Dialogue

Dialogue Incident Response Plan

Version: 2.5
Date of last revision: October 3rd, 2024

CONFIDENTIAL

1. Introduction

1.1 Application:

This Incident Response Plan (this "**Plan**") applies to all incidents and events that constitute or might constitute a **Data Security Incident** (defined below) regarding **Data** (defined below) in the possession or control of Dialogue Health Technologies Inc. ("Dialogue").

1.2 Purpose of Plan:

This Plan is a critical component of Dialogue's Incident Management Program, the Requirements of which are set out in Attachment A below.

a. This Plan is designed to enable Dialogue to appropriately respond to and recover from a Data Security Incident, assess and mitigate the business and legal risks resulting from a Data Security Incident, comply with legal obligations relating to a Data Security Incident, and take appropriate measures to prevent the same or similar Data Security Incidents in the future.

1.3 Activation of Plan:

Dialogue's Incident Reporting and Plan Activation Guidelines (see Attachment B) explain how incidents, breaches or threats (or possible incidents, breaches or threats) must be reported and outlines the process to determine whether an incident or event will be considered a Data Security Incident that activates this Plan.

1.4 Key Definitions:

In this Plan:

"**Cell Leader(s)**"	means the individual(s) assigned to lead a specific sub-team of the Team regarding a Data Security Incident. See Incident Response Team Contact List.
"**CTO**"	means Dialogue's Chief Technology Officer.
"**PO**"	means Dialogue's Privacy Officer.
"**Data**"	means **any kind of written, printed or electronic documents, records or data** (including Personal Information and other data about Dialogue's business, employees, members/clients and service delivery partners) that is owned by, or in the possession or control of, Dialogue. Data may be stored/recorded by Dialogue on paper records or in local or cloud IT systems (e.g. servers, personal computers/laptops, mobile devices and portable storage media), or transferred by Dialogue to a service provider (including a cloud service provider) for processing or storage.
"**Data Security Incident**"	means **any loss of, unauthorized access to, or unauthorized use, disclosure or deletion of, Data** or any other unauthorized activity or event that **adversely affects the confidentiality, availability, integrity or security of Data** (including unauthorized changes, copying, deleting, removing or transferring of Data). For example, a Data Security Incident may include a stolen or lost device or paper file, an attack on an IT system by a cybercriminal, a misdirected email or postal mail, a mistaken disclosure of data to an unauthorized recipient, or the deletion of data resulting from a hardware failure or an operational break-down. For the purpose of this Plan, newly identified vulnerabilities and/or near misses shall also constitute Data Security Incidents requiring the same procedural response. A Dedata Security Incident also includes a Privacy Incident.
"**Legal Representative**"	means a lawyer (from Dialogue's Legal Department or outside legal counsel) assigned to provide legal advice regarding a Data Security Incident.

"**Personal Information**"	Refer to Appendix A of the Internal Privacy Policy for the Glossary of Terms.
"**Team**"	means the incident response team assigned to a Data Security Incident, as outlined in the Incident Response Team Contact List (see Attachment C).

1.5 **Sound Judgment:**

This Plan sets out a multi-step process for assessing, responding to and learning from Data Security Incidents. Each of those steps might not be suitable for every Data Security Incident. The CTO and Cell Leader(s), with advice from the Legal Representative, must exercise sound judgment when executing this Plan for each Data Security Incident.

1.6 **Other Plans:**

A Data Security Incident might also constitute another kind of incident (e.g. a physical security/safety incident or disaster, minor Clinical Quality, MedOps incident) that is governed by another written response plan. In those circumstances, the response to the Data Security Incident must be a coordinated effort by the relevant response teams, and any conflict between the plans must be resolved by the relevant cell leaders including implementation of the **Privacy Breach Response Procedure**.

1.7 **Confidentiality – Internal Disclosures:**

All information regarding a Data Security Incident must be kept strictly confidential within the Team, and must not be disclosed outside the Team to any other Dialogue employee except on a need-to-know basis if and when a Dialogue employee has been assigned to assist the Team to respond to the Data Security Incident or in accordance with the procedures set out in section 3.6 below.

