CognisantMD Privacy Impact Assessment

Version 1.41

Apr 1, 2021

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.

Contents

1 Executive Summary

CognisantMD's Ocean platform is used by thousands of clinicians across Canada to improve patient engagement through waiting room tablets, kiosks and online clinical administration and data collection tools, as well as to refer patients between providers for care. Ocean includes products for patient messaging, reminders, online booking, secure website forms, anonymized studies, eReferrals, eConsults 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 CognisantMD's privacy practices. It covers how CognisantMD 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 purposes of patient engagement or eReferrals, either in the context of a region (e.g. a LHIN in Ontario) 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 (e.g. tablets) as well as eReferrals.

4 Out of Scope

This PIA does not include considerations relating to:

- EMRs
- 3rd party systems integrated with Ocean
- the Ocean Studies module

[1] The assessment has been updated in 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

CognisantMD operates as an Electronic Service Provider and, in some scenarios, as a Health Information Network Provider (HINP) under PHIPA. The following are the privacy principles to be assessed.

5.1.1 Electronic Service Provider

CognisantMD, 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

CognisantMD, via the Ocean platform, acts as a HINP when providing eReferral services. In some cases, HINP responsibilities are carried out by a third party, such as in the case of the Ontario eServices program.

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 only as long as 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 CognisantMD is a system that facilitates the sharing of data between patients and their healthcare providers ("Patient Engagement products") as well as between healthcare providers (e.g. "eReferrals, eConsults, Provider Messaging").

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 Messages & 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 eReferral and Provider Messaging module is used by referring clinicians ("Referrers" 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 direct message.

A primary feature of Ocean is the availability of modules that allow common electronic medical record systems (EMRs) used in many physician offices to interface with Ocean. Integration modules are currently available for EMRs including TELUS Practice Solutions, TELUS Med Access, QHR Accuro and OSCAR 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. For this reason, the Shared Encryption Key is not stored or logged on the Ocean server. It is not visible to CognisantMD system administrators. As a policy, CognisantMD employees will not request to see a client's shared encryption key.

For pragmatic reasons, individual clinics may nonetheless choose to store their encryption key privately on a separate Ocean Cloud Connect server. This storage is used mainly 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). CognisantMD uses dedicated access restriction protocols and specific safeguards in Cloud Connect to keep the shared encryption key private for clinics.

7 Privacy Analysis

7.1 Principles Analysis

7.1.1 Accountability

- CognisantMD has a publicly designated privacy officer to provide leadership on compliance with privacy accountability. Dr. Doug Kavanagh is the CognisantMD Privacy Officer. The Privacy Officer can be reached at privacy.officer@cognisantmd.com, or by phone at 1-888-864-8655 x701.
- All CognisantMD employees and representatives are provided with resources to learn the fundamentals of privacy and must sign a Privacy and Security agreement that describes their obligations under PHIPA. Employees must also successfully complete an online privacy training module annually.

7.1.2 Identifying Purposes

- CognisantMD / Ocean does not collect patient health information without providing a clear explanation of the intent in the system's user interface.
- Patient information is encrypted prior to transmission to Ocean using encryption keys known only to the relevant health information custodians and providers (the clinics).
- The personal health information required for the fulfillment of specific Ocean services (such as the sending of an eReferral) is used only for the service and nothing else.
- Where patient health information must be used directly by Ocean (such as the use of a patient's email for notification purposes, which results in an email address being stored in the Ocean audit event log), the system confirms with the health service provider that the patient has provided informed consent for the use of personal, unencrypted email for purpose of clinical notifications.

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 {text messages}) and recording it 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 communication sent to patients via a text message includes instructions on how to opt-out of text message delivery. CognisantMD 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

- CognisantMD / Ocean never collects personal health information beyond what is clearly 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 CognisantMD 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

- CognisantMD / 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 eReferral 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. CognisantMD 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, CognisantMD/Ocean is

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

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.

