PIA Executive Summary

Background

OceanMD is Canada's leading provider of integrated solutions designed to connect patients, providers, and healthcare systems. The OceanMD Platform is an EMR-integrated solution that provides tools to healthcare providers for improving patient engagement. The platform facilitates outbound communications between healthcare providers and patients with email, text, and web-based chat, while offering a system for patients to securely submit Personal Health Information (PHI) to their provider online. All PHI then syncs with the EMR for accurate recordkeeping. OceanMD itself does not directly interact with patients.

Disclaimer and Sign-off

This Privacy Impact Assessment (PIA) is current as of 2024-07-09. Any alterations or changes with respect to roles and responsibilities, agreements, data flows, processes and/or technology, related to OceanMD after this date may require the PIA to be revised to ensure it remains accurate and up to date. In some cases, a new PIA may be necessary.

This report is based on the information collected from OceanMD and Privacy Horizon Inc. believes this report to be accurate. Privacy Horizon Inc. is not responsible for inaccuracies or omissions associated with information collected.

The discussion of legal authorities and agreements contained in this document is in no way to be construed as a legal opinion.

PIA Methodology and Team

OceanMD has developed this PIA in conformance with generally recognized best practices for Privacy Impact Assessment. To assist with the research and analysis, OceanMD contracted with Privacy Horizon to provide skilled resources in privacy, security, and risk management.

The PIA methodology has been adapted from ISO/IEC 29134: Information technology – Security techniques – Guidelines for privacy impact assessment.

The OceanMD project team recognizes and acknowledges that the PIA is a dynamic “living” document that will be updated as required to reflect changing privacy risks and risk management strategies to mitigate those risks.

The following individuals were part of the OceanMD PIA team:

Individual	Position	Role
Victoria McIntosh, CIPT, (#000135489I)	Privacy Horizon Consultant	PIA Lead
Patrick Lo, CISSP, CIPP/C, (#000004871I)	Privacy Horizon Consultant	PIA SME
Ritesh Gawande	Director, Cloud Operations and Security, OceanMD	Sponsor
Gila Pyke	Director, GRC and Privacy, WELL Health	Sponsor

Table of Contents

The following is the original table of contents included within the original PIA.

Table of Contents

Report Objectives

This Privacy Impact Assessment (PIA) has been created to meet the following objectives:

- To demonstrate to stakeholders that the proper due diligence with respect to privacy has been conducted by OceanMD on its OceanMD platform.

- To identify privacy risks and to recommend strategies to manage those risks.

Scope

In scope

The scope of the PIA analysis includes the following:

- Personal health information is processed, stored, and transmitted via the OceanMD solution.
- OceanMD organizational privacy and security safeguards, where OceanMD personnel may have access to PHI to provide technical support of the OceanMD solution to healthcare practitioners.
- Privacy legislations within Canada, as they apply.

Out of scope

The following are out of scope of this PIA assessment:

- Other healthcare solutions and services that healthcare providers may use in addition to the OceanMD solution platform.
- Assessment of Health Information Custodian (HIC) privacy practices.
- Assessment of HIC EMRs.
- Privacy practices of OceanMD's parent company, WELL Health Technologies.[1]
- Privacy legislations outside of Canada.

[1] With the exception of when OceanMD has been confirmed to rely on WELL Health practices as part of privacy compliance. WELL Health practices integrated into OceanMD are discussed within this PIA.

Principle Findings

Privacy Observations

OceanMD retains personal information (PI) and personal health information (PHI)[2]. Provincial health privacy legislations apply to OceanMD, where Health Information Custodians (HICs)[3] use the OceanMD platform for the purpose of better patient communications and engagement to improve care. The Personal Information Protection and Electronic Documents Act (PIPEDA) will apply to OceanMD if another substantially similar legislation is not in force, such as the Personal Information Protection Act (PIPA) of British Columbia, and the Act Respecting the Protection of Personal Information in the Private Sector (ARPPIPS) in Quebec. However, it has been determined that the Personal Information Protection Act (PIPA) of Alberta will not apply, as PIPA does not apply to information covered under Alberta's Health Information Act and OceanMD will only be used for the provision of care.