1.8 **Confidentiality – External Disclosures:**

Information regarding a Data Security Incident must not be disclosed to any person outside Dialogue, including any vendor or service provider, except on a need-to-know basis with the prior approval of the CTO or the relevant Cell Leader(s) after consultation with the Legal Representative or in accordance with the notification/inquiry procedures set out in section 3.6 below.

1.9 **Timing and Triage:**

This Plan must be executed as quickly as reasonably possible for each Data Security Incident. If there are insufficient resources to immediately respond to all Data Security Incidents in accordance with this Plan, then the Data Security Incidents must be handled on a relative priority basis based on an assessment of all relevant circumstances (e.g. the cause, nature, extent and severity of the Data Security Incidents, the resulting risks to Dialogue, its clients/members and other organizations, and the need to comply with legal reporting and notification obligations). Prioritization decisions must be made by the CTO and/or Cell Leader(s) after consultation with the Legal Representatives responsible for the Data Security Incidents.

1.10 **No Change to Plan:**

This Plan must not be modified in any way without the prior written approval of the CTO after consultation with the Legal Representative.

This Plan is reviewed by the Team at least annually. The Plan and any changes to the Plan have been or will be distributed to the Team and appropriate stakeholders.

2. Incident Response Team

2.1 **Responsibility:**

The Team assigned to a Data Security Incident is responsible for the execution of this Plan regarding the Data Security Incident. The CTO and Cell Leaders have overall responsibility for the performance of the Team and compliance with this Plan regarding the Data Security Incident.

2.2 **Team Members:**

The Incident Response Team Contact List lists the Dialogue employees and external consultants/advisors who are available to be appointed to the Team for a Data Security Incident, and their respective areas of expertise and potential roles and responsibilities. The initial Cell Leader(s) for each reported Data Security Incident will be automatically designated as set out in the Incident Response Team Contact List. Subject to section 2.3, the CTO and/or the applicable Cell Leader(s) must determine size and composition of the Team for a Data Security Incident in light of the cause, nature, extent and severity of the Data Security Incident.

b. All individuals Dialogue expects to sit on the Team will be familiar with this Plan and trained in incident response best practices and will periodically participate in scenario-based exercises with a view to developing and documenting learnings about anticipated scenarios in a "Playbook". The CTO will maintain the Playbook and an up-to-date contact list for these individuals that supports rapid, off-hours contact.

2.3 **Required Team Members – Legal and Privacy:**

Each Team must include a Legal Representative. If a Data Security Incident involves (or might involve) Personal Information, then the Team for that Data Security Incident must include Dialogue's Privacy Officer (PO) and/or delegate.

2.4 **Additional/Replacement Team Members:**

The CTO and/or applicable Cell Leader(s) may designate other Dialogue employees or external consultants/advisors (subject to sections 1.8 and 2.6) as additional members of a Team or as replacements for existing Team members. Each of those additional or replacement Team members must comply with this Plan.

2.5 **Other Dialogue Employees:**

A Team member may request the assistance of Dialogue employees to perform specific tasks under the direct supervision of the Team member, but those employees will not be members of the Team (unless approved by the CTO and/or the applicable Team Leader(s)). (Please note the confidentiality requirements in section 1.7).

2.6 **External Consultants/Advisors:**

An external consultant or advisor may not be engaged to assist a Team, or assigned to a Team, without the express, prior approval of the CTO or the applicable Cell Leader(s) after consultation with the Legal Representative or another member of Dialogue's Legal Department and consideration of applicable insurance requirements and benefits. All external consultants and advisors must be engaged by Dialogue pursuant to a written agreement that includes appropriate confidentiality and legal privilege provisions and is reviewed and approved by the Legal Representative or another member of Dialogue's Legal Department.

c. Dialogue has retained insurer-approved external legal and technical experts and has a protocol for engaging them without delay should external assistance be required.

