Dialogue

Internal Privacy Policy

Version: 2
Date of last revision: August 1, 2024
Effective Date: August 1, 2024

CONFIDENTIAL

1. Objective

1.1 Dialogue is committed to Processing Personal Information in accordance with its policies and practices relating to the protection of Personal Information and relevant Applicable Privacy Legislation. This is a team effort that requires the full cooperation of all Dialogue Agents and involves using appropriate processes and technologies to ensure the appropriate Processing and protection of Personal Information throughout the information lifecycle, in accordance with Dialogue's policies and procedures.

1.2 This Internal Privacy Policy is relevant for any Dialogue Agent responsible for, or otherwise involved in the Processing of Personal Information in the custody or under the control of Dialogue. This includes Personal Information about Members, Dialogue Agents or suppliers of Dialogue in Canada as well as any Personal Information Processed on behalf of Dialogue's corporate clients, if applicable.

1.3 This Internal Privacy Policy explains how Dialogue Agents are required to Process Personal Information so as to ensure that Dialogue complies with legal and contractual requirements concerning the Processing of Personal Information. In particular, this Internal Privacy Policy sets out standard requirements for Processing Personal Information and applies to all Processing Activities or operations carried out for or on behalf of Dialogue. This Internal Privacy Policy may be supplemented or superseded from time to time by any specific and valid procedures governing a given Processing activity or operation.

2. Definitions

2.1 Refer to Appendix A of this Internal Privacy Policy for the Glossary of Terms

3. Roles and Responsibilities

3.1 The Privacy Officer is responsible for the implementation and revision of the Internal Privacy Policy.

3.2 Dialogue Agents are required to read and adhere to this Internal Privacy Policy, and to Process Personal Information in accordance with this Internal Privacy Policy.

3.3 Dialogue executives are responsible for the compliance with this Internal Privacy Policy within their respective business units.

4. Scope

4.1 This Internal Privacy Policy applies to Dialogue's Personal Information Processing practices, including with respect to the Processing of Personal Health Information. Where a specific requirement only applies to the Processing of Personal Health Information, such requirement will expressly refer to Personal Health Information. Dialogue Processes Personal Information in two ways:

4.1.1 **Dialogue acting as an Information Manager:** In some cases, Dialogue Processes Personal Health Information in its capacity as an Information Manager (sometimes also referred to as an "agent" under Provincial Health Privacy Legislation). It does so on behalf of Health Service Providers who are accountable for the Personal Health Information (sometimes referred to as "**Custodians**" or "**trustees**" under Provincial Health Privacy Legislation). Please review Part 5.1 – How Dialogue Processes Personal Health Information as an Information Manager of this Internal Privacy Policy for specific information about this. Part 5.2 also details the relevant processes and safeguards applicable to all Processing by Dialogue and its Custodians.

4.1.2 **Dialogue acting in its own capacity:** Dialogue Processes Personal Information, including Personal Health Information, in its own capacity (including, for example, to provide Clinical Services in jurisdictions where Dialogue is considered a Custodian, for non-Clinical Services, to comply with Dialogue's legal obligations, and to manage Dialogue Agents). In those circumstances, Dialogue does so as the entity accountable for the Personal Information (or as Custodian of Personal Health Information in applicable jurisdictions). Please review Part 5.2 – How Dialogue Processes Personal Information Acting in its Own Capacity of this Internal Privacy Policy for more information.

4.2 This Internal Privacy Policy also establishes some general policies and procedures that relate to privacy matters, including retention/disposal of Personal Information, use of third-party Service Providers, cross-border transfers of Personal Information, PIAs, information security, breaches of security safeguards, breaches of this Internal Privacy Policy, training/awareness, who to contact to make a complaint/report a violation and who to contact with questions.

5. DETAILS

5.1 How Dialogue Processes Personal Health Information as a Information Manager

5.1.1 Application of this Part 5.1

5.1.1.1 This Part 5.1 applies in jurisdictions where Dialogue is not considered a Custodian under Provincial Health Privacy Legislation and whereby Dialogue Processes Personal Health Information in its capacity as a Information Manager of Health Services Provider that provides Clinical Services using the Virtual Care App. For example, Dialogue might Process Personal Information on behalf of a registered psychologist who meets with Members using the Virtual Care App to assist the psychologist to manage Member appointments and maintain Member records.

5.1.1.2 As another example, in the province of Alberta, Dialogue may Process Personal Health Information on behalf of a nurse in connection with the nurse meeting with a Member to discuss the Member's health concern.

5.1.1.3 In those circumstances, Dialogue is not the accountable entity for the Personal Health Information that Dialogue Processes on behalf of a Health Services Provider that are Custodians of Personal Health Information, which means that Dialogue does not determine what Personal Health Information to collect on behalf of a Custodians or how the Personal Health Information is used, disclosed or retained by or on behalf of the Custodians.