7.1.6 Accuracy

- The Ocean system interfaces with the healthcare practitioner's electronic medical record (EMR) system, 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 with regard to 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. "Check digit" tests are done 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 patient health information is inaccessible to third parties, including CognisantMD employees.
- 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).
- Industry-standard techniques such as 256-bit encryption, strong password policy management, two-factor authentication and user access restrictions are universally used within CognisantMD 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 eReferral 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 CognisantMD 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 the safeguards put in place to result in an overall "low" risk to personal health data.

7.1.8 Openness

- CognisantMD endeavours to publish its policies and procedures openly on our support portal, which is publicly available.
- CognisantMD 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. A summary of the TRA is available on our website.

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 CognisantMD / Ocean does not store unencrypted personal health information it is unable to provide patients with direct access to their personal health information. If a patient makes a personal health information request from Ocean, CognisantMD 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 electronic medical records systems 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.)
- CognisantMD 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

- CognisantMD'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.

[4] Because all PHI within Ocean is encrypted, CognisantMD 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.

- Health information network providers (HINPs) interacting with CognisantMD as an electronic service provider are encouraged to contact CognisantMD with any concerns as they arise.
- Individuals are also encouraged to contact CognisantMD'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

CognisantMD 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 Findings spreadsheet 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 Findings spreadsheet. 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

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 the manner by which personal health information will be securely destroyed.	Y	Yes, as per CognisantMD's privacy policy (https://www.cognisantmd.com/privacy-policy), CognisantMD 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 CognisantMD does not have access to the PHI due to client-side encryption technology. Data retention policies can be found on the CognisantMD 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@cognisantmd.com.
A7. Does a reporting process exist to ensure that the organization's management is informed of any privacy compliance issues?	Y	CognisantMD 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	Y	Yes. Employees also sign an agreement as a condition of employment that confirms their PHIPA

privacy protection?		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 CMD 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 CognisantMD 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 the information system, technology or program?	Y	See website Privacy Policy: https://www.cognisantmd.com/privacy-policy
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 CognisantMD 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 used (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 risks are maintained in the Privacy Risk Findings 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	The "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, CognisantMD 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 manner by which personal health information in the proposed or existing information system, technology or program may be securely destroyed	Y	Documented on CognisantMD Support site. See Exhibit 8.7.
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 CognisantMD's privacy policy as it relates to the Canadian Standards Association Model of Privacy Principles.

8 Exhibits

8.1 CognisantMD Privacy Breach Management Policy

See CMD 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. You can contact CognisantMD 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 Cognisant MD 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 CognisantMD adhere to the 10 Privacy Principles of PHIPA?

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

8.8 What is CognisantMD/Ocean's Role Under PHIPA?

See What is CognisantMD/Ocean's Role Under PHIPA?

