Privacy Protection Operating Guideline - Outsourcing

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

CONFIDENTIAL

1. Objective

1.1 Dialogue uses Personal Information and information technology systems in some aspects of its business. Dialogue is responsible for Personal Information in its custody or under its control, including information that has been transferred to third-party Service Providers for Processing.

1.2 Contracts with third-party Service Providers must provide guarantees of confidentiality and security of Personal Information. Failure to protect the confidentiality and security of Personal Information could result in potentially significant losses and liabilities to Dialogue.

1.3 This Operating Guideline provides guidance to Dialogue Agents for assessing and managing privacy risks with respect to the Processing of Personal Information by third-party Service Providers.

1.4 This Operating Guideline must be read together with the most current version of Dialogue's DPA.

2. DEFINITIONS

2.1 Refer to Appendix A of the 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 this Operating Guideline.

3.2 Dialogue Agents are required to adhere to this Operating Guideline.

4. SCOPE

4.1 This Operating Guideline applies to all Dialogue Agents involved in establishing or administering a service agreement with any third-party Service Provider who provides Dialogue with any kind of service that involves the Processing of Dialogue Data.

4.2 Service agreements can involve information technology services, operational technology services or data Processing services such as payroll and benefit processing, digital advertising services, cloud hosting services, SaaS, electronic medical record, etc.

4.3 This Operating Guideline does not apply to other circumstances in which Dialogue may disclose Dialogue Data to a third party (e.g. law enforcement or a government agency). Dialogue Agents must obtain advice from Dialogue's Privacy Officer/Legal & Compliance Department regarding those circumstances.

4.4 If you have any question about this Operating Guideline, please contact Dialogue's Legal & Compliance Department at legal@dialogue.co or privacy@dialogue.co.

5. DETAILS

5.1 Third-Party Service Provider Selection Process

5.1.1 A proposed third-party Service Provider that will Process Personal Information must be asked by the Contracting Employee to agree to complete the Third Party Privacy Assessment Checklist attached as APPENDIX A of this Operating Guideline, before the third-party Service Provider is selected by Dialogue to begin contract negotiations as well as to confirm its willingness to agree to the DPA, including the proposed "Security Program Minimum Requirements" included in Schedule "B" of the DPA. If Dialogue is conducting a formal procurement process, it might be appropriate to include the relevant DPA and Third-Party Privacy Assessment Checklist in the request for proposals or similar documents. A proposed third-party Service Provider's willingness or refusal to agree to the DPA or to complete the Third-Party Privacy Assessment Checklist might be an important consideration for Dialogue when determining whether to engage in contract negotiations with the third-party Service Provider.

5.2 Guidance

5.2.1 Step 1: Initial Privacy Risk Assessment of Service Agreement

5.2.1.1 **Personal Information.** The Contracting Employee responsible for a service agreement must determine if the services to be provided under the agreement involves Personal Information. If this initial privacy risk assessment reveals that the services involve Personal Information, then the Contracting Employee responsible for the service agreement must complete Step 2 and consult with Dialogue's Privacy Officer/Legal & Compliance Department to determine whether it is necessary to conduct a PIA in connection with the proposed services and to negotiate the service agreement.

5.2.1.2 **Subcontracting.** The Contracting Employee responsible for a service agreement must determine if the Personal Information to be outsourced is subject to a contract between Dialogue and a corporate client and if the subcontracting is permitted under such contract.

5.2.1.3 **Information or Service Delivery Systems.** The Contracting Employee responsible for a service agreement must determine if the service agreement relates to a project to acquire, develop or overhaul an information system or electronic service delivery system involving the collection, use, disclosure, retention or destruction of Personal Information. If this initial privacy risk assessment reveals that the services to be provided involve this

type of project, the Contracting Employee must consult the Privacy Officer/Legal & Compliance Department to determine if a PIA must be carried out.

5.2.1.4 **Health Services Providers/Custodians.** The Contracting Employee responsible for a service agreement must determine if Personal Information to be outsourced is subject to Provincial Health Privacy Legislation, such as the HIA, which may require Dialogue to conduct a PIA on behalf of the relevant Health Services Providers or include specific language in the DPA or service agreement to ensure compliance with applicable Provincial Health Privacy Legislation. The Contracting Employee must ensure to include the Health Services Providers/Custodians in the assessment and the PIA, when required.

5.2.1.5 **Cross-border Transfer of Personal Information.**

(a) The Contracting Employee responsible for a service agreement must determine if the services involve the transfer of Personal Information outside the country or province of individuals whose Personal Information is in the custody or control of Dialogue, in which case the Contracting Employee must consult the Privacy Officer to determine if a risk assessment must be conducted, which would take into account the following factors:

(i) sensitivity of the Personal Information;

(ii) purposes for which the Personal Information will be used;

(iii) protection measures, including those that are contractual, that will apply to the Personal Information; and

(iv) legal framework applicable in the jurisdiction in which the Personal Information will be communicated under the service agreement, including the Personal Information protection principles applicable in that jurisdiction.

5.2.1.6 **Adequate protection**. If the assessment conducted by the Privacy Officer concludes that the Personal Information "would receive adequate protection, in particular in light of generally recognized principles regarding the protection of personal information" and that Personal Information Processed outside of the home jurisdiction (country or province) by third-party Service Provider will be sufficiently protected with a contract that incorporates the requirements detailed in this Operating Guideline, the Contracting Employee responsible for the service agreement must complete Step 2.

5.2.1.7 **Inadequate protection.** If the assessment conducted by the Privacy Officer concludes that the Processing of Personal Information abroad creates a risk that would result in inadequate protection of the Personal Information, then Dialogue and the third-party Service Provider will have to agree on measures to reduce that risk to an adequate level, which measures must be approved by the Privacy Officer. The Contracting Employee responsible for the service agreement must follow the instructions of the Privacy Officer before completing Step 2.