5.1.1.4 In those circumstances, Dialogue will assist Health Services Provider that are Custodians of Personal Health Information with their compliance with applicable Provincial Health Privacy Legislation, including by assisting the Custodians :

(a) collect only the information necessary to deliver Clinical Services;

(b) appropriately safeguard Personal Health Information;

(c) respond to requests for access to or correction of Personal Health Information;

(d) prepare and submit PIAs to privacy regulators; and

(e) complete ongoing privacy and security training to promote compliance with Applicable Privacy Legislation.

5.1.2 Information Manager and Custodian Agreement

5.1.2.1 When Dialogue acts as an Information Manager and provides Information Management Services to a Health Services Provider that are Custodians of Personal Health Information for the purpose of assisting the Custodians r in their provision of Clinical Services to Dialogue Members, Dialogue will enter into an Information Manager and Custodian Agreement with the Custodians. The purpose of the Information Manager and Custodian Agreement is to ensure that the Processing of Personal Health Information in connection with the Information Management Services complies with the requirements of Provincial Health Privacy Legislation. For detailed information regarding the Information Manager and Custodian Agreement, as well as the roles and responsibilities of Custodians under the *Health Information Act* and its regulation in Alberta, refer to the Custodian Manual.

5.1.2.2 The Health Service Providers that are Custodians of Personal Health Information designate Dialogue's Privacy Officer to support them in complying with their duties and obligations under Applicable Provincial Health Privacy Legislation. The Custodians remain ultimately accountable for complying with such Legislation and for ensuring the protection of Personal Health Information under their control or custody.

5.1.3 Collection, Use and Disclosure of Personal Information

5.1.3.1 Dialogue will only collect, use and disclose Personal Health Information on behalf of a Custodiansto provide Information Management Services to the Custodians in order to facilitate the provision of Clinical Services and in accordance with the terms of the Information Manager and Custodian Agreement and as otherwise permitted or required by applicable law.

5.1.3.2 When implementing new procedures, products and services that impact the delivery of Clinical Services, the Care Team will coordinate with any relevant Health Services Providers and Custodians to ensure that a PIA is conducted, where required, or other steps are taken to promote compliance with Applicable Privacy Legislation.

5.2 How Dialogue Processes Personal Information Acting In Its Own Capacity

5.2.1 Application of this Part 5.2

5.2.2 This Part 5.2 applies in circumstances where Dialogue Processes Personal Information in its own capacity (including, for example, to provide Clinical Services in jurisdictions where Dialogue is considered a Custodian, to provide non-Clinical Services, to comply with its legal obligations and to manage Dialogue Agents). In those circumstances, Dialogue does so as the accountable entity (or Custodian, where applicable) of the Personal Information.

5.2.3 Aside from the Dialogue accountabilities stated in this Part 5.2, the processes and safeguards detailed in this Part also apply to Dialogue and its Custodians of Personal Health Information when Dialogue is acting as an Information Manager.

5.2.4 General Accountability

5.2.4.1 Dialogue is committed to Processing Personal Information in compliance with Applicable Privacy Legislation. Dialogue has established and maintains a set of policies, procedures and other practices governing its Processing of Personal Information, including policies and practices (i) on the retention and

destruction of Personal Information; (ii) on the roles and responsibilities of Dialogue Agents throughout the information life cycle; (iii) for managing individual privacy rights and related requests as well as complaints regarding Dialogue's Processing or protection of Personal Information; (iv) to help safeguard Personal Information in Dialogue's custody or control and ensure its accuracy; (v) to ensure that privacy training is conducted; and (vi) to manage the company's response to a Privacy Incident. Dialogue must publish and maintain information about these policies and practices, including this Internal Privacy Policy, on its website, in accordance with Applicable Privacy Legislation. The Privacy Officer is responsible for ensuring that information about Dialogue's policies and practices is published, in clear and simple terms, on Dialogue's website and to review and, if necessary, update such information at least annually to ensure that it remains accurate and continues to reflect Dialogue's policies and practices.

5.2.5 Privacy Officer

5.2.5.1 As Dialogue is subject to Applicable Privacy Legislation, it is required to identify a contact person who is responsible for ensuring compliance with Applicable Privacy Legislation. Dialogue designates a Privacy Officer to exercise the role and function of the person in charge of the protection of Personal Information within its organization. The Privacy Officer is responsible for ensuring Dialogue has policies, procedures and other practices in place that accurately reflect Dialogue's activities and operations regarding information Processing and that implement and comply with Dialogue's legal and contractual obligations, including relevant Applicable Privacy Legislation. As stated above, where Health Service Providers are Custodians of Personal Health Information, these Custodians designate Dialogue's Privacy Officer to support them in complying with their duties and obligations under Applicable Provincial Health Privacy Legislation. The Custodians remain ultimately accountable for complying with such Legislation and for ensuring the protection of Personal Health Information under their control or custody.