As part of its solution, OceanMD has agreements with HICs, although some provinces will require additional contracts with specific written requirements. OceanMD's role will be a provider of services, an information manager, a health information network provider, or an agent, depending on the applicable health privacy legislation. All staff sign confidentiality agreements and security policies and have security training in place.

Security Observations

OceanMD is hosted on AWS, which provides physical and technical security safeguards. Additional safeguards that protect PHI in OceanMD include information security policies, data backups, and encryption of information in transit and at rest. Critically, where most patient PHI is encrypted and not visible to OceanMD administrators and support, OceanMD's platform offers strong protection against malicious insiders or inside attack should an internal account be compromised. A Threat/Risk Assessment was previously completed with no high risks identified. OceanMD maintains ISO 27001 certification and is currently undergoing a SOC 2 Type 2 compliance audit.

[2] To avoid confusion, this PIA uses PHI when referring to individual information processed by OceanMD, including personal information and personal health information, unless the discussion requires distinction.
[3] For simplicity, this PIA uses Health Information Custodians (HIC) when referring to healthcare provider customers of the OceanMD platform. HICs, also referred to in some privacy legislations as Custodians, are legal entities under Canadian Privacy Legislations who enforce compliance and are accountable under the law.

Application of Ontario Privacy and Analysis

For a list of the legislations reviewed in the full PIA, see Appendix A

Health Sector Privacy Legislation

Participating Organization	Role Under PHIPA	Accountable for Compliance with:
Physicians	Health Information Custodian	PHIPA: Part II – Practices to Protect PHI Part III – Consent Concerning PHI Part IV – Collection, Use and Disclosure of PHI Part V – Access to Records of PHI
OceanMD	Electronic Service Provider	Section 6(1) O.Reg. 329/04 – prescribed requirements
OceanMD	Health Information Network Provider	Section 6(3) O.Reg. 329/04 – prescribed requirements

Compliance with Ontario Personal Health Information Protection Act (PHIPA)

Section	Description	Compliance	Evidence/Comments
PHIPA			
10 (4)	**Providers to custodians**: A person who provides goods or services for the purpose of enabling a health information custodian to use electronic means to collect, use, modify, disclose, retain or dispose of personal health information shall comply with the prescribed requirements, if any.	Yes	• Per below, OceanMD complies with Provider requirements.
10.1 (1)	Subject to any prescribed exceptions, a health information custodian that uses electronic means to collect, use, disclose, modify, retain or dispose of personal health information shall, (a) maintain, or require the maintenance of, an electronic audit log described in subsection (4); (b) audit and monitor the electronic audit log as often as is required by the regulations; and	Yes	• OceanMD has event logs that capture the information as required. OceanMD's solution enables HIC to export reports for auditing and monitoring of logs.

	(c) comply with any requirements that may be prescribed. 2020, c. 5, Sched. 6, s. 3.		
10.1 (4)	The electronic audit log must include, for every instance in which a record or part of a record of personal health information that is accessible by electronic means is viewed, handled, modified or otherwise dealt with, a) the type of information that was viewed, handled, modified or otherwise dealt with; b) the date and time on which the information was viewed, handled, modified or otherwise dealt with; c) the identity of all persons who viewed, handled, modified or otherwise dealt with the personal health information; d) the identity of the individual to whom the personal health information relates; and e) any other information that may be prescribed. 2020, c. 5, Sched. 6, s. 3.	Yes	• OceanMD has event logs that capture the information as required. • OceanMD's solution enables HIC to export reports for auditing and monitoring of logs.
PHIPA Regulation 329/04			
6 (1)	**Persons who provide to custodians** Except as otherwise required by law, the following are prescribed as requirements for the purposes of subsection 10 (4) of the Act with respect to a person who supplies services for the purpose of enabling a health information custodian to use electronic means to collect, use, modify, disclose, retain or dispose of personal health information, and who is not an agent of the custodian: 1. The person shall not use any personal health information to which it has access in the course of providing the services for the health information	In Progress	• Confidentiality of information part of employee agreement and included in Code of Conduct for staff. • Limited access by OceanMD staff to PHI. • Internal Privacy Policy needed. See RM 1.