5.2.2 Step 2: Privacy Due Diligence of Third-Party Service Provider

5.2.2.1 If the initial privacy risk assessment reveals that the service agreement involves Personal Information, then the Contracting Employee responsible for the service agreement must conduct an appropriate due diligence investigation of the potential third-party Service Provider and its practices and procedures relevant to the handling of Dialogue Data. To do so, the Contracting Employee must request that the third-party Service Provider complete the "Third Party Privacy Assessment Checklist" using the template attached as APPENDIX A. The Contracting Employee must then transmit a copy of the Third Party Privacy Assessment Checklist duly completed by the third-party Service Provider to the Legal & Compliance Department/Privacy Officer.

5.2.2.2 Upon receiving these documents from the Contracting Employee, the Legal & Compliance Department/Privacy Officer (shall review, in consultation with the IT Security Department, the answers provided by the third-party Service Provider in the Third Party Privacy Assessment Checklist and provide instructions to the Dialogue Contracting Employee, as further detailed in Step 3 of this Operating Guideline. The Legal & Compliance Department/Privacy Officer, in consultation with the IT Security Department, will either conclude that the third-party Service Provider's safeguards are acceptable or insufficient.

5.2.3 Step 3: Contract Negotiation

5.2.3.1 No Personal Information shall be transferred to the third-party Service Provider until a service agreement and DPA has been executed by both parties.

5.2.3.2 Each proposed service agreement must be governed by a written contract which must include, at the very minimum, provisions dealing with the following issues:

(a) **Compliance With Applicable Privacy Legislation** – The third-party Service Provider must undertake to comply with Applicable Privacy Legislation;

(b) **Purpose Limitation** – The third-party Service Provider must Process Personal Information only as directed by Dialogue and only for the purposes of providing the services requested;

(c) **Transfers to Third Parties** – The third-party Service Provider must be prohibited from transferring Personal Information to a third party without the prior authorization of Dialogue; and if so authorized, the third-party Service Provider must ensure that the third party is bound by a written agreement that provides Personal Information with an equivalent level of protection;

(d) **Individual Privacy Rights** – If the third-party Service Provider receives an access or rectification request or any other similar request regarding Personal Information Processed on behalf of Dialogue, the third-party Service Provider must forward the request to Dialogue and cooperate with the latter in responding to such request;

(e) **Limitations on Access** – The third-party Service Provider must limit access to Personal Information to only those individuals that need access to deliver the services and have been appropriately trained about the third-party Service Provider's privacy and security obligations under the DPA and Applicable Privacy Legislation;

(f) **Information Security** – The third-party Service Provider must protect Personal Information using adequate physical, technical and organizational safeguards that are adapted to the volume and sensitivity of the Personal Information;

(g) **Privacy Incidents** – The third-party Service Provider must immediately and without delay notify Dialogue of any Privacy Incident;

(h) **Security Review and Audit** – The third-party Service Provider must allow Dialogue to conduct any verification relating to privacy and information security requirements;

(i) **Retention and Secure Disposal** – The third-party Service Provider must return or securely dispose of all Personal Information Processed on behalf of Dialogue upon the termination of the service agreement or at the request of Dialogue;

(j) **Cross-border Transfers** – The third-party Service Provider may Process Personal Information only in Canada, or any other specified location such as a Canadian, if so requested by Dialogue, unless otherwise authorized in writing by Dialogue.

5.2.3.3 LOW risk level

(a) When the privacy due diligence of the third-party Service Provider reveals a LOW risk level, the Contracting Employee shall ensure the inclusion of the DPA to the service agreement. The DPA is designed to be attached to the main part of the service agreement (which might be prepared by either the proposed third-party Service Provider or by Dialogue's Legal & Compliance Department), and takes priority over all other provisions in the service agreement.

(b) The Contracting Employee responsible for a particular service agreement must finalize the DPA. To do so, the Contracting Employee must prepare the DPA by inserting the following information on the relevant pages and once completed, remove any drafting notes:

(c) **On page 1**: the Contracting Employee must insert:

(i) The full name of the Dialogue legal entity contracting with the third-party Service Provider defined as "Company";

(ii) The full name of the legal entity providing the services defined as "Service Provider"; and

(iii) The type of services provided (such as hosting, payroll processing, EMR, etc.).

(d) **On the last page**: the Contracting Employee must insert in the signature blocks:

(i) The full name of the Dialogue legal entity contracting with the third-party Service Provider; and

(ii) The full name of the third-party Service Provider (i.e. legal entity providing the services).

(e) **On Schedule "A" of the DPA:** the Contracting Employee must insert the type of Personal Information transferred to the third-party Service Provider, including:

(i) whether this information relates to Dialogue's customers (or corporate customers' employees) or employees; and

(ii) the type of information transferred, such as name, address, age, personal identification number, Personal Health Information, etc.

(f) The Contracting Employee should consult with:

(i) the Legal & Compliance Department as required, including if any changes are required to the DPA by the third-party Service Provider; and

(ii) the IT Security Department as required, including if any changes are required to Schedule "B" of the DPA entitled "Security Program Minimum Requirements".

5.2.3.4 MODERATE and higher risk level

(a) When the privacy due diligence of the third-party Service Provider reveals a MODERATE and higher risk level, the Contracting Employee shall refer the matter to the Legal & Compliance Department, who will assess:

(iii) in consultation with IT Security Department, if Schedule "B" of the DPA or other Security Program Minimum Requirements are appropriate upon consideration of the answers provided by the third-party Service Provider in the Third-Party Privacy Assessment Checklist; and

(iv) if the DPA or a different agreement is appropriate in the circumstances and may consider adding restrictions/requirements and more detailed and specific privacy or security controls to address the risks presented by the service agreement.