5.2.5.2 The responsibilities of the Privacy Officer include:

(a) **Compliance and Monitoring** – Identifying, assessing, mitigating and monitoring any potential or actual privacy compliance issues involving Dialogue's Processing or Processing of Personal Information.

(b) **Policies, Procedures and Practices** – Ensuring that relevant policies, procedures and other practices are developed, implemented and

maintained as necessary to ensure compliance with this Internal Privacy Policy and Applicable Privacy Legislation, and approving any policies, procedures and other practices governing Dialogue's processing or protection of Personal Information, including any material changes thereto;

(c) **Raise Awareness** – Ensuring that Dialogue Agents are aware of their duties, roles and responsibilities when Processing Personal Information for or on behalf of Dialogue;

(d) **Assistance and Support** – In consultation and collaboration with relevant stakeholders, including Dialogue Agents, providing timely advice or opinion on any real-world application of Applicable Privacy Legislation, as applicable to Dialogue's activities and operations, including matters pertaining to the release or non-release of Personal Information;

(e) **Individual Privacy Rights and Complaints Management** – Managing individual privacy rights and related requests as well as complaints regarding Dialogue's Processing or protection of Personal Information. This includes overseeing and implementing processes to facilitate the exercise of individual privacy rights, providing access to or rectification of Personal Information in accordance with Applicable Privacy Legislation, respecting any other privacy rights that may be afforded to individuals if so required by these laws, investigating any relevant and credible complaints, and responding to such requests or complaints in a manner that respects Dialogue's policies and procedures as well as legal and contractual requirements;

(f) **Information Security** – Ensuring the overall security and protection of Personal Information, including Personal Health Information, in the custody or control of Dialogue;

(g) **Privacy Impact Assessments** – Participating in the elaboration of any PIA carried out under Section 5.3.4 and proposing appropriate measures to help ensure the protection of Personal Information;

(h) **Breach of Security Safeguards** – In the context of a breach of security safeguards, responding to any Privacy Incident, recording any disclosures of Personal Information to a third party that may mitigate the injury or harm caused by, or resulting from, the breach of security safeguards, and participating in the assessment of such injury or harm, as further detailed in Section 5.3.6;

(i) **Represent Dialogue in Privacy Matters** – Representing Dialogue in its dealings with third parties, including federal and provincial governments, law enforcement and privacy commissioners, on matters relating to Personal Information in the custody or control of Dialogue or Dialogue's Processing of such information.

5.2.5.3 The Privacy Officer may delegate these responsibilities, in whole or in part, to any other person. Any such delegation of responsibility may be made, in writing or orally, and will be reflected in Dialogue's policies and procedures, including this Internal Privacy Policy, as appropriate.

5.2.5.4 The Privacy Officer can be reached at privacy@dialogue.co. Dialogue will endeavor to publish and maintain the title and contact details of the Privacy Officer on Dialogue's website.

5.2.6 Collection, Use and Disclosure of Personal Information

5.2.6.1 **Privacy Policy.** Dialogue has published a Privacy Policy (www.dialogue.co/privacy) on its website, which describes its practices with respect to the Processing of Personal Information about Members, website visitors and job applicants (hereafter, "**Privacy Policy**"). Dialogue must ensure that this Privacy Policy continues to accurately reflect its practices in a manner that complies with Applicable Privacy Legislation. At a minimum, the Privacy Policy must respect the following requirements:

(a) Describe the categories of Personal Information collected by Dialogue;

(b) Describe the means by which the information will be collected;

(c) Describe the purposes for which this information will be used;

(d) List the names or, if not practicable in the circumstances, the categories of third parties to which Personal Information may be disclosed and for which purposes;

(e) List the categories of third-party Service Providers to which Personal Information may be transferred for Processing;

(f) Inform individuals of their rights of access and rectification, and how to exercise these rights;

(g) Inform individuals of their right to withdraw consent, and how to exercise this right and any consequences related thereto, including relevant legal or contractual restrictions, if any;

(h) Indicate whether Personal Information may be transferred outside the jurisdiction (province/territory/country) where individuals are located, if applicable; and

(i) Provide the title and contact details of the Privacy Officer.

The Privacy Policy is presented to Members before or at the time of collection of their Personal Information.

5.2.6.2 **Personnel Privacy Notice.** Dialogue has published a Personnel Privacy Notice on internal communication channels, which

describes its practices with respect to the Processing of personnel Personal Information (hereafter, "**Personnel Privacy Notice**"). Dialogue must ensure that this Personnel Privacy Notice complies with the same requirements as those described above.

5.2.6.3 **Notice of Collection.** Before or at the time of collection of Personal Information directly from individuals to whom such information relates, Dialogue must provide notice to individuals, informing them of the purposes for which the company collects, uses and discloses Personal Information as well as any other relevant information required by law.