	custodian except as necessary in the course of providing the services. 2. The person shall not disclose any personal health information to which it has access in the course of providing the services for the health information custodian. 3. The person shall not permit its employees or any person acting on its behalf to be able to have access to the information unless the employee or person acting on its behalf agrees to comply with the restrictions that apply to the person who is subject to this subsection. O. Reg. 329/04, s. 6 (1).		
6 (2)	The provider shall provide to each applicable health information custodian a plain language description of the services that the provider provides to the custodians, that is appropriate for sharing with the individuals to whom the personal health information relates, including a general description of the safeguards in place to protect against unauthorized use and disclosure, and to protect the integrity of the information.	Yes	• Corporate Policy / Privacy Notice on website.
6 (3)	The provider shall make available to the public, i. the description referred to in paragraph 2, ii. any directives, guidelines and policies of the provider that apply to the services that the provider provides to the health information custodians to the extent that these do not reveal a trade secret or confidential scientific, technical, commercial or labour relations information, and iii. a general description of the safeguards implemented by the person in relation to the security and confidentiality of the information.	Yes	• Corporate Policy / Privacy Notice on website.

6 (4)	The provider shall to the extent reasonably practical, and in a manner that is reasonably practical, keep and make available to each applicable health information custodian, on the request of the custodian, an electronic record of, i. all accesses to all or part of the personal health information associated with the custodian being held in equipment controlled by the provider, which record shall identify the person who accessed the information and the date and time of the access, and ii. all transfers of all or part of the information associated with the custodian by means of equipment controlled by the provider, which record shall identify the person who transferred the information and the person or address to whom it was sent, and the date and time it was sent.	Yes	• OceanMD has event logs that capture the information as required. • OceanMD's solution enables HIC to export reports for auditing and monitoring of logs.
6 (5)	The provider shall perform, and provide to each applicable health information custodian a written copy of the results of, an assessment of the services provided to the health information custodians, with respect to, i. threats, vulnerabilities and risks to the security and integrity of the personal health information, and ii. how the services may affect the privacy of the individuals who are the subject of the information.	Yes	• Privacy Impact Assessment completed. Includes compliance with legislation. • Threat/Risk Assessment completed.
6 (7)	The provider shall enter into a written agreement with each health information custodian concerning the services provided to the custodian that, i. describes the services that the provider is required to provide for the custodian, ii. describes the administrative, technical and physical safeguards	TBC if onboarding PHI regulated by PHIPA and acting as a HINP	• Specific contract needed if providing services to HIC in Ontario when acting as a HINP. See RM 4.

	relating to the confidentiality and security of the information, and iii. requires the provider to comply with the Act and the regulations. O. Reg. 329/04, s. 6 (3).		

Privacy Principle Analysis

The table below demonstrates compliance with the 10 principles of the CSA model code for the protection of personal information, which is attached as a schedule to the Personal Information Protection and Electronic Documents Act (PIPEDA).

#	Privacy Principle	Description	Comments	Compliance
1	Accountability	An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles.	• Privacy Officer in place. • Security policies in place. • Agreements with HIC • Agreements with vendors in place. • Confidentiality part of employee agreement. • Staff training in place. • Third-party review. • Workforce security controls. • Additional policies needed. See RM 1	In Progress
2	Identifying Purposes	The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.	• Data element inventory part of PIA. • Purpose for health information collection determined by the HIC.	Yes
3	Consent	The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except when inappropriate.	• Patient consent is the responsibility of the HIC.	Yes