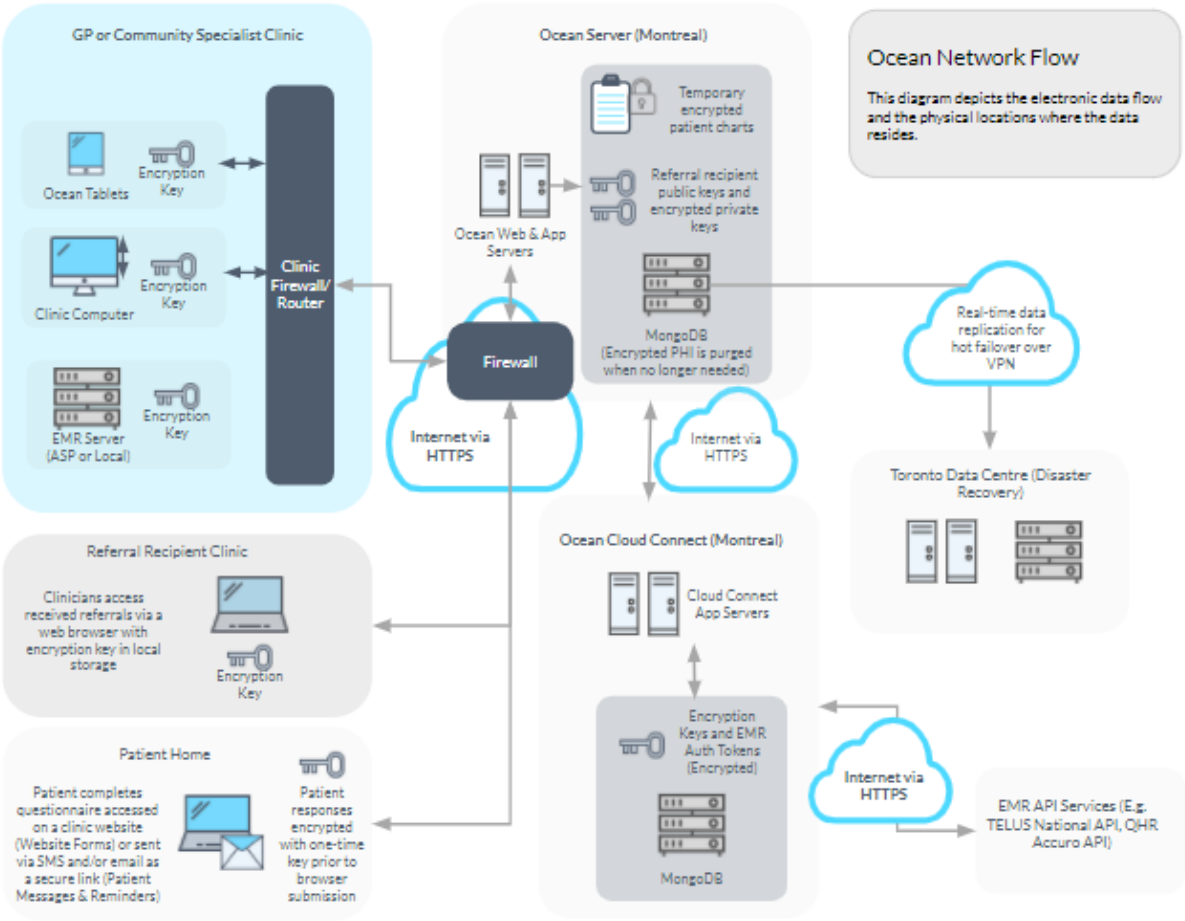
8.9 How does CognisantMD validate health service directory listings as legitimate health information custodians (HICs)?

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

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

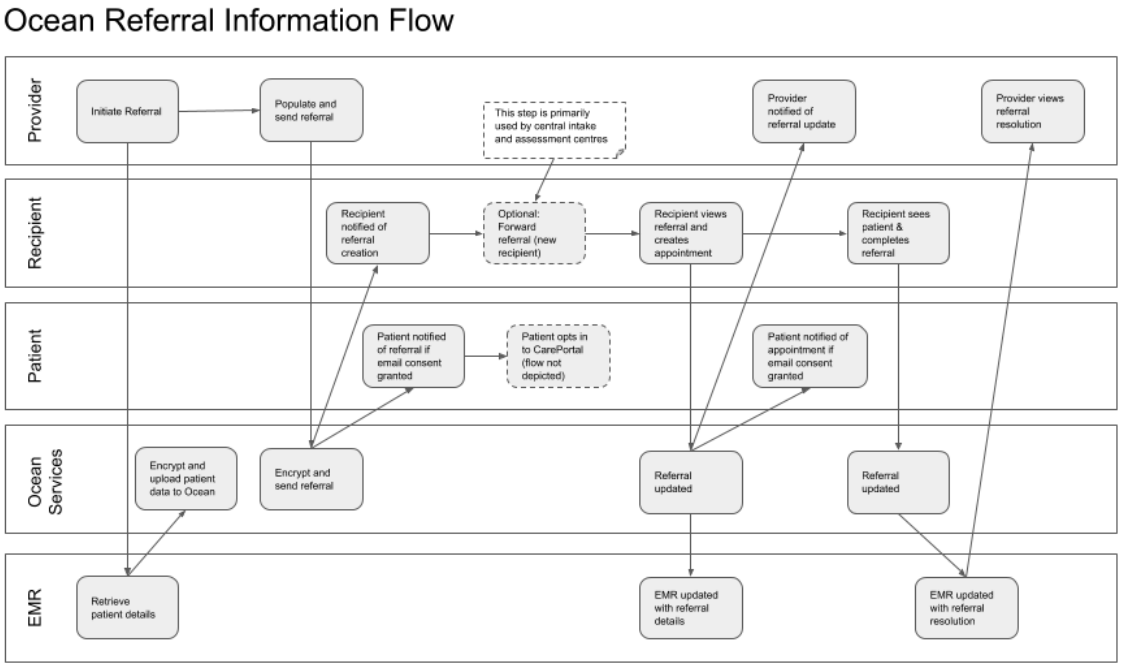
See How does CognisantMD validate referrers as legitimate health service providers (HSPs)?