5.2.6.4 **Collection of Personal Information**. Unless otherwise permitted or required by law, Dialogue must generally collect Personal Information directly from the individual to whom such information relates and obtain valid consent, which may be express or implied depending on the context and Applicable Privacy Legislation. In addition, Dialogue may collect Personal Information only when necessary for the following purposes: To manage Dialogue's business operations, including responding to inquiries or requests from Members, Dialogue Agents, and job applicants, and protecting Dialogue's properties, clients and Dialogue Agents against fraud or other types of harm;

(a) To provide Dialogue's products or services if so requested;

(b) To establish, manage or terminate an employment relationship or Dialogue's relationship with a contractor or third-party Service Provider;

(c) To comply with applicable legal or contractual requirements; and

(d) Any other reasonable purpose with the individual's valid consent or as otherwise permitted or required by law.

5.2.6.5 **Exceptions.** Depending on Applicable Privacy Legislation, Dialogue may collect Personal Information from sources other than the individual to whom such information relates and/or for purposes other than those mentioned above, without obtaining prior consent, in the following situations:

(a) When collection is clearly in the interests of the individual concerned and consent cannot be obtained in a timely way;

(b) When it is reasonable to expect that collection with the knowledge and consent of the individual would compromise the availability or accuracy of such information, and the collection is reasonable for the purposes of investigating a breach of an agreement or a contravention of an applicable law or regulation; and

(c) As otherwise required or permitted by law.

5.2.6.6 **Use and Disclosure of Personal Information.** Dialogue must use and disclose Personal Information only in accordance with the relevant privacy notice or as otherwise permitted or required by law. Applicable Privacy Legislation may permit Dialogue to use or disclose Personal Information without obtaining prior consent, in the following situations:

(a) When shared with a third-party Service Provider or contractor who Processes such information on behalf of Dialogue, provided the parties enter into a written agreement that contains adequate privacy and information security safeguards, in accordance with Section 5.3.2;

(b) To obtain legal advice from Dialogue's lawyers;

(c) To collect a debt owed by the individual to Dialogue;

(d) When required to comply with a subpoena, warrant or order issued, or made by, a court, regulator, law enforcement or governmental authority with jurisdiction to compel disclosure, or otherwise to comply with court processes, in accordance with Section 5.2.6;

(e) To respond to an emergency that threatens the life, health or security of an individual, provided Dialogue informs the individual to whom the information relates as soon as possible of such use when required by law;

(f) To investigate a breach of an agreement or a contravention of applicable laws, if use with the knowledge or consent of the individual would compromise the investigation; To detect or suppress fraud or prevent fraud that is likely to be committed, if use with the knowledge or consent of the individual would compromise the ability to prevent, detect or suppress the fraud;

(g) Where 20 years have passed since the individual's death, or 100 years have passed since the record was created; and

(h) As otherwise required or permitted by law.

5.2.6.7 Please note that the specific conditions for relying on the above exceptions may vary depending on Applicable Privacy Legislation. Real-world application of these exceptions should be validated with the Privacy Officer, as appropriate.

5.2.6.8 Dialogue Agents may access Personal Information if they have a "need-to-know" in the course of their duties. They must only use or disclose Personal Information if this is required to perform their duties.

5.2.7 Request from Regulators, Law Enforcement and Government

5.2.7.1 **Regulators.** If a Dialogue Agent receives an inquiry, request or other form of communication from a regulator, such as the Office of the Privacy Commissioner of Canada or the Commission d'accès à l'information du Québec, regarding Dialogue's Processing of Personal Information, the Dialogue Agent must immediately inform the Privacy Officer at the address indicated in Section 5.2.4.4. The Privacy Officer is responsible for Processing and responding to such inquiry, request or communication and consulting with relevant Dialogue Agents and other stakeholders. If a request relates to Personal Information Dialogue processes on behalf of its corporate client, where applicable, the Privacy Officer may need to consult with that client before responding to the request.

5.2.7.2 **Law Enforcement, Government and Legal Process.** If a Dialogue Agent receives a subpoena, court order or a similar request from law enforcement or a governmental authority seeking to obtain access to Personal Information under the custody or control of Dialogue, the Dialogue Agent must immediately inform the Privacy Officer at the address indicated in Section 5.2.4.4. The Privacy Officer shall be responsible for Processing and responding to this request, and where appropriate, consulting with relevant Dialogue Agents and other stakeholders. If a request relates to Personal Information Dialogue Processes on behalf of its corporate client, the Privacy Officer may need to consult with that client before responding to the request.

5.2.8 Accuracy of Personal Information

5.2.8.1 Dialogue must endeavor to use Personal Information that is accurate, complete, and up-to-date as is necessary for the purposes for which the information is to be used and taking into account the interests of the individual to whom the information relates.

5.2.8.2 Dialogue Agents have access to their employment file through our human resources information system and can update their Personal Information as needed.

5.2.8.3 Clients' human resources administrators may update their personnel list and other information through coordination with the Customer Success Team.