2.7 **Protocols**

(a) Team Communications:

When executing the Discovery, Containment, Remedy/Recovery and Investigation elements of this Plan, all members of the Team must communicate with each other using designated procedures (e.g. secure war room) in accordance with the Team Communications Protocol (see Attachment D). The Team Communications Protocol is designed to facilitate execution of this Plan by preserving the security and confidentiality of communications among Team members.

(b) **General Communications:**

When executing any element of this Plan, all communications from any Team member to any person who is not a Team member must conform to the General Communications Protocol (see Attachment E). For example, the General Communications Protocol applies to communications

with other Dialogue employees (not Team members), law enforcement, regulators and other businesses and organizations.

(c) **Evidence and Record Keeping:**

When executing the Discovery, Containment, Remedy/Recovery and Investigation elements of this Plan, each member of the Team must create time-stamped records of their activities and findings in accordance with the Evidence and Record Keeping Protocol (see Attachment F). Accurate and complete records are essential for proper execution of this Plan and may be required for legal compliance purposes and as evidence in legal proceedings. Any questions or concerns regarding evidence must be immediately directed to the CTO or the Legal Representative.

2.8 **Availability:**

Each Team, represented by at least one person, is reachable to ensure 24/7/365 response. Team members may delegate their responsibility when they are not available.

2.9 **Compensation for incident response outside working hours**

Dialogue acknowledges the significance of maintaining a healthy work-life balance. However, we recognize that there are instances where overtime becomes unavoidable. In the event of an incident, if an employee is reached by telephone outside of Dialogue regular office hours, and must respond to that incident, they are entitled to overtime compensation as follows:

1. Overtime earned will be recorded based on each completed fifteen minutes.
2. An employee who is required to work overtime shall receive compensation at time and one half for the overtime worked (1.5X).
3. Overtime shall be compensated in cash except where, upon request of an employee and with the approval of their manager, overtime may be compensated on the equivalent time off with pay.
4. Any compensatory leave credits earned in a fiscal year and not taken by the end of the fiscal year will be paid in cash.

3. Incident Response Procedure

The procedure for responding to a Data Security Incident is comprised of the following steps outlined below:

- Discovery;
- Containment;
- Remedy/Recovery;
- Investigation;
- Risk Assessment;
- Reporting/Notifications and Communications;
- Post-Incident Review; and
- Final Reports and Records.

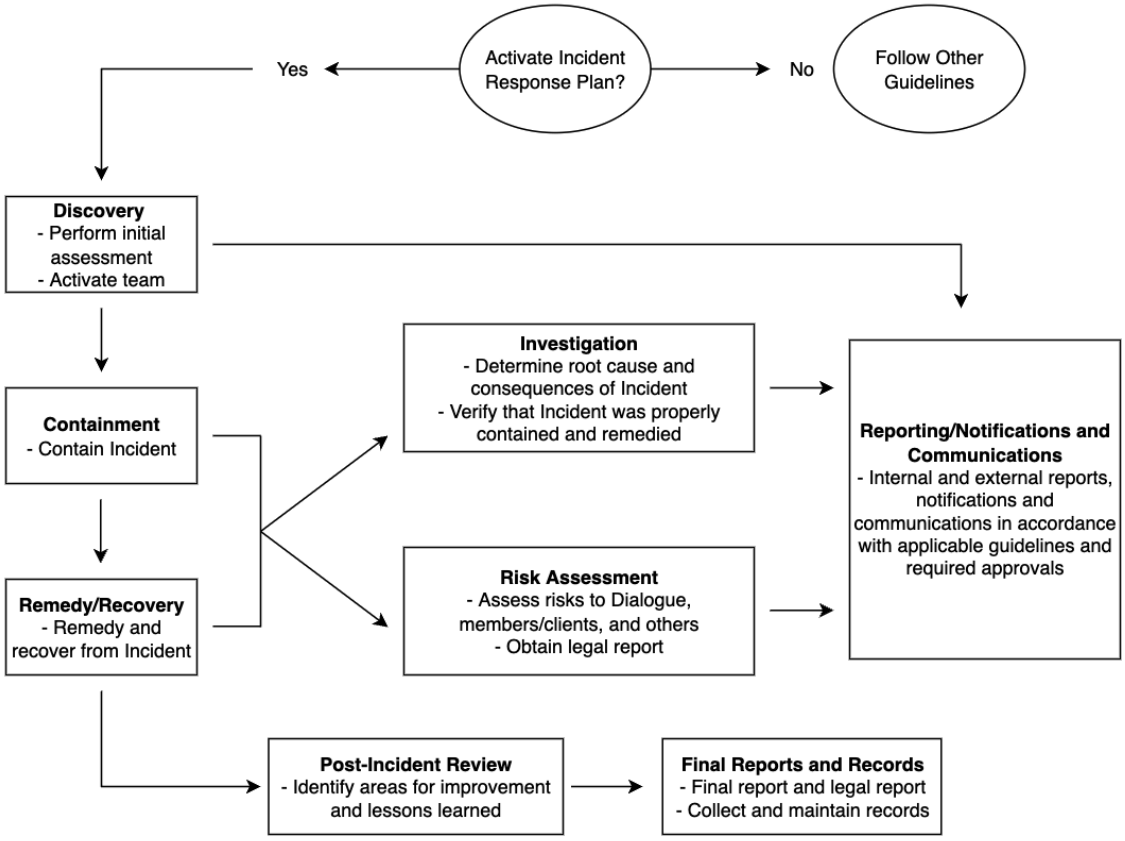
The initial steps – Discovery, Containment and Remedy/Recovery – must be performed as quickly as practicable in the circumstances and either simultaneously or in quick succession.