#	Privacy Principle	Description	Comments	Compliance
4	Limiting Collection	The collection of personal 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.	• Information collected for the purpose of contacting patient. • Health information collection determined by the HIC.	Yes
5	Limiting, Use Disclosure and Retention	Personal 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 information shall be retained only as long as necessary for the fulfillment of those purposes.	• Data Retention Policy in place. • Responsible Disclosure Policy in place. • See RM 1 (Privacy policy, acceptable use of PHI) • Limited staff access to PHI. • Data disposal and media sanitization.	Yes
6	Accuracy	Personal information shall be as accurate, complete and up-to-date as is necessary for the purposes for which it is to be used.	• PHI syncs with EMR. • Amending information is the responsibility of HIC. • Encryption of data. • Antivirus to detect unauthorized modification.	Yes
7	Safeguards	Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.	• Administrative, technical, physical controls in place. • Access controls. • Anti-malware and patching. • Authentication. • Backups. • Encryption in transit. Encryption at rest for sensitive data. • Risk assessments. • Event logging and monitoring. • Secure AWS data center. • Vulnerability testing.	In Progress

#	Privacy Principle	Description	Comments	Compliance
			• ISO 27001 certification in place and SOC 2 Type 2 Audit in progress. • Threat/ Risk Assessment completed. See RM 2.	
8	Openness	An organization shall make readily available to individuals' specific information about its policies and practices relating to the management of personal information.	• Privacy Notice for patients is the responsibility of HIC. • Corporate Policy / Privacy Notice on website.	Yes
9	Individual Access	Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal 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.	• Individual access requests the responsibility of HIC. • Access requests must be sent to / individual differed to the HIC, per contracts.	Yes
10	Challenging Compliance	An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization's compliance.	• Privacy complaints and challenges are processed as they come in. The Corporate Privacy Policy/ Privacy Notice proves the contact privacy.officer@oceanmd.com. • Additional policy needed for BC, Quebec. See RM 1.	In Progress

Privacy Risks

OceanMD Risk Map

R1. Unauthorized use or disclosure by internal agent (non-malicious)

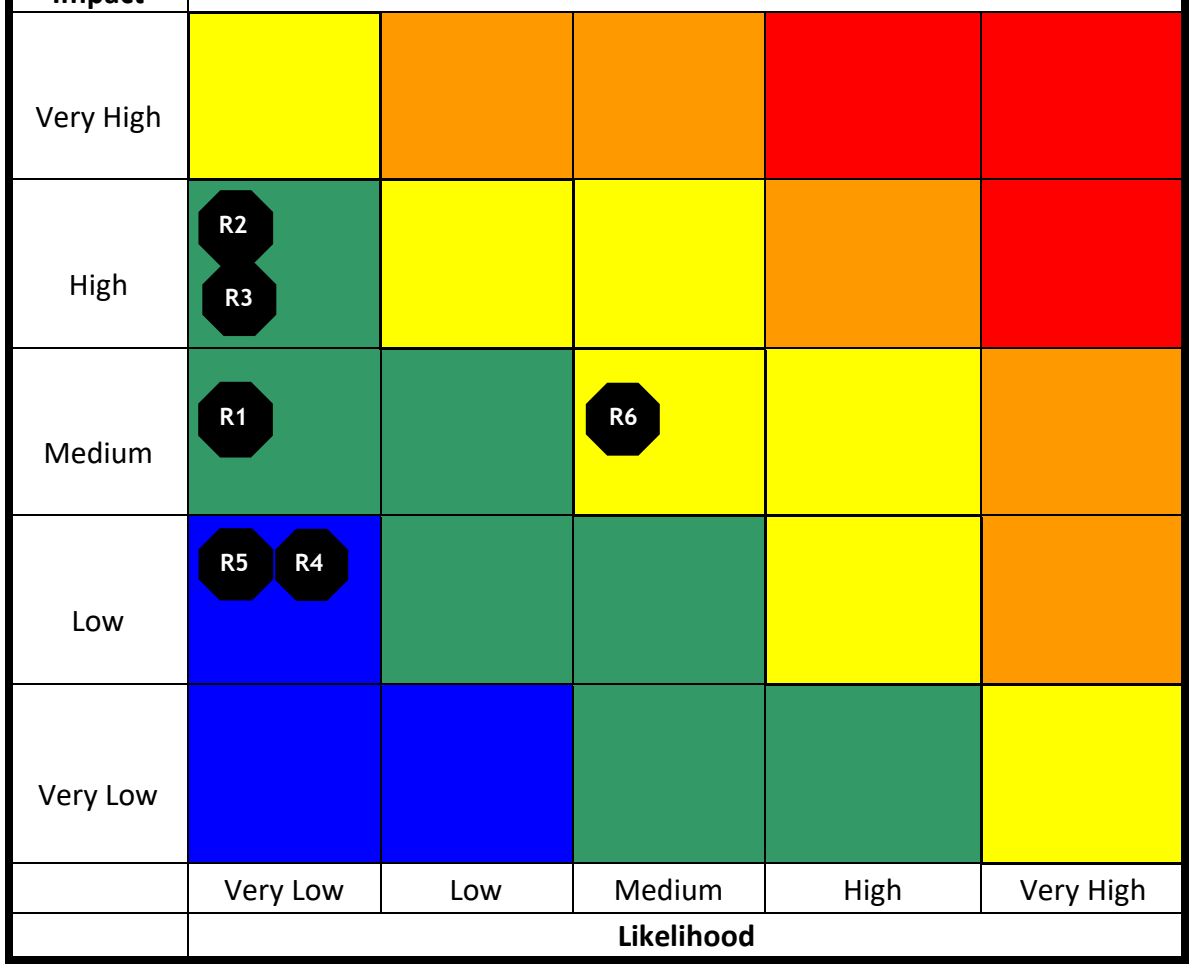
R2. Unauthorized use or disclosure by internal agent (malicious)

