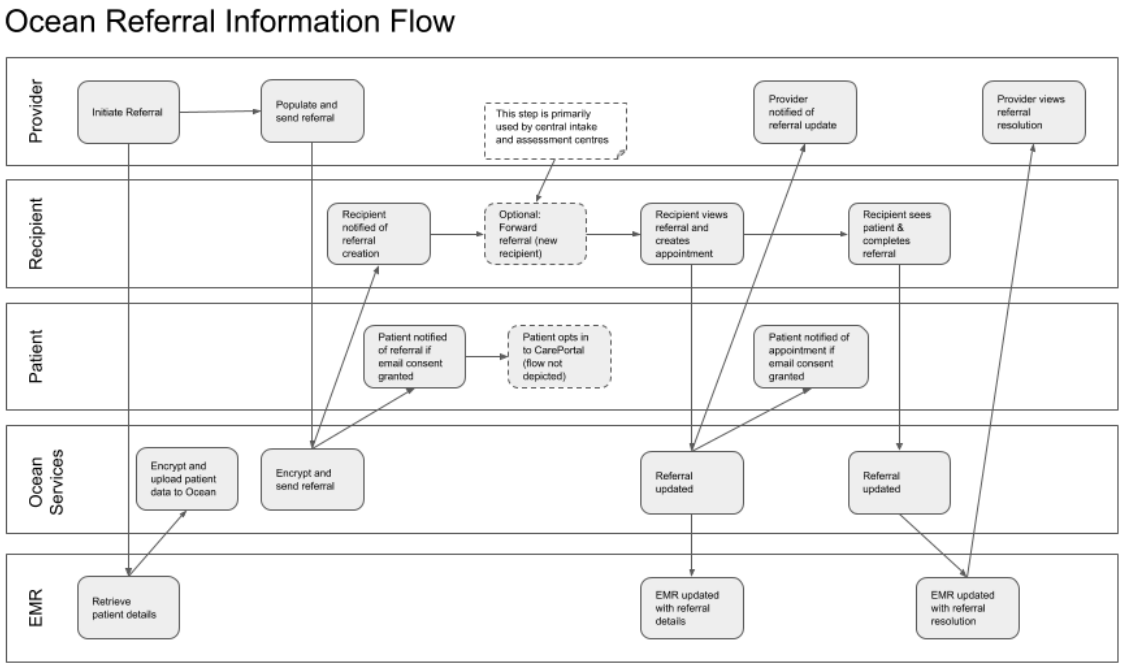
See How does OceanMD validate referrers as legitimate health service providers (HSPs)?

8.11 Ocean Network Flow Diagram



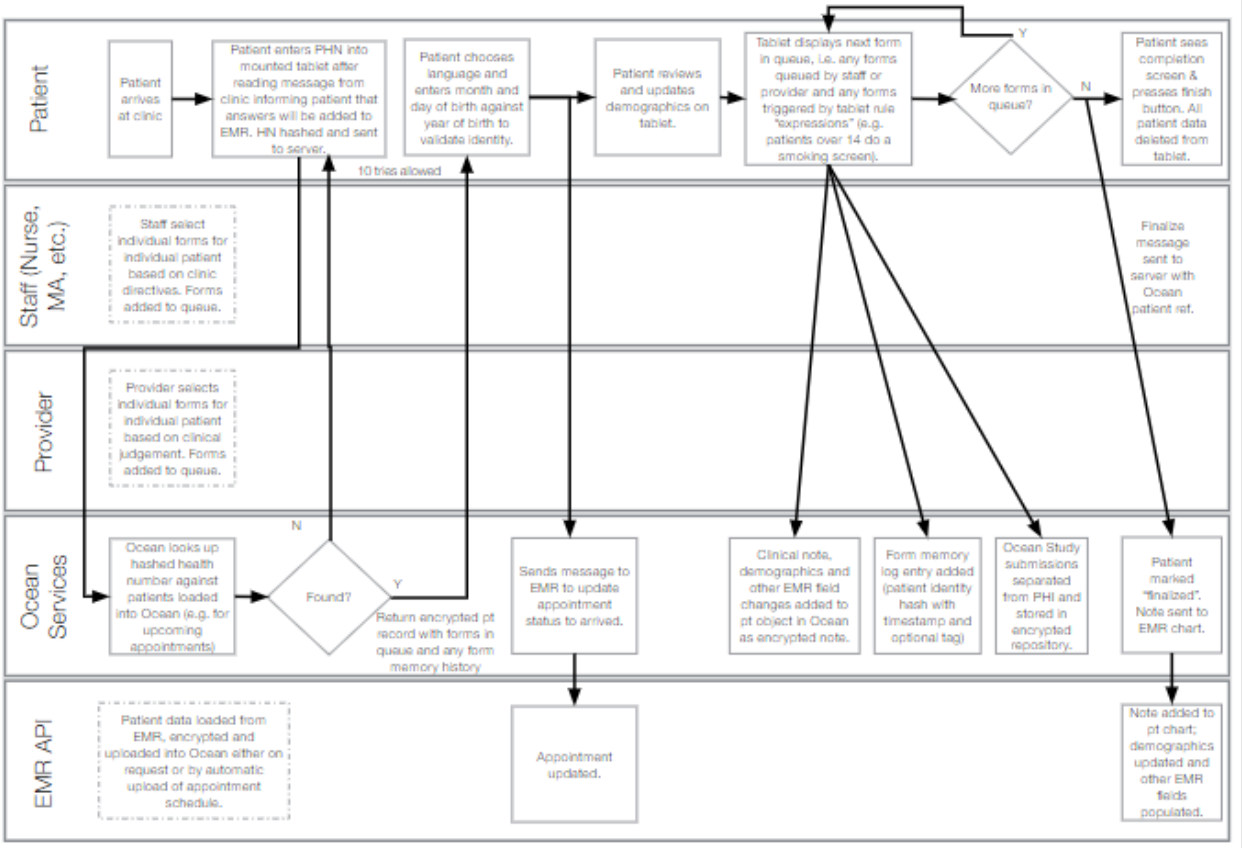
8.12 Ocean Referral Information Flow Diagram