5.2.8.4 Members may update their Personal Information by contacting the Customer Success Team at support@dialogue.co (or through the Virtual Care App, where applicable).

5.2.8.5 Dialogue minimizes the possibility of using incorrect information when making a decision about the individual, or when disclosing information to third parties.

5.2.9 Access and Rectification of Personal Information, and Other Individual Privacy Rights

5.2.9.1 Dialogue respects an individual's right to access or rectify their Personal Information, to withdraw consent and to obtain details about Dialogue's Processing of their Personal Information, in accordance with Applicable Privacy Legislation. Depending on the jurisdiction in which an individual resides, an individual interacting with Dialogue may also be entitled to request to have their Personal Information deleted or communicated in a structured, commonly used technological format, and to obtain details about Dialogue's use of automated decision-making systems, in limited circumstances. Dialogue is responsible for informing individuals of their rights through the relevant privacy notice and for maintaining procedures that allow for the effective exercise of these rights.

5.2.9.2 **Request from Dialogue Agents.** A Dialogue Agent may access or rectify their Personal Information through our human resources information system, and if they have any issues or specific requests should contact the Talent and Culture Team, as further detailed in the Personnel Privacy Notice. If the Dialogue Agent is not satisfied with the response, they may contact the Privacy Officer by submitting a written request at the address indicated in Section 5.2.4.4. Any other request related to the Dialogue's Processing of personnel Personal Information, including, where applicable, a request to have such information deleted or communicated in a particular format or to obtain details about Dialogue's Processing of personnel Personal Information or use of automated decision-making systems, must be directed to the Privacy Officer in writing. The Privacy Officer is responsible for responding to such request in accordance with Applicable Privacy Legislation.

5.2.9.3 **Request from Individuals other than Dialogue Agents.** Any individual other than a Dialogue Agent must direct their access or rectification request, or any other request relating to Dialogue's Processing of their Personal Information, as follows:

(a) in the case of a Member, to the Customer Success Team at support@dialogue.co (or through the Virtual Care App, where applicable);

(b) otherwise, to the Privacy Officer by submitting a written request at the

address indicated in Section 5.2.4.4; so that the request can be managed as per the Management of Individual Rights Requests Operating Guideline.

5.2.9.4 If a Dialogue Agent receives such request directly, the Dialogue Agent must immediately forward the request to the Privacy Officer who will then coordinate review and response by the Appropriate Team. While the Dialogue Agent who received the request may send an acknowledgment of receipt, the Dialogue Agent must refrain from responding to the request without express written authorization from the Privacy Officer. The Privacy Officer is responsible for facilitating the response to such request in accordance with relevant legal and contractual obligations.

5.3 Other Matters

5.3.1 Retention and Disposal of Personal Information

5.3.1.1 Dialogue retains Personal Information only for as long as necessary to fulfill the purposes for which this information was originally collected, unless further retention is required for legitimate legal, regulatory or business purposes. When Personal Information is no longer required to be retained, Dialogue must securely destroy, erase or anonymize the information in accordance with relevant legal, regulatory and contractual requirements. Dialogue's record retention and disposal procedures are outlined in Dialogue's Personal Information Retention and Destruction Operating Guideline. Dialogue Agents are responsible for complying with these requirements, including by using secure methods when performing authorized destruction of Personal Information.

5.3.1.2 Retention and disposal of Personal Information will be in accordance with Dialogue's Personal Information Retention and Destruction Operating Guideline and any related retention schedules established. In keeping with these schedules, Personal Information no longer required to fulfill the purposes for which it was collected (or which are no longer required to be retained for legitimate legal, regulatory or business purposes) should be destroyed, erased, or made anonymous. Care must be used in the disposal or destruction of Personal Information to prevent unauthorized parties from gaining access to the information. When disposal of hard copy information is authorized, shredding must be used to maintain confidentiality.

5.3.2 Third-Party Service Providers and Contractors

5.3.2.1 Dialogue may retain the services of a third-party Service Provider to collect, use, retain, destroy, disclose or otherwise Process Personal Information on Dialogue's behalf. Dialogue uses contractual and other means to ensure that Personal Information receives an adequate and comparable level of protection while it is being Processed by a third-party Service Provider. It is the responsibility of the business unit making the procurement request to obtain all required internal approvals prior to engaging a third-party Service Provider, in accordance with the Dialogue Privacy Protection Operating Guideline – Outsourcing. Any third-party Service Provider retained by Dialogue must comply with relevant legal and contractual obligations as well as the Dialogue Privacy Protection Operating Guideline - Outsourcing.

5.3.3 Cross-border Transfers of Personal Information

5.3.3.1 Third-party Service Providers may be located in jurisdictions outside of Canada or may access, store or otherwise transfer Personal Information to other jurisdictions in the course of providing their services to Dialogue. Before transferring any Personal Information outside of Canada or a Canadian province, Dialogue must inform individuals of this possibility through the relevant privacy notice and ensure that the transfer complies with relevant legal and contractual obligations, as further detailed in our Data Protection Addendum in the Privacy Protection Operating Guideline - Outsourcing.