R3. Attack by external malicious agent

R4. Improper disposal of media

R5. Accidental corruption of PHI

R6. Denial of Patient Rights



Recommendations

After analysis, the following recommendations are made:

RM 1 - Include Privacy in Policies

OceanMD has a number of security policies in place, but no policy that addresses Canadian privacy. However, while OceanMD has limited access to PHI as platform restricts OceanMD administration from having access to patient data, from discussions with the OceanMD team there are exceptions, and this is not always the case when processing information for each HIC client. The 10 Fair Information Principles while public on OceanMD's website, is not an internal privacy policy as it has not been implemented with staff.

To improve privacy compliance, it is advised OceanMD add the following:

- Develop and implement internal privacy policy for all staff.
- Updates to the Data Retention Policy are required for: Manitoba, Quebec, and Saskatchewan. Updates should include specifications on how data is destroyed, and that data will be anonymized to provincial standards, if applicable.
- A policy on how privacy complaints are processed is required for compliance with BC's PIPA and Quebec's ARPPIPS.
- For OceanMD's Data Classification Policy, the policy and terminology are based off the EU GDPR and California's CCPA. Updates that the policy will also comply with Canadian PHI is advised.
- If OceanMD ever decides to use AI tools, information on the tool's decision-making capability will need to be included in OceanMD's existing asset inventory.
- Minor updates to the Incident Response Plan are advised if OceanMD is sold to Alberta or Quebec HIC. Communications in the event of a breach will comply with the Alberta's requirements, and Quebec has specific information that must be included in Incident Reports.

RM 2 - Implementation of mitigating solutions to address risks identified in the TRA

A Threat/Risk Assessment (TRA) was completed in 2024 on the OceanMD Platform. The TRA takes a more technical review of the solution against malicious attackers, both outside the organization and within. As of June 2024, mitigation of TRA risks is still in progress. It is strongly recommended that OceanMD mitigate and, where possible, remove risks identified by the TRA.

RM 3 - Additional requirements for Quebec

A requirement of Quebec's new privacy legislations, including the Act Respecting Access to Documents Held by Public Bodies and the Protection of Personal Information, and the Act Respecting Protection of Personal Information in the Private Sector (commonly known as Law 25), is the ability to communicate information in structured, commonly used technological

format. Currently OceanMD's platform cannot export patient data. OceanMD will need to insert functionality that allows for the export of patient data with its solution for the platform to be in compliance.