Investigation and Risk Assessment should be performed after Containment. Post-Incident Review and Final Reports and Records should be performed after Investigation is completed.

Reporting/Notifications and Communications must be performed throughout the incident response process.

Team members, with guidance and instructions from the Cell Leader(s) and the CTO, must exercise reasonable judgment to determine how each step will be executed in the particular circumstances of a Data Security Incident.

Each step (summarized below) may be supplemented with additional guidelines and procedures for specific circumstances published by the CTO.



3.1 Discovery (Initial Assessment and Team Activation)

Timing: Immediately after this Plan is activated for a Data Security Incident.

This step involves an **immediate** initial assessment of the Data Security Incident (including attempting to identify the root cause of the Incident), assignment of an appropriate Team and other appropriate immediate action.

- □ **Initial Assessment:** The TechOps Cell must immediately gather initial, basic information regarding the cause, nature, extent and severity of the Data Security Incident to enable the TechOps Cell Leader to determine the appropriate initial response to the Data Security Incident and the priority of the response (relative to other current Data Security Incidents).
- □ **Team Activation:** Based on the TechOps Cell Leader's initial assessment of the Data Security Incident, the TechOps Cell Leader must immediately activate an appropriate core Team to respond to the Data Security Incident. (External consultants and advisors must be engaged with the assistance of the Legal Representative in accordance with section 2.6.)
- □ **Team Communications:** The TechOps Cell Leader and/or CTO must determine whether to prohibit the use of specific communications systems/services (e.g. systems/services affected or possibly affected by the Data Security Incident) by Team members, and give appropriate instructions to Team members.
- □ **Team Meeting:** The CTO must organize an initial meeting (in person or virtual) of the Team, in accordance with the Team Communications Protocol, to discuss the Data Security Incident and the required initial response.
- □ **Internal Escalation:** Based on the CTO's initial assessment of the Data Security Incident, the CTO with advice from the Legal Representative must determine whether to notify the Executive Leadership Team and Board (if appropriate) about the Data Security Incident in accordance with the Escalation Response - IT Incident Preparedness Protocol.
- □ **Notifications:** Based on the Legal&Comms Cell's initial assessment of the Data Security Incident, the Legal&Comms Cell Leader must consider whether immediate internal notifications (e.g. to Dialogue employees/custodians) or external notifications (e.g. to members/clients, insurers, law enforcement, service providers or other organizations) are required, and must provide required information and advice to the CTO and the Legal Representative for action in accordance with the notification/inquiry procedures in section 3.6 below.
- □ **Evidence:** Cell Leaders must collect, protect and preserve all initial evidence the Cell Leaders obtain (directly and indirectly from other Team members) regarding the Data Security Incident in accordance with the Evidence and Record Keeping Protocol. Cell Leaders must immediately create a new record retention file for the Data Security Incident in accordance with the Evidence and Record Keeping Protocol.
- □ **False Alarms:** If the TechOps Cell Leader's initial assessment of a Data Security Incident is that the Data Security Incident is a false alarm (i.e. newly identified vulnerability, near miss, etc.), then an investigation (with appropriate monitoring) must be conducted to verify the initial assessment (see section 3.4), a brief post-incident review must be conducted (see section 3.7) and a final report must be delivered (see section 3.8).