5.3.3.2 Where the transfer involves Personal Information about Quebec residents, Dialogue must conduct a PIA to ensure that the information would receive adequate protection. In particular, the PIA must take into account the sensitivity of the Personal Information, the purposes of Processing, the security measures in place as well as the legal framework applicable in the jurisdiction to which the information is transferred. Dialogue may proceed with the transfer only if it is established that Personal Information would receive adequate protection, in particular in light of generally recognized principles regarding the protection of Personal Information. The Privacy Officer is responsible for establishing procedures and practices to comply with this section, and the relevant business unit and procurement specialist are responsible for consulting with the Privacy Officer and Legal & Compliance Department to ensure that the PIA is carried out in accordance with Dialogue's policies and procedures and Applicable Privacy Legislation.

5.3.4 Projects Impacting Privacy of Individuals

5.3.4.1 Some activities and practices involving Personal Information may create a higher risk for the privacy of individuals and require Dialogue to conduct a PIA to identify and mitigate those risks.

5.3.4.2 Dialogue has developed Privacy Impact Assessment Operating Guideline which outline the steps that must be taken by relevant business units/Dialogue Agents in determining whether a PIA is needed:

(a) Review the Privacy Impact assessment Operating Guideline;

(b) Complete a Privacy Impact Assessment Intake Form; and

(c) Follow instructions to complete a full Privacy Impact Assessment (Template).

5.3.5 Information Security

5.3.5.1 Dialogue implements and maintains appropriate technical, physical and organizational security measures to protect Personal Information under its custody or control against any loss or unauthorized access, use or disclosure. Dialogue Agents share this responsibility and must treat as confidential all Personal Information in Dialogue's possession or control, in accordance with this Internal Privacy Policy and other relevant policies and procedures. Dialogue's Information Security Policy covers the following important components:

(a) IT Acceptable Use

(b) Guest Access

(c) Password

(d) Security Awareness Training

(e) Account Management

(f) Asset Management

(g) Incident Management

(h) Third Party Service Provider

(i) Data Classification

5.3.5.2 The Chief information Security Officer (CISO) is responsible for the Information Security Policy.

5.3.5.3 **Transmission / Sharing of Personal Information.** Extreme care must be taken when transmitting Personal Information internally or externally to ensure that: (i) the persons who have requested the information and those to whom you are sending it have been

authenticated, and (ii) the method of transmission (whether by telephone, mail, fax, through the Virtual Care App or otherwise) is appropriate to protect the confidentiality of the information in light of its sensitivity. If mailed, the information should be enclosed in a securely sealed envelope and stamped "Private and Confidential". In all instances, the name of the intended recipient must be clearly identified.

5.3.5.4 Because of the ease with which email is transmitted, and issues relating to control over storage of multiple copies of email, the use of email to transmit Personal Information is prohibited. All Personal Information and Personal Health Information should be transmitted via the Virtual Care App or fax/mail.

5.3.6 Breaches of Security Safeguards

5.3.6.1 Dialogue Agents must remain vigilant for Privacy incidents and breaches and must immediately report any potential Privacy Incident through the appropriate channel This will allow Dialogue to promptly investigate and respond to the incident in accordance with Dialogue's Incident Response Plan and related policies and procedures, and to help protect Dialogue, affected individuals and other organizations against resulting harm. This includes consulting the Privacy Officer to determine whether the breach meets the threshold provided under Applicable Privacy Legislation, which would trigger obligations to notify affected individuals, relevant privacy regulators and possibly other third parties.

5.3.6.2 A Privacy Incident could occur when there is any loss of Personal Information, or any unauthorized access, use or disclosure of Personal Information. For example:

(a) **Accident:** Personal Information is disclosed to an unintended recipient by accident. For example: a letter or fax containing information about a Member is sent to the wrong address/location due to mechanical or human error;

(b) **Loss:** Personal Information goes missing. For example, a Dialogue Agent's laptop, mobile device or briefcase containing Personal Information is lost.

(c) **Unauthorized Access, Use or Disclosure:** Personal Information is accessed, used or disclosed by an unauthorized person, or in an unauthorized manner, or for an unauthorized purpose, including in contravention of any of Dialogue's applicable policies or applicable law. For example: (i) a Dialogue Agent's laptop, mobile device or briefcase containing Personal Information is stolen; (ii) a Dialogue

Agent accesses Personal Information of another Dialogue Agent or a Member for an unauthorized purpose (e.g. personal curiosity); or (iii) Dialogue's IT systems storing Member Personal Information are hacked or accessed by cybercriminals.