The diagram below depicts information flow during the referral process. The Provider initiates a referral and sends to a Recipient. Optionally, the Recipient may forward the referral to additional Recipients, as in the central intake workflow. The Provider and Recipient are acting as HICs in this workflow. If the provider is not an HIC, this is noted in the provider's Ocean directory listing, which will warn the referrer to obtain explicit patient consent because the recipient is not an HIC.

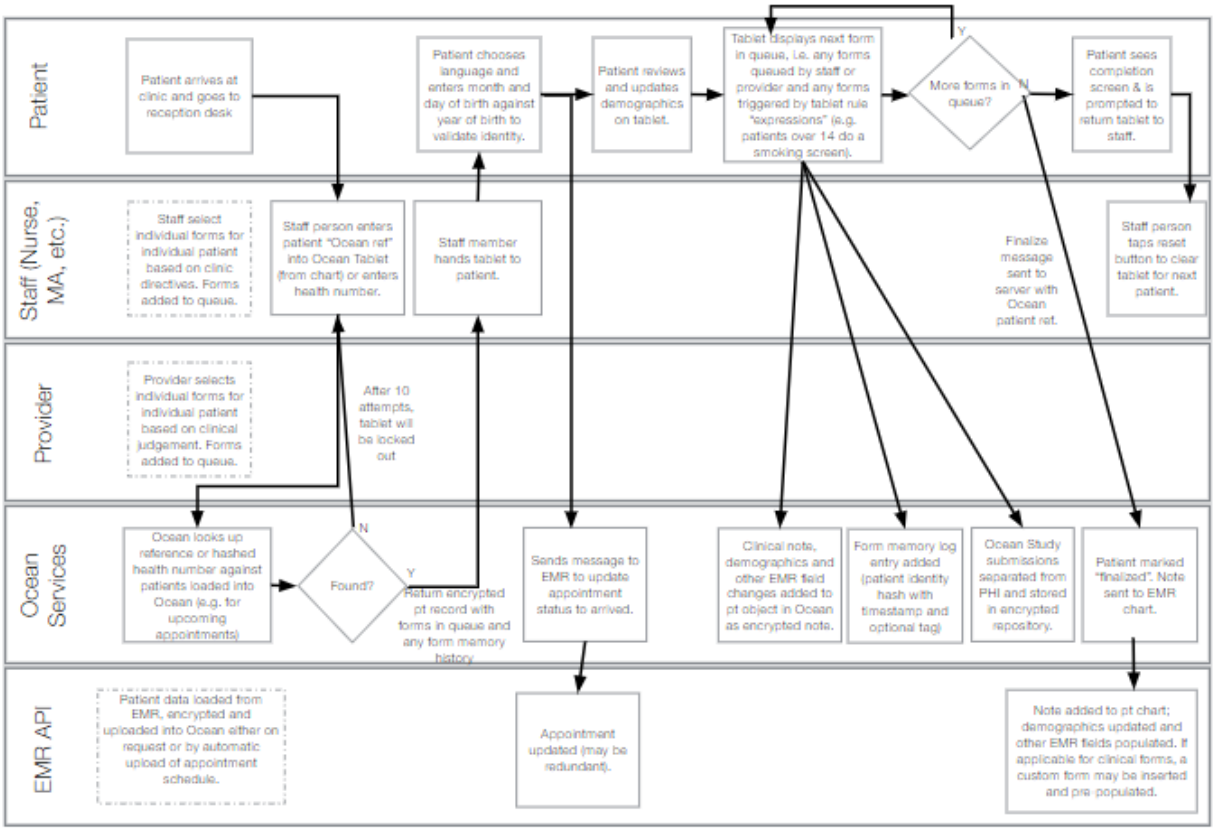


8.13 Ocean Information Flow Diagrams (non-referral)

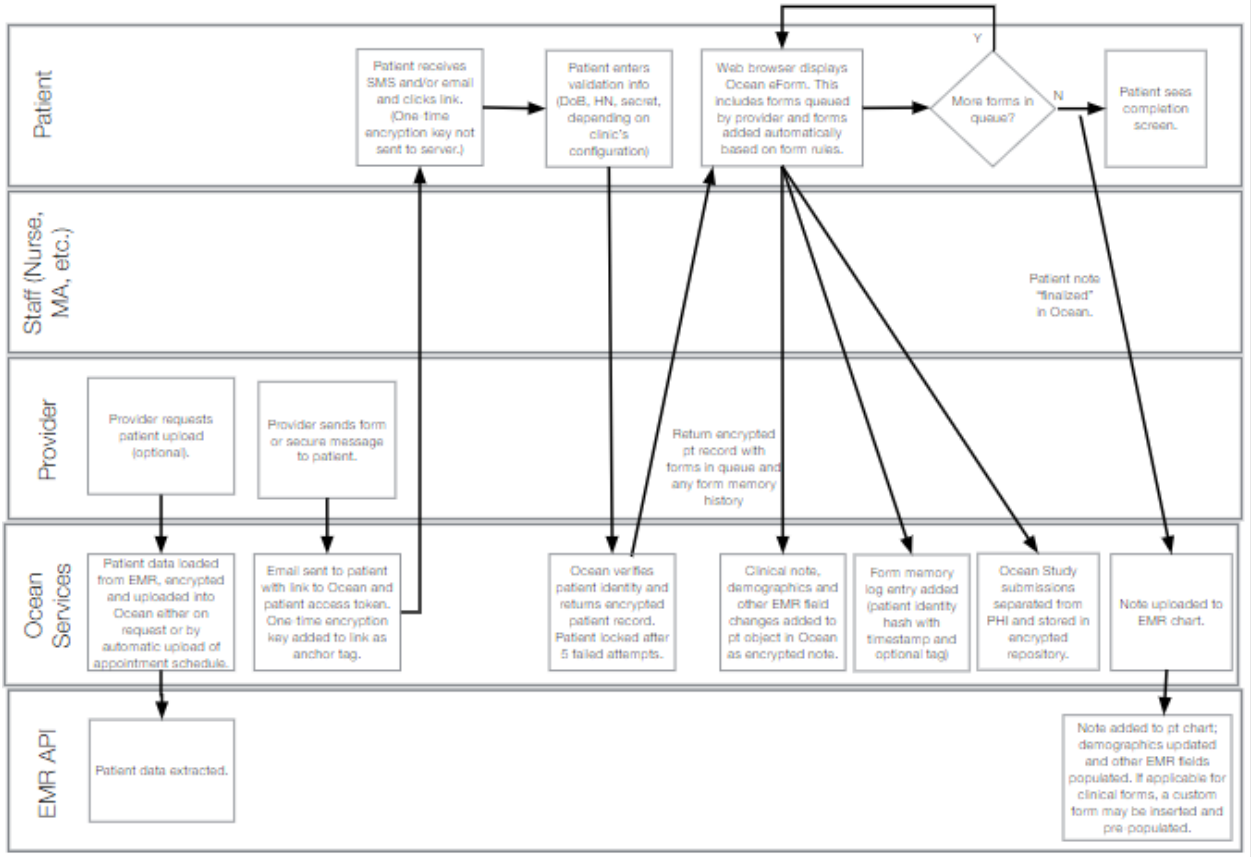
1. Ocean Tablet Flow (Kiosk Mode)



2. Ocean Tablet Flow (Staff-Initiated)



3. Ocean Patient Messages and Reminders Flow



4. Ocean Website Form Flow