Specific training will be required if providing OceanMD to HIC in Quebec, where regulations require completed training on the legislation's requirements with respect to the protection of information.

It is also recommended OceanMD monitor developments in the healthcare sector and discuss client requirements when providing the solution to HIC in Quebec. Per Quebec's Act Respecting Health and Social Service Information (ARHSSI)[4], (Section 92), additional certifications and rules may be required as determined by the Deputy Minister of the Ministère de la Cybersécurité et du Numérique and future regulations.

RM 4 - Amend Agreements to Meet Future Customer Provincial Requirements

OceanMD will need specific agreements to be in compliance with provincial Canadian privacy laws if offering its patient communications platform in different provincial jurisdictions. Contractual requirements as written and required by applicable legislation are included in this PIA. See the Legislation Analysis Tables under Appendix C for details.

[4] Quebec's Act Respecting Health and Social Service Information received royal assent on April 4, 2023; regulations come into force July 2024.

Mitigation Plan

Risk	Risk Level	Recommendation	Status	Timeline
R1 - Unauthorized use or disclosure of PI or PHI by internal agent (non-malicious)	VL	RM 1 - Include Privacy in Policies		
R3 - Attack by external malicious agent	L	RM 2 Implementation of mitigating solutions to address risks identified in the TRA		
R6 - Denial of patient rights (PIA Only)	M	RM 1 - Include Privacy in Policies		
		RM 3 - Additional requirements for Quebec		
		RM 4 - Amend Agreements to Meet Future Customer Provincial Requirements		

Sign-Off

Ritesh Suresh Gawande

Ritesh Suresh Gawande

Director, Cloud Operations and Security

10th July 2024

Date

Appendix A: PIA Legislation Analysis List

The following legislations have been assessed in the completed PIA. See PIA: Appendix C – Legislation Analysis for full details.

Province	Legislation
Alberta	Information and Protection of Privacy Act[5]
Alberta	Health Information Act
British Columbia	Freedom of Information and Protection of Privacy Act
British Columbia	Personal Information Protection Act
Manitoba	Freedom of Information and Protection of Privacy Amendment Act
Manitoba	Personal Health Information Act
New Brunswick	Personal Health Information Privacy and Access Act
New Brunswick	Right to Information and Protection of Privacy Act
Newfound-land and Labrador	Access to Information and Protection of Privacy Act
Newfound-land and Labrador	Personal Health Information Act
Northwest Territories	Access to Information and Protection of Privacy Act
Northwest Territories	Health Information Act
Nova Scotia	Freedom of Information and Protection of Privacy Act
Nova Scotia	Personal Health Information Act
Nova Scotia	Personal Information International Disclosure Protection Act
Nunavut	Access to Information and Protection of Privacy Act
Ontario	Freedom of Information and Protection of Privacy Act

[5] Public sector legislations are included herein where OceanMD has clients who receive public sector funding and require OceanMD to comply with public sector privacy legislations as part of their funding agreements.

Ontario	Personal Health Information Protection Act
Prince Edward Island	Freedom of Information and Protection of Privacy Act
Prince Edward Island	Health Information Act
Quebec	Respecting Access to Documents Held by Public Bodies and the Protection of Personal Information
Quebec	Act Protection of Personal Information in the Private Sector
Quebec	Act Respecting Health and Social Service Information
Quebec	Act Respecting the Sharing of Certain Health Information[6]
Saskatchewan	Freedom of Information and Protection of Privacy Act
Saskatchewan	Health Information Protection Act
Yukon Territory	Access to Information and Protection of Privacy Act
Yukon Territory	Health Information Privacy and Management Act

[6] Act is set to be replaced by *Act Respecting Health and Social Service Information (ARHSSI)*.

Appendix B: Third-Party Agreements

Agreements with the following third parties have been assessed in the completed PIA, where they may collect, process, or retain PHI on OceanMD's behalf.

- *Amazon Web Services (AWS).* Cloud hosting;
- *Twilio.* Used for SMS messaging and Voice over Internet (VoIP) phone calls and video.