(b) If the Legal & Compliance Department in consultation with the IT Security Department determines that the level of privacy risk is too high in the circumstances, which risk cannot be mitigated by contract or by other measures to be implemented, Dialogue shall refrain from entering into the proposed service agreement.

5.2.4 Contract Administration – Oversight and Monitoring

5.2.4.1 Filing of the DPA

(a) Once a services agreement and DPA are finalized by the Contracting Employee or the Legal & Compliance Department and executed by the third-party Service Provider, it must be sent to the Legal & Compliance Department by email and filed in the appropriate Google Drive - Procurement folder and updated in Dialogue's third-party Service Provider inventory.

5.2.4.2 Ongoing Monitoring of Third-Party Service Provider's Compliance with the DPA

(a) The DPA that governs a service agreement provides Dialogue with various oversight and monitoring rights such as the right to request the third-party Service Provider to provide reports, information and certifications, and rights to conduct audits or investigations of the third-party Service Provider.

(b) If the privacy due diligence of the third-party Service Provider reveals a MODERATE and higher risk level for a third-party Service Provider,

once the service agreement has been signed, the Legal & Compliance Department, in consultation with the IT Security Department must determine the degree to which Dialogue must oversee and monitor the relevant third-party Service Provider's performance of the contract, including with respect to Dialogue Data and Dialogue IT Assets. This monitoring may include annual questionnaires to complete, specific audit or monitoring following an incident reported by the third-party Service Provider, etc.

5.2.4.3 Incidents and Events

(a) The Contracting Employee responsible for a service agreement must immediately report to the Legal & Compliance Department/Privacy Officer/IT Security Department any incident or event that has affected, or is likely to affect, the security, confidentiality, integrity or availability of any Dialogue Data, such as a Privacy Incident.

5.2.5 Step 5: Changes to Scope or Contract Amendment/Renewal/Extension

5.2.5.1 In the event that the scope of a service agreement is modified, including to the extent that there is a change in the Process, system, or to the Dialogue Data impacted by a service agreement, or upon the service agreement being renewed or extended, the Contract Employee shall carry out steps 1 to 3 in light of the change and/or revised scope.

5.2.6 Step 6: Contract Expiration/Termination

5.2.6.1 Return and/or destruction of Dialogue Data

(a) Pursuant to the DPA, at the end of a service agreement, the Contracting Employee shall ensure that the third-party Service Provider return all Dialogue Data, securely delete/destroy all records of Dialogue Data in its possession or control and deliver a written confirmation of compliance to Dialogue.

5.2.6.2 Information security measures

(a) The Contracting Employee must take steps to manage information security risks when a service agreement ends. This may include, for example, cancelling a third-party Service Provider's credentials to remotely access Dialogue Data using Dialogue IT Assets.

6. ENFORCEMENT

6.1 The Privacy Officer may audit at any time to ensure compliance with this Operating Guideline. 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.]

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

THIRD PARTY PRIVACY ASSESSMENT CHECKLIST

Personal Information protection requirements for Dialogue third-party Service Providers are based on Applicable Privacy Legislation in Canada. All Dialogue third-party Service Providers Processing Personal Information on behalf of Dialogue must complete the following questionnaire so that Dialogue can analyse their maturity levels and assess the level of privacy risks they present.

Name of the third party Service Provider ("**Service Provider**"):	
Title and date of current or prospective contract with Dialogue ("**Agreement**"):	
Name of the legal representative of Service Provider:	
Name and contact of privacy officer of Service Provider:	
Date of creation of the checklist:	
Signature of Service Provider's legal representative:	

For internal use only:	

Received by Dialogue on:	
Name and title of Dialogue (Manager or other):	
Reviewed by Dialogue Legal & Compliance Department on:	
Reviewed by the Cybersecurity Department on:	

DEFINITIONS

"**Agreement**" means any kind of arrangement between Dialogue and the Service Provider according to which the latter provides Dialogue with any kind of service that involves the Processing of Personal Information.

"**Applicable Privacy Legislation**" means applicable laws governing the collection, use, disclosure and security of Personal Information applicable to Dialogue and/or the Service Provider, as same may be amended, supplemented and interpreted by regulatory authorities and courts from time to time, including, in Canada, the *Personal Information Protection and Electronic Documents Act* (PIPEDA) and substantially similar provincial laws from Quebec, British Columbia and Alberta, and/or to the extent such Personal Information is processed in the provision of health care, Provincial Health Information Laws.

"**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 to Process Personal Information.

"**Personal Information**" refers to 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.

"**Personal Health Information**" refers to any information concerning an identifiable individual's physical or mental health; the provision of their health care; the eligibility of 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. Personal Health Information also includes information about an identifiable individual that is not Personal Health Information but is contained in the same record or file as Personal Health Information about the individual. It includes demographic and registration information (including billing information).

"**Personnel**" means Service Provider's directors, officers, employees, contract workers, consultants, agents, representatives, partners and other personnel.

"**Processing**" means any operation or set of operations, whether or not by automated means, which is performed upon Personal Information (such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination of otherwise making available, alignment or combination, blocking, erasure or destruction) performed by Service Provider pursuant to an Agreement with Dialogue.

"**Provincial Health Information Laws**" means the applicable privacy statutes and regulations that govern the processing of personal information in the provision of health care, including the relevant and applicable Quebec data protection law, the Alberta Health Information Act, the Saskatchewan Health Information Act, the Manitoba Personal Health Information Act, the Ontario Personal

Health Information Protection Act, 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 and Privacy Management Act and the Northwest Territories Health Information Act.