8.11 Ocean Network Flow Diagram



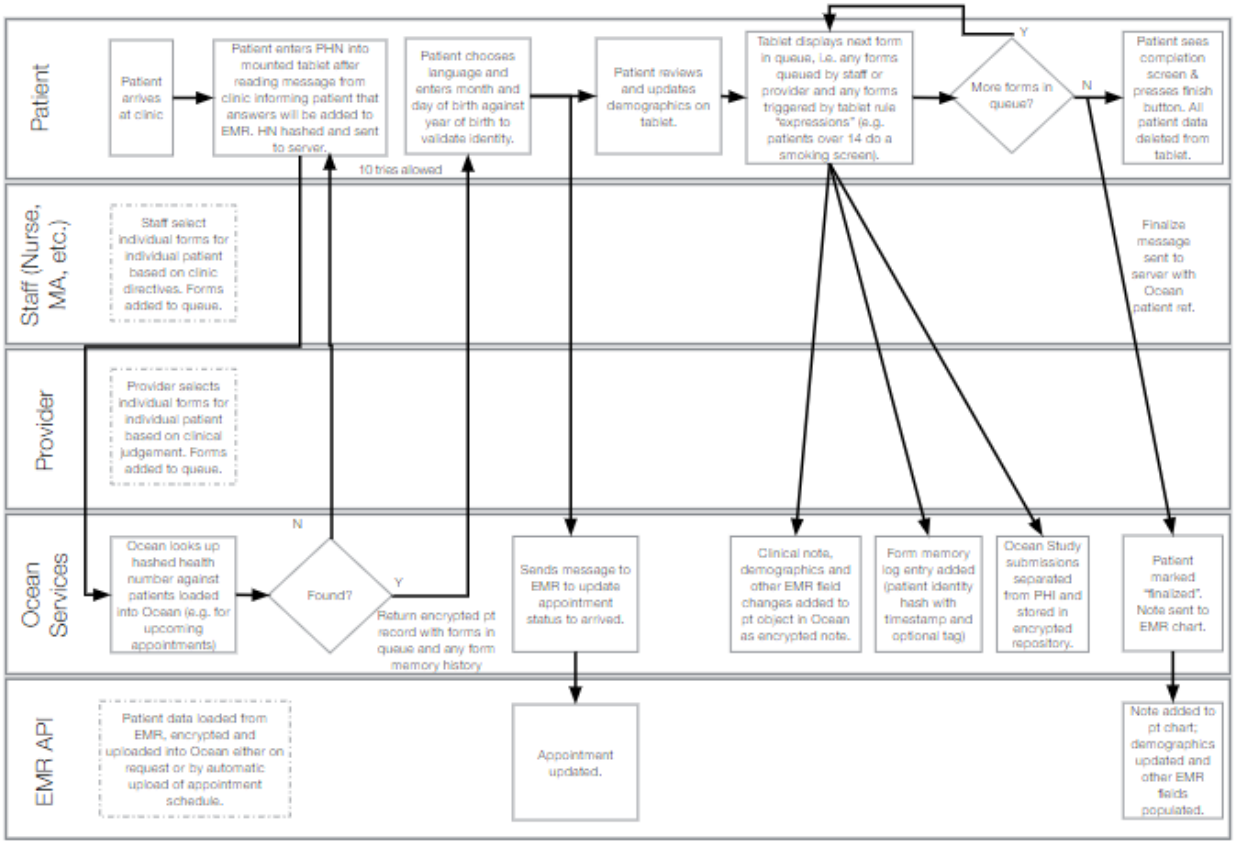
8.12 Ocean Referral Information Flow Diagram