5.3.6.3 Immediate reporting of an actual or suspected breach of security safeguards will allow designated Dialogue Agents to promptly investigate and respond to the breach in accordance with Dialogue's policies and guidelines, to help protect Dialogue and all affected individuals and other organizations. The sooner Dialogue takes action regarding a breach of security safeguards, the better it will be able to effectively contain the breach and avoid and mitigate resulting harm.

5.3.6.4 Dialogue Agents are expected to be cognizant of the increased risk of cyber threats and to take several practical steps to stay secure:

(a) ***MFA:*** set up multi-factor authentication everywhere.

(b) ***Strong Unique Passwords:*** Do not reuse passwords. Make sure that they are long or include at least 8 characters and at least one number and one special character.

(c) ***Keep Systems Updated:*** Make sure all of your devices, including personal ones, are fully updated.

(d) ***Run Security Software on Your Laptop:*** If you are part of the Care Team and using your own laptop for work, remember to install SentinalOne.

(e) ***Remain Vigilant:*** Most successful attacks still start with people being tricked with all sorts of phishing schemes and scams. Expect phishing attempts on every communication channel; emails, texts, LinkedIn, etc.

5.3.7 Training and Awareness

5.3.7.1 The Privacy Officer shall develop a privacy training and awareness program to foster a privacy respectful culture within Dialogue and to ensure that Dialogue Agents comply with this Internal Privacy Policy. This may include:

(a) Providing privacy training as part of the onboarding program for recently hired personnel, and on a regular basis thereafter; and

(b) Role-specific training for Dialogue Agents who Process a particularly large amount of Personal Information, or sensitive Personal Information (e.g. payroll managers, MedOps and the Care Team).

5.3.8 Complaints and Reporting Violations

5.3.8.1 **Dialogue Agents**. Dialogue Agents who believe there has been a breach of Applicable Privacy Legislation or of this Internal Privacy Policy, or otherwise wish to complain about Dialogue's information Processing practices, are encouraged to raise their concerns directly with their manager, who may consult with the Privacy Officer as necessary. In addition, Dialogue Agents who receive a complaint related to the Processing of Personal Information from an individual should promptly report the complaint and the individual's name and contact information (if available) to the Privacy Officer.

5.3.8.2 **Other individuals**. Individuals (other than Dialogue Agents) who believe there has been a breach of Applicable Privacy Legislation or of this Internal Privacy Policy, or otherwise wish to complain about Dialogue's information Processing practices, should be advised to submit their complaint through Dialogue's privacy email: privacy@dialogue.co.

5.3.8.3 There will be no retaliation against any individual for reporting violations or suspected violations, so long as the report is made in good faith.

5.3.9 Questions and Relevant Contact Information

5.3.10 Dialogue Agents who have any questions or require additional information about this Internal Privacy Policy are encouraged to contact their manager or the Privacy Officer at privacy@dialogue.co.

5.3.11 Changes to this Internal Privacy Policy

5.3.11.1 Dialogue regularly reviews its policies and procedures, and from time to time, this Internal Privacy Policy will be reviewed as required in case of any legislative or other relevant developments, taking into account new practices or recommendations issued by the Privacy Officer and/or external privacy/data protection authority guidelines. This Internal Privacy Policy, as revised from time to time, may be found on Dialogue's Privacy Program Notion page.

6. ENFORCEMENT

6.1 The Privacy Officer may audit at any time to ensure compliance with this Internal Privacy Policy and its related Operating Guidelines. Failure to report known violations of this Operating Guideline to the Privacy Officer is considered a violation of this Operating Guideline.

6.2 Dialogue Agents who violate this Operating Guideline may be subject to appropriate disciplinary action up to and including termination or termination of contractual agreements, denial of access to information technology resources, and other actions as well as both civil and criminal penalties.

6.2.1 Other Related Dialogue Policies, Procedures and Guidelines

6.2.1.1 Please also consider the following Dialogue guidelines procedures:

(a) Privacy Policy
(b) Personnel Privacy Notice
(c) Management of Individual Rights Requests Operating Guideline
(d) Personal Information Retention and Destruction Operating Guideline
(e) Privacy Impact Assessment Operating Guidelines
(f) Privacy Protection Operating Guidelines – Outsourcing
(g) Information Security Policy
(h) Incident Response Plan

Version History:

Version Number	Effective Date	Revision Date	Approval
1	August 1, 2022	August 1, 2022	Nathalie Delisle, Chief Privacy Officer Dr. Marc Robin, Medical Director
2	August 1, 2024	August 1, 2024	Dominique Payette, Privacy Officer

Appendix A

GLOSSARY OF TERMS

"**Applicable Privacy Legislation**" means applicable laws and regulations relating to the Processing and/or Protection of Personal Information, including Provincial Health Privacy Legislation.

"**Appropriate Team**" means either the Care Team or Customer Success Team.

"**Authorized Person**" means a person authorized to exercise a right or power conferred on an individual under Applicable Privacy Legislation, including the right to access, correct or amend Personal Information.