"**Regulator**" means a government regulator or other government authority (including a privacy commissioner) with lawful jurisdiction over Dialogue or Dialogue's business operations and activities.

"**Privacy Incident**" means any breach of security safeguards or other event or incident that adversely affects, or is likely to adversely affect (a) the security, confidentiality, integrity or availability of any Personal Information, including any loss or theft of, or unauthorized access, use (including copying or modification), disclosure (including any kind of transmission), deletion or disposal of, any Personal Information; or (b) the security, confidentiality, integrity or availability of Service Provider's IT Assets to the extent they are used to Process Personal Information.

"**Services**" means the services performed by or on behalf of Service Provider for Dialogue pursuant to an Agreement.

GENERAL QUESTIONS	
Questions	**Answers**
1. What category of individuals does Personal Information Processed by your organization pursuant to the Agreement relate to?	☐ Dialogue customers' employees (Dialogue members/users) ☐ Dialogue employees ☐ Others, please specify:
2. What type of Personal Information does your organization process pursuant to the Agreement?	*[Include type of information e.g. name, address, email, phone, DoB, health, biometrics, IP address, etc.]*
3. Does your organization Process sensitive information pursuant to the Agreement?	☐ No ☐ Yes – Please specify the type of sensitive information: *[e.g. health information; financial information; biometric information; location*

	information; personal lifestyle and interests; payment; payroll information; or the context surrounding the Personal Information which makes it particularly sensitive]
4. Approximately how many records of Personal Information does your organization Process pursuant to the Agreement?	*[Include approximate number of individual records processed]*
ACCOUNTABILITY	
Questions	**Answers**
5. Has an individual been designated in your organization who is accountable generally for the protection of privacy (Privacy Officer or equivalent)?	☐ No ☐ Yes - Please provide: Name: Title: Email address: Phone number:
6. Has an individual been designated in your organization who is accountable generally for information security (Chief Information Security Officer or equivalent)?	☐ No ☐ Yes - Please provide: Name: Title: Email address: Phone number:

<table>
<tr>
<td>7. Are information security roles and responsibilities clearly defined in your organization?</td>
<td>☐ No
☐ Yes

- Broad responsibilities associated with information security in the organization: [insert details]
- Key roles in information security: [insert details]</td>
</tr>
<tr>
<td>8. Does your organization transfer or otherwise make available Personal Information to other organizations within your group (“Affiliates”)? Why and for which purpose(s)?</td>
<td>☐ No
☐ Yes - Please detail:

<table><tr><th>Name of Affiliate</th><th>Location/Jurisdiction</th><th>Purpose of Processing</th></tr><tr><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td></tr></table></td>
</tr>
<tr>
<td>9. Does your organization transfer or otherwise make available Personal Information to third party service providers? Why and for which purpose(s</td>
<td>☐ No
☐ Yes - Please detail:

<table><tr><th>Name of organization</th><th>Location/ Jurisdiction</th><th>Purpose of Processing</th></tr><tr><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td></tr></table></td>
</tr>
</table>

10. If you answered yes to Question 8 and/or 9, can you confirm that your organization has entered into an agreement ("**Subprocessing Agreement**") with each recipient organization listed above ("**Subprocessor**") specifying: (i) what Personal Information is being handled by the Subprocessor, including both information shared by the organization and any information collected directly by the Subprocessor on behalf of your organization or Dialogue; (ii) what specific rules, regulations and standards need to be complied with in the Processing of the information, including Applicable Privacy Legislation; (iii) the roles and responsibilities of your Subprocessor for the Processing of Personal Information, including responsibilities for specific functions, decision-making, safeguards and breach response; (iv) information security obligations; (v) acceptable uses of the information; (vi) retention and destruction obligations; and (vii) reporting and oversight arrangements to ensure compliance with the above, including reporting obligations in the case of a breach that could compromise the Personal Information?	☐ No ☐ Yes - If you are using a template Subprocessing Agreement, please provide a copy.
11. Are Subprocessors subject to a background check?	☐ No ☐ Yes

	- Organization who conducts the background check: [*insert details*] - How do you ensure that the background check is conducted: [*insert details*]
12. If you answered yes to Question 8 and/or 9 does your organization monitor compliance of its Subprocessor(s) with the Subprocessing Agreement(s)? How? At what frequency?	☐ No ☐ Yes - Means of monitoring: [*insert details*] - Frequency of monitoring: [*insert details*]
13. Does your organization monitor compliance with Applicable Privacy Legislation? How? At what frequency?	☐ No ☐ Yes - Means of monitoring: [*insert details*] - Frequency of monitoring: [*insert details*]
14. Does your organization monitor compliance with information security requirements? How? At what frequency?	☐ No ☐ Yes – Please describe the approach used to verify and maintain compliance with information security requirements (in relation to laws, regulations and security policies) and the roles and responsibilities related to compliance management.
SECURITY SAFEGUARDS	
Organisational Measures	

Questions	Answers
15. Who in your organization has access to Personal Information?	*[Indicate titles and approximate number of Personnel having access to Personal Information] and why they need to access the Personal Information]*
16. Are all Personnel accessing Personal Information bound by a contractual or statutory obligation of confidentiality?	☐ No ☐ Yes
17. Are all Personnel accessing Personal Information subject to background checks?	☐ No ☐ Yes - Background check process: [*insert details*] - Type of verification performed: [*insert details*] - Frequency of verification: [*insert details*]
18. Are all your organization's personnel trained on the privacy and information security aspects of the Services? Is this training regularly updated and carried out every year?	☐ No ☐ Yes - Please describe the privacy and information security training program and activities aimed at your Personnel: [*insert details*]
19. How is your organization managing information security risks?	*[Indicate the approach used to identify information security risks, the methodology used to assess the risks, and the roles and responsibilities related to risk management.]*
20. How is your organization managing third party information security risks?	*[Indicate the approach used to identify third party information security risks, the methodology used to assess the risks, and the roles and responsibilities related to risk management.]*