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.

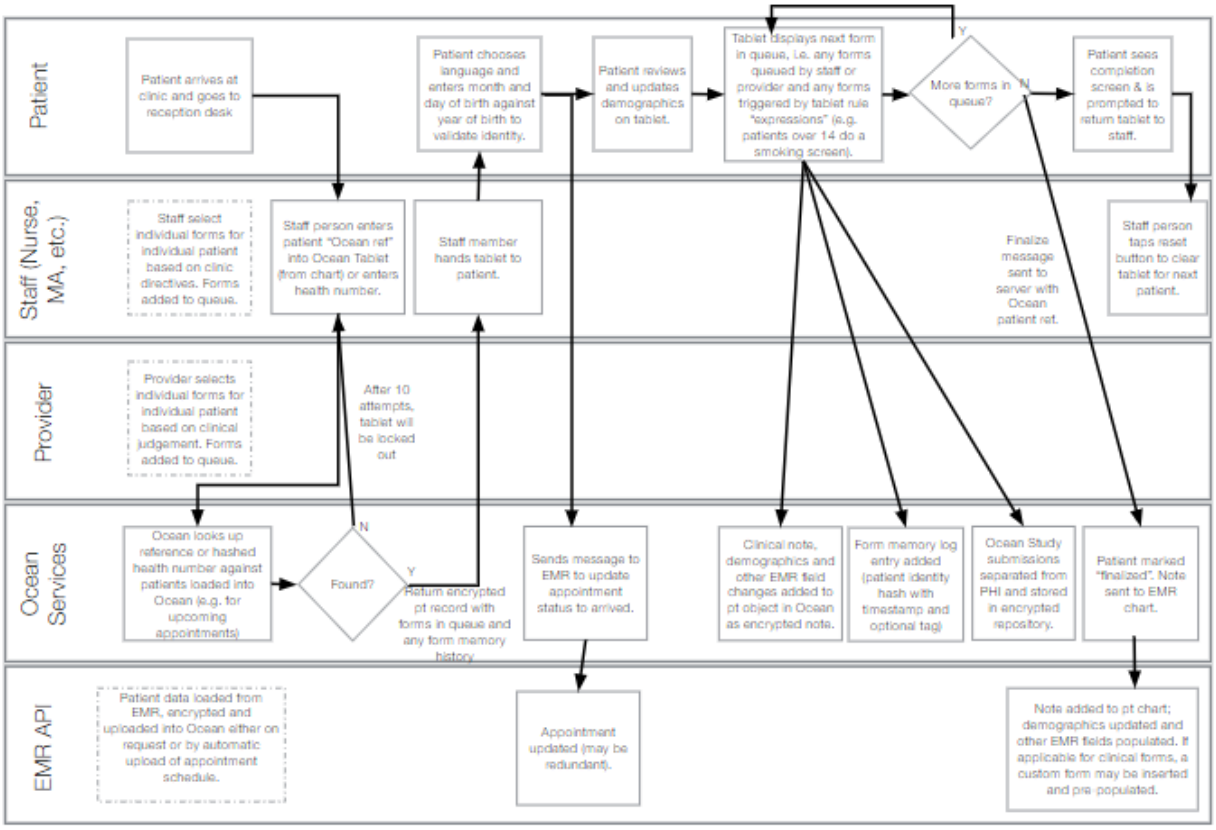


8.13 Ocean Information Flow Diagrams (non-referral)

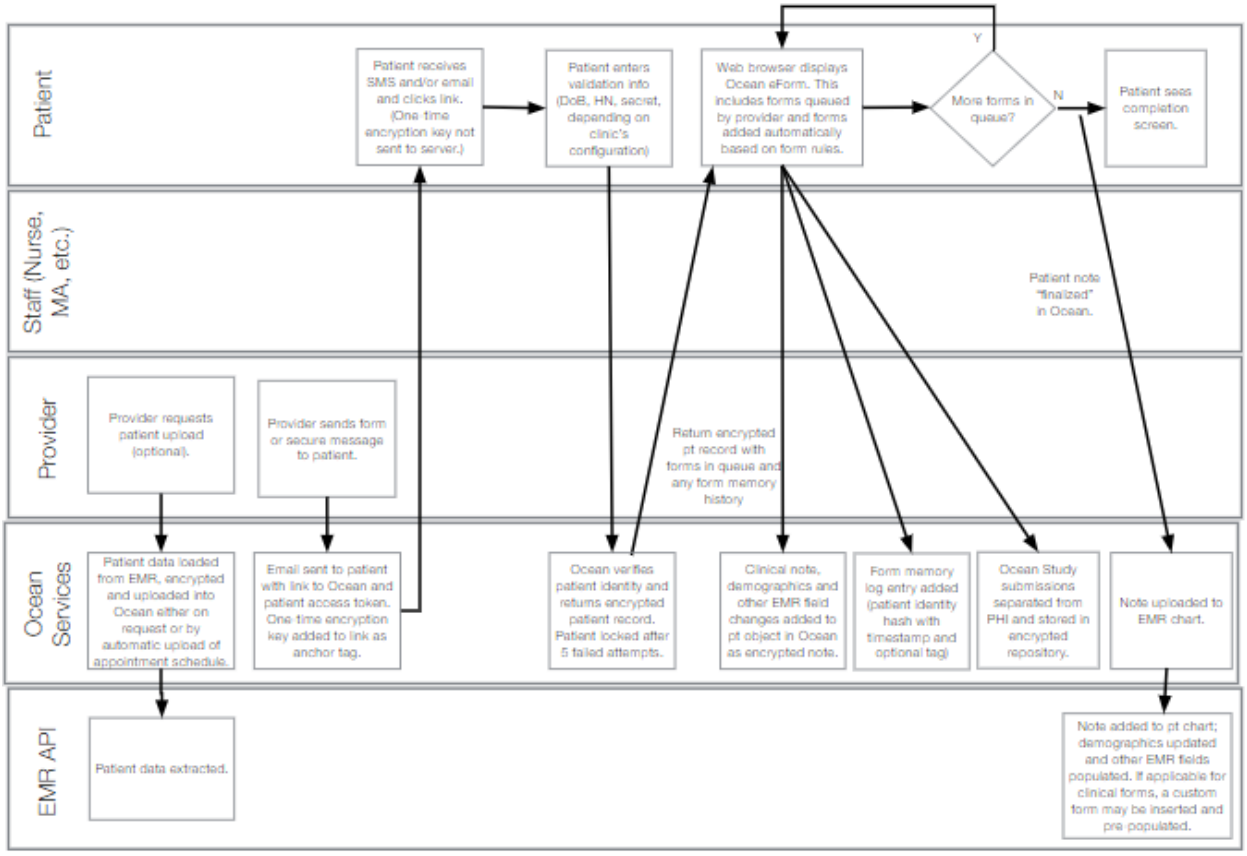
1. Ocean Tablet Flow (Kiosk Mode)



2. Ocean Tablet Flow (Staff-Initiated)



3. Ocean Patient Messages and Reminders Flow



4. Ocean Website Form Flow