"**Clinical Services**" means the provision of virtual health care services synchronously and asynchronously to Members by Health Services Providers via the Virtual Care App.

"**Contracting Employee**" means the Dialogue Agent who has the relationship with a third-party Service Provider and is responsible for entering into a service agreement with the third-party Service Provider.

"**Custodian**" means a person who has custody or control of Personal Health Information, and as otherwise defined as a "custodian" or "trustee" under applicable Provincial Health Privacy Legislation.

"**Dialogue**" means Dialogue Health Technologies Inc. and its affiliates.

"**Dialogue Agent**" means any employee, independent contractor, consultant, director or officer of Dialogue.

"**Dialogue Data**" means any data or record of any nature and kind, in any form (including paper or electronic) or on any medium, that includes Personal Information, which is under the control or possession of Dialogue.

"**Dialogue IT Assets**" means all information technologies, operational technologies and other kinds of information technology systems, environments, networks, equipment, servers, computers, devices, applications, software, services, facilities and infrastructure used by Dialogue to Process Personal Information.

"**DPA**" means Dialogue's template Data Protection Addendum.

"**HIA**" or "**AB HIA**" means the Alberta *Health Information Act*, RSA 2000 c H-5.

"**Health Services Providers**" means health care professionals, including physicians, psychologists, nurses and other allied health care professionals acting as Custodians (or as agents of Dialogue in jurisdictions where Dialogue is the Custodian) and providing Clinical Services.

"**Information Management Services**" means the provision of access to Dialogue's software platform and electronic medical record systems, related information technology, information management and administrative and clinical support services and staff, including text-based, audio and video consultation technology and any associated technological updates, maintenance, quality control and support.

"**Information Manager**" means a person who supplies services for the purpose of enabling a Custodian to collect, use, modify, disclose, retain or dispose of Personal Health Information or as otherwise defined under Provincial Health Privacy Legislation.

"**Information Manager and Custodian Agreement**" means the agreement between Dialogue and Health Services Providers that are Custodians of Personal Health Information and operate in the province of Alberta. In all Dialogue policies and procedures, terms such as "Information Management Agreement", "IMA" and "IMCA" also mean Information Manager and Custodian Agreement.

"**Manager**" means a business department manager.

"**Member(s)**" means individuals who use or access Dialogue's products and services, including users or patients of the Virtual Care App. In all Dialogue policies and procedures, terms such as "User(s)" or "Patient(s)" also mean Member(s).

"**OPC**" or **Office of the Privacy Commissioner**" means the Office of the Privacy Commissioner of Canada.

"**Personal Health Information"** means any Personal Information regulated under applicable Provincial Health Privacy legislation, including information concerning an individual's physical or mental health; the provision of their health care; the eligibility or payment for their health care; the identity of the provider of their health care; when they received health care; and, where required for an authorized purpose, their health care number. In all Dialogue policies and procedures, terms such as "health information," "PHI," "medical information," or "medical record" also mean Personal Health Information.

"**Personal Information**" means any information that identifies, or could be reasonably associated with, an individual, regardless of the form and/or recorded on any medium (e.g. paper, computer disk or memory storage, audio, video and internet cloud storage), and includes Personal Health Information.

"**PIA**" means a privacy impact assessment.

"**Privacy Officer**" means Dialogue's Privacy Officer.

"**Privacy Policy**" means the public facing privacy policy that Dialogue makes available.

"Process" or "Processing" means the collection, use, modification, retrieval, transfer, disclosure, storage, de-identification, anonymization, deletion, destruction, and/or management of Personal Information.

"**Processing Activity"** means any project, initiative, program or activity that involves the Processing of Personal Information.

"**Provincial Health Privacy Legislation**" means the applicable privacy laws and regulations that govern the Processing of Personal Information in the provision of health care, including the Quebec *Act respecting health and social services information*, the Alberta HIA, the Saskatchewan *Health Information Act*, the Manitoba *Personal Health Information Act*, the Ontario *Personal Health Information Protection Act, 2004*, the New Brunswick *Personal Health Information Privacy and Access Act*, the Prince Edward Island *Health Information Act*, the Nova Scotia *Personal Health Information Act*, the Newfoundland and Labrador *Personal Health Information Act*, the Yukon *Health Information Privacy and Management Act* and the Northwest Territories *Health Information Act*.

"**Privacy Incident**" means any reasonably suspected or actual loss of, or unauthorized access to or use or disclosure of, Personal Information or any other breach or attempted breach, by any person, of any obligation concerning the confidentiality of Personal Information. In all Dialogue policies and procedures, terms such as "privacy breach" and "data security incident" also mean Privacy Incident.

"**Service Provider**" means any person or entity that provides services to another entity.

"**Third Party Privacy Assessment Checklist**" means the documentation that prospective third-party Service Providers must complete prior to an engagement by Dialogue.

"**Virtual Care App**" means Dialogue's integrated virtual care application that Members install on their own smartphone, desktop or tablet computer.