21. Have you implemented an internal privacy protection policy applicable to your Personnel that would protect Personal Information processed on behalf of Dialogue?	☐ No ☐ Yes
22. Have you implemented an information security policy applicable to your Personnel that would protect Personal Information processed on behalf of Dialogue?	☐ No ☐ Yes
23. Have you implemented a notification policy to Dialogue in the event of a Privacy Incident concerning Personal Information?	☐ No ☐ Yes – Please provide details about triggering events, timeline etc.:
24. Do you keep records of all Privacy Incidents, whether or not they concern Personal Information?	☐ No ☐ Yes
25. Have you implemented policies and procedures to handle answers to complaints and requests by individuals regarding the exercise of their privacy rights?	☐ No ☐ Yes
26. 27. Have you implemented policies and procedures to handle answers to requests from third parties and Regulators regarding access to Personal Information?	☐ No ☐ Yes

27. What is your organization's Personal Information retention policy? How long is Personal Information held before being erased or anonymized?	*[Insert details about the retention policy and timelines. If available, please enclose a copy of your retention policy. If the Personal Information managed under the Agreement is not subject to your retention policy (i.e. it is be deleted at the end of the Agreement, please indicate so.]*
28. Does your organization have processes in place for the major information security functions (access management, vulnerability management, security incident management, etc.)?	☐ No ☐ Yes – please describe the following processes - Access management (granting, revocation, periodic review of access): [*insert details*] - Firewall management: [*insert details*] - Security patch management: [*insert details*] - Vulnerability management: [*insert details*] - Privacy incident management: [*insert details*] - Backup management: [*insert details*]
Physical and Technical Measures	
Questions	**Answers**
29. Which systems/platforms/databases/applications are used by your organization to Process Personal Information?	*[List storage systems/platforms/databases/applications used e.g. proprietary servers hosted on premise; Microsoft Azure Cloud Services etc.]*
30. Where does your organization Process the Personal Information provided by Dialogue and/or that your	*[List location(s) where Personal Information is hosted and backed up/location of redundancy servers. If Personal Information is accessed remotely through Dialogue IT assets, please specify.]*

organization collects in the context of the Agreement?	
31. Does your organization encrypt Personal Information in transit and at rest?	☐ No ☐ Yes – Please describe the means implemented for ensuring the confidentiality of data stored (in the database, in flat files, backups, etc.), as well as the procedure for managing encryption keys (creation, storage, change in the event of suspected cases of data compromise, etc.). Describe the encryption means employed for data flows (VPN, TLS, etc.) implemented in the Processing.
32. Does your organization anonymize or de-identify Personal Information? How?	☐ No ☐ Yes – Please indicate here whether anonymization mechanisms are implemented, which ones and for what purpose.
33. How does your organization limit access by your Personnel to Personal Information (Logical access control)?	[*Indicate here whether users' profiles are defined and attributed, and describe the processes for access management (granting, revocation, periodic review of access). Specify the authentication means implemented for the various scenarios, if applicable (e.g. access to workstations, access to mobile devices, remote access to the corporate network, access by IT operators to IT resources, etc.). Where applicable, specify whether multi-factor authentication is used and the rules applicable to passwords (minimum length, required characters, validity duration, number of failed attempts before access to account is locked, inactivity period before session expires, password reset process, etc.).]*

34. How does your organization track access and use of Personal Information (Logging and alerts)?	*[Indicate here whether events are logged (e.g. authentication events, configuration changes, user transactions, access to Personal Information, etc.), whether each event/action logged is attributable to a unique individual, how long these traces are stored for, and the procedures applied during alerts raised.]*
35. What measure has your organization implemented to protect against the compromise of Personal Information and IT Assets? (Integrity monitoring)	*[Indicate here whether mechanisms are implemented for integrity monitoring of stored data and IT Assets, which ones (e.g. SIEM, IDS, etc.), for what purpose (e.g. brute force attack, DDoS, etc.) and the procedures applied during alerts raised. Specify which integrity control mechanisms are implemented on data flows.]*
36. What physical and technical measures has your organization implemented to secure your networks?	*[Indicate here whether, and if so what, technical security controls are implemented to protect networks (e.g. firewall, network segmentation, micro-segmentation, NAC, NIDS/NIPS, SIEM, Web security gateway, anti-virus gateway, multi-factor authentication, etc.)* *Indicate here whether, and if so what, physical and environmental security controls are implemented to protect the network infrastructure (e.g. physical access control, video surveillance, intrusion detection, temperature control, fire protection, power supply, etc.)]*
37. What measures has your organization implemented to secure workstations and mobile devices?	*[Indicate here whether, and if so what, security controls are implemented to protect workstations and mobile devices (e.g. antivirus, host-based firewall, hard disk encryption, desktop management, MDM, MCM, etc.)]*

38. What measures has your organization implemented to secure the premises where Personnel work?	*[Indicate here whether, and if so what, physical security controls are implemented to protect your organization's premises (e.g. physical access control, video surveillance, intrusion detection, etc.)]*
39. How does your organization dispose of Personal Information?	*[Indicate here the processes followed to destroy or erase Personal Information in electronic or paper format, and the means of disposal.]*
40. Does your organization hold any current certification(s) for compliance with privacy industry standards (e.g. ISO/IEC 27001; SOC 2 etc.)?	☐ No ☐ Yes - Please attach your organization's most recent certificate(s).
41. Does your organization comply with cybersecurity standards or recognized security frameworks (e.g. ISO/IEC 27001, NERC, NIST CSF, Tier III (Uptime Institute) or equivalent, etc.)?	☐ No ☐ Yes – For each standard/framework, please indicate: - Name of standard/framework: - Description of the standard/framework and how it affects security measures: [*insert details*]
42. Is your organization periodically audited by an independent third party for compliance with privacy or information security standards (e.g. SOC 2 Type II or equivalent security audit)?	☐ No ☐ Yes – Please attach your organization's most recent audit report, and specify: - Type of audit: - Frequency of audits: - Date and scope of the last audit: - Remediation status of the security defects identified during the last audit:

43. Does your organization continuously monitor and maintain the effectiveness of the security controls implemented in its organization?	☐ No ☐ Yes - Please provide description of the approach used to verify, evaluate and maintain the effectiveness of the security controls implemented (e.g. software updates, security patches, etc.): [*insert details*]

List of documents provided by Service Provider:

- [*Insert list*]

APPENDIX B

DATA PROTECTION ADDENDUM

This Data Protection Addendum ("**Addendum**") is entered between Dialogue Health Technologies Inc. ("**Company**") and **[*Insert the full name of the legal entity providing the services*]** ("**Service Provider**"). This Addendum applies to the collection, use, disclosure, storage and any other types of processing (collectively "**processing**") of personal information or personal health information by the Service Provider on behalf of the Company ("**Company Personal Information**") in order to perform services **[*insert types of services*]** ("**Services**") to the Company pursuant to the agreement **[*insert title and date of service agreement or details on the verbal agreement*]** ("**Agreement**") between the parties. Schedule A sets out the details of the processing under this Addendum.

The parties agree as follows:

1. **Compliance with Data Protection Laws.** Each of the Company and Service Provider shall comply with applicable Canadian federal and provincial laws governing the processing of personal information and/or, as the case may be, personal health information ("**Data Protection Laws**"). The Service Provider shall further comply with (i) the Company's policies and procedures pertaining to the processing of Company Personal Information that may be transferred, communicated or otherwise made available by the Company to the Service Provider from time to time; and (ii) all applicable industry standards concerning privacy, data protection, confidentiality or information security.
2. **Purpose limitation; control and custody**. Any processing of Company Personal Information by the Service Provider shall be limited to what is necessary to provide the Services or such other purposes expressly authorized by the Company. If applicable, health service providers that are custodians of personal health information under applicable Data Protection Laws ("**Custodians**") remain ultimately accountable for complying with such Laws and for ensuring the protection of personal health information under their control or custody.
3. **Sub-processors**. The Company authorizes the Service Provider to appoint sub-processors to process Company Personal Information on its behalf. A list of sub-processors (including third parties and Service Provider's affiliates) is included in Schedule A. The Service Provider shall give the Company prior notice of the appointment of a sub-processor, including the details of the processing to be undertaken by the sub-processor. The Service Provider shall ensure that the arrangement between the Service Provider and the sub-processor is governed by a written contract which offers at least the same level of protection for Company Personal Information as those set out in this Addendum. The Service Provider shall be solely responsible for all actions and omissions of those third parties.
4. **Cross-border Transfers.** The Service Provider may only process, and shall ensure that sub-processor only processes, Company Personal Information in Canada. The Service

Provider shall obtain the Company's written authorization before processing Company Personal Information outside of Canada.

5. **Data Subjects' Requests under Data Protection Laws**. If a Service Provider receives an individual's request regarding Company Personal Information under Data Protection Laws, it shall promptly inform the Company and provide all relevant information to the Company. The Service Provider shall promptly comply with the Company's instructions relating to responding to an individual's request regarding the Company Personal Information under Data Protection Laws.

6. **Notice of Process**. In the event that the Service Provider receives a governmental or other regulatory request for any Company Personal Information, it agrees to immediately notify the Company to allow the Company to have the option to defend such action. The Service Provider shall reasonably cooperate with the Company in such defence.

7. **Data Security Program.** The Service Provider shall maintain a comprehensive, written information security program that contains administrative, technical, and physical safeguards that are appropriate to (a) the size, scope and type of the Service Provider's business; (b) the type and sensitivity level of information that Service Provider will process; and (c) the need for security and confidentiality of such information ("**Security Program**"). The Service Provider's Security Program shall include the measures detailed under Schedule B and be designed to: (a) protect the confidentiality, integrity, and availability of the Company Personal Information in the Service Provider's possession or control or to which the Service Provider has access; (b) protect against any anticipated threats or hazards to the confidentiality, integrity, and availability of the Company Personal Information; (c) protect against unauthorized or unlawful access, use, disclosure, alteration, or destruction of the Company Personal Information; (d) protect against accidental loss or destruction of, or damage to, Company Personal Information; and (e) safeguard Company Personal Information in accordance with Data Protection Laws.

8. Data Incidents

8.1. Informing Company of Data Incident. The Service Provider shall immediately notify the Company of any reasonably suspected or actual unauthorized access to, use, loss or disclosure of Company Personal Information ("**Data Incident**"). While the initial phone notice may be in summary form, a comprehensive written notice shall be given within 48 hours to the Company. The notice shall summarize, in reasonable detail, the nature and scope of the Data Incident (including each Company Personal Information element, if any) and the corrective action already taken or to be taken by the Service Provider. The notice shall be timely supplemented with the details reasonably requested by the Company, inclusive of relevant forensic reports. The Service Provider shall promptly take all necessary and advisable corrective actions, and shall cooperate fully with the Company in all reasonable efforts to mitigate the adverse effects of Data Incident and to prevent its recurrence.

8.2. Notice of Data Incident. The parties will collaborate on whether any notice of the Data Incident is required to be given to any person, and if so, the content of that notice. The Service Provider will bear all costs of the notice.

9. Privacy Impact Assessments. If the Services involve processing Company Personal Information that requires the Company to conduct a privacy impact assessment or any similar assessment or periodic reassessment that the Company considers to be required under applicable Data Protection Laws, including any acquisition, development or overhaul of an information system or electronic service delivery system involving the collection, use, disclosure, retention or destruction of Company Personal Information, the Service Provider agrees to cooperate fully and promptly with the Company in conducting any such assessment or reassessment and implementing any reasonable measures the parties deem appropriate to mitigate any potential privacy or data security risks identified by the Company as a result of the assessment or reassessment so as to ensure that the Company complies with its obligations under applicable Data Protection Laws (including any applicable data subject rights) at all times. The Company may also request the Service Provider to provide it with a copy of any impact assessment it would already have conducted regarding its Services.

10. Liability and Indemnification

10.1. No Limitation of Liability. Any limitation of liability set forth in the Agreement shall not apply to the Service Provider's indemnity obligations under this Addendum and to the Service Provider's liability arising from its breach of any obligation under this Addendum, including in the case of any claims, demands, actions or proceedings brought against the Company as a result of the Service Provider's breach of any obligation under this Addendum.

10.2. Indemnification. Any clause in the Agreement with respect to indemnification shall extend to any claims, demands, actions or proceedings brought against the Company as a result of the Service Provider's breach of any obligation under this Addendum. In the absence of such indemnification clause in the Agreement, the Service Provider shall indemnify and hold the Company harmless against any claims, demands, actions or proceedings brought against the Company as a result of the Service Provider's breach of any obligation under the Addendum; for the sake of clarity, this indemnification shall include, but not be limited to, any breach of this Addendum resulting from the actions or omissions of a third party to whom the Service Provider has transferred Company Personal Information under Section 3 of this Addendum.

11. Security Review and Audit

11.1. At the Company and/or Custodians request, the Service Provider will provide copies of its data privacy and security policies and procedures including the Security Program that apply to the Company Personal Information. Subject to reasonable notice, the Service Provider shall provide the Company and/or Custodians an opportunity to conduct a privacy and security audit of the Service Provider's Security Program, systems and procedures that are applicable to the Company Personal Information. Such audit may be conducted on-site, by

the Company personnel and/or Custodians or the Company and/or Custodians contracted third party assessors, or through surveys and interviews, at the option of the Company and/or Custodians.

11.2. In the event the Service Provider has any security audits or reviews of its own systems performed by the Service Provider or a third party, including vulnerability and penetration assessments, it will give the Company and/or Custodians notice of any findings that are likely to adversely impact the Company Personal Information, and will keep the Company and/or Custodians timely informed of its remediation efforts.

12. Interpretation, Termination and Secure Disposition

12.1. This Addendum shall be an integral part of the Agreement and constitute, with the Agreement, the entire agreement between the parties with respect to the subject matter thereof, and any prior representations, statements, and agreements relating thereto are superseded by the terms of the Agreement. In the event of any inconsistencies between the provisions of this Addendum and any other agreements between the parties, including the Agreement, this Addendum shall take precedence over the Agreement or any other agreements.

12.2. The Company may terminate the Agreement with cause immediately upon notice to the Service Provider if the Service Provider has materially breached this Addendum and the Company has given at least thirty (30) days' notice of such breach (such notice to specify the reasonable particulars thereof) during which notice period the Service Provider has not remedied its breach.

12.3. The Service Provider shall either securely return or dispose of all Company Personal Information under its possession or in the possession of any third party to whom it transferred Company Personal Information upon termination of the Agreement or upon the Company's instructions following the Service Provider's breach of any provision of this Addendum. Any such disposal must ensure that Company Personal Information wherever located is rendered permanently unreadable and unrecoverable. Upon reasonable notice and if requested by the Company, the Service Provider shall provide the Company a certification of compliance with this section by an authorized officer.

12.4. Provisions in this Addendum that are intended to survive termination will continue in full force and effect after the termination of this Addendum.

[Signature page follows]

IN WITNESS WHEREOF The Company and the Service Provider have executed this Addendum attested to by the signatures of their duly authorized officers in that behalf as of the day and year set out above.

Dialogue Health Technologies Inc.

By:

Name:
Title:
Date:

[*INSERT FULL SERVICE PROVIDER'S LEGAL NAME*]

By:

Name:
Title:
Date:

SCHEDULE A

DETAILS OF THE PROCESSING

1. **Categories of individuals**

The Company Personal Information concern the following categories of individuals, such as member, dependant, user, contractor, employee or professional (please specify):

[ ]

2. **Categories of personal information**

The Company Personal Information concern the following categories of data (please specify):

[ ]

3. **Service Provider**

Service Provider's details (name, reg. no, address, contact details)	**Processing activities**	**Processing/storage location (address)**

4. **Sub-processors**

Details (name, reg. no, address, contact details)	**Processing activities**	**Processing/storage location (address)**

SCHEDULE B

SECURITY PROGRAM MINIMUM REQUIREMENTS

Without limiting the generality of the foregoing, the Service Provider's Security Program must include at the very minimum:

(a) **Security Awareness and Training.** A mandatory security awareness and training program for all members of the Service Provider's workforce (including management), which includes: (i) training on how to implement and comply with its Security Program; and (ii) promoting a culture of security awareness through periodic communications from senior management with employees.

(b) **Background Assessment and Monitoring.** Policies and procedures to conduct background assessments for all current and prospective members of the Service Provider's workforce who have access to Company Personal Information including criminal background verification procedures to the extent allowed under applicable law. Such assessments shall be performed annually to ensure members of the Service Provider's workforce continue to comply with applicable standards and requirements related thereto.

(c) **Access Controls.** Policies, procedures, and logical controls: (i) to limit access to its information systems and the facility or facilities in which they are housed to properly authorized persons with a genuine need-to-know; (ii) to ensure that the least amount of Company Personal Information is made accessible to authorized persons as required to carry out their job-related functions; (iii) to prevent those workforce members and others who should not have access from obtaining access; and (iv) to remove access in a timely basis in the event of a change in job responsibilities or job status or as a result of a failed background assessment. These policies, procedures and logical controls include the use of multi-factor authentication and the implementation of a password policy guaranteeing that passwords are periodically updated and are of a reasonable level of complexity.

(d) **Physical and Environmental Security.** Controls that provide reasonable assurance that physical access to facilities where Company Personal Information is stored, including physical servers, is limited to properly authorized individuals and that environmental controls are established to detect, prevent and control destruction due to environmental extremes. These controls include: (i) logging and monitoring of unauthorized access attempts to the Service Provider's facilities by security personnel; (ii) camera surveillance systems at critical internal and external entry points of the Service Provider's facilities; (iii) systems that monitor and control the air temperature and humidity at appropriate levels for the computing equipment; and (d) Uninterruptible Power Supply (UPS) modules and backup generators that provide back-up power in the event of an electrical failure.

(e) **Data Incident Procedures**. A data incident response plan that includes procedures to be followed in the event of any actual or reasonably suspected Data Incident. Such procedures include: (i) formation of an internal incident response team with a response leader; (ii) assessing the risk the incident poses and determining who may be affected; (iii) internal reporting as well as a notification process in the event of unauthorized disclosure of Company Personal Information; (iv) keeping a record of what was done and by whom to help

in later analysis and possible legal action; and (v) conducting and documenting root cause analysis and remediation plan.

(f) **Contingency Planning.** Policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, pandemic flu, and natural disaster) that could damage Company Personal Information or production systems that contain Company Personal Information. Such procedures include: (i) a policy for performing periodic backups of production file systems and databases containing Company Personal Information, according to a defined schedule; (ii) a formal disaster recovery plan for the Service Provider's facilities where Company Personal Information is stored, including requirements for the disaster plan to be tested on a regular basis and a documented executive summary of the Disaster Recovery testing, at least annually, which is available upon request to the Company; (iii) a formal process to address the framework by which an unplanned event might be managed in order to minimize the loss of vital resources.

(g) **Audit Controls.** Hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic information. Such mechanisms must ensure that actions are attributable to an identifiable individual.

(h) **Data Integrity.** Policies and procedures to ensure the confidentiality, integrity, and availability of Company Personal Information and protect it from disclosure, improper alteration, or destruction.

(i) **Storage and Transmission Security.** Security measures to guard against unauthorized access to Company Personal Information that is being transmitted over a public electronic communications network or stored electronically. Such measures include (i) limiting the use of portable storage devices, such as USB (Universal Serial Bus) drives, to store or transfer Company Personal Information to the extent demonstrably necessary to fulfill a specific and documented purpose; (iii) anonymization and pseudonymization where this does not prevent the performance of the Services; and (iv) encryption during transmission.

(j) **Segmentation.** Measures ensuring the segmentation of Company Personal Information from data of others.

(k) **Assigned Security Responsibility.** Assigning responsibility for the development, implementation, and maintenance of its Security Program, including: (i) designating a security official with overall responsibility; and (ii) defining security roles and responsibilities for individuals with security responsibilities.

(l) **Testing.** Periodically testing the key controls, systems and procedures of its Security Program to validate that they are properly implemented and effective in addressing the threats and risks identified. Such testing shall be conducted at least annually by qualified independent parties. Where applicable, such testing includes: (i) internal risk assessments; (ii) ISO 27001 and ISO 27018 certifications; and (iii) Service Organization Control 1 (SOC1) and Service Organization Control 2 (SOC2) audit reports (or industry-standard successor reports);

(m) **Logging and Monitoring.** Network and systems monitoring, including error logs on servers, disks and security events for any potential problems. Such monitoring includes: (i) reviewing changes affecting systems handling authentication, authorization, and auditing; (ii) reviewing privileged access to the Service Provider's production systems; and (iii) engaging third parties to perform network vulnerability assessments and penetration testing on a regular basis.

(n) **Change and Configuration Management.** Maintaining policies and procedures for managing changes the Service Provider makes to production systems, applications, and databases. Such policies and procedures must include: (i) a process for documenting, testing and approving the patching and maintenance of the Service; (ii) a security patching process that requires patching systems in a timely manner based on a risk analysis; and (iii) a process for the Service Provider to utilize a third party to conduct web application level security assessments.

(o) **Program Adjustments.** The Service Provider must monitor, evaluate, and adjust, as appropriate, the Security Program in light of: (i) any relevant changes in technology and any internal or external threats to the Service Provider or the Company Personal Information; (ii) security and data privacy regulations applicable to the Company and/or the Service Provider; and (iii) The Service Provider's own changing business arrangements, such as mergers and acquisitions, alliances and joint ventures, outsourcing arrangements, and changes to information systems.

(p) **Devices.** All laptop and desktop computing devices utilized by the Service Provider and any subcontractors when accessing Company Personal Information must: (i) be equipped with a minimum of AES 128 bit full hard disk drive encryption; (ii) have up to date virus and malware detection and prevention software installed with virus definitions updated on a regular basis; and (iii) maintain virus and malware detection and prevention software so as to remain on a supported release. This shall include, but not be limited to, promptly implementing any applicable security-related enhancement or fix made available by the supplier of such software.