3.2 Containment

Timing: Immediately after this Plan is activated for a Data Security Incident.

This step involves **immediate** containment of the Data Security Incident to limit/prevent harm.

- □ **General Rule:** Unless the CTO or the TechOps Cell Leader expressly instructs otherwise based on exceptional circumstances (discussed below), the TechOps Cell must take all necessary measures to **immediately contain** the Data Security Incident (e.g. stopping unauthorized activities, disconnecting or isolating affected systems or devices, and suspending compromised access credentials) and collect and preserve evidence of the Data Security Incident in accordance with the Evidence and Record Keeping Protocol.

- **Exceptional Circumstances:** In exceptional circumstances (determined by the CTO or the TechOps Cell Leader) it might be appropriate to **not** stop unauthorized activities that do not present a risk of imminent harm in order to not compromise the investigation of the Data Security Incident. Only the CTO or the TechOps Cell Leader can determine that exceptional circumstances apply and can give appropriate instructions.
- **Specific Procedures:** The containment activities should include compliance with applicable written Playbooks for specific kinds of Data Security Incidents published.
- **Internal Assistance:** The CTO or the TechOps Cell Leader must identify the individuals within Dialogue who are required to assist with the response to the Data Security Incident, and must communicate with those individuals in accordance with the Team Communications Protocol.
- **Internal Escalation:** The CTO, based on information provided by the Cell Leader(s) and after consultation with the Legal Representative, must determine whether to report the Data Security Incident to the Executive Leadership Team and the Board (if appropriate) in accordance with the Escalation Response - IT Incident Preparedness Protocol.
- **Reporting:** TechOps Cell members must immediately report to the TechOps Cell Leader the results of their containment activities and any additional information about the Data Security Incident that might challenge the then-current assessment of the cause, nature, extent or severity of the Data Security Incident.
- **Reassessment:** During the containment activities, the TechOps Cell Leader and/or CTO must reassess the Data Security Incident based on information reported by the TechOps Cell, and working with the Legal & Comms Cell take appropriate action (e.g. internal notifications/inquiries and changes/additions to Team composition) if there is a material change in the assessment of the cause, nature, extent or severity of the Data Security Incident.
- **Evidence and Record Keeping:** Each Team member must collect, protect and preserve all evidence of the Data Security Incident in accordance with the Evidence and Record Keeping Protocol. Team members must be careful to not inadvertently modify or destroy evidence (e.g. log files) that might be important to the investigation and assessment of the Data Security Incident or necessary to enable appropriate corrective action. Each Team member must create records of their containment activities as they perform the activities.
- **Monitoring:** If the Data Security Incident involves a compromised IT system or equipment (e.g. network, server, personal computer/laptop or mobile device), then the Team must monitor the IT system or equipment, and related systems and equipment, until the investigation of the Data Security Incident (section 3.4).

3.3 Remedy/Recovery

Timing: As soon as possible after the Data Security Incident is discovered.

This step involves taking measures required to remedy and recover from the Data Security Incident and to restore operations affected by the Data Security Incident. In addition, the CTO and Legal Representative must begin assessing legal reporting/notification obligations and other communications considerations.

- **General Rule:** Unless the CTO or the TechOps Cell Leader expressly instructs otherwise based on exceptional circumstances (discussed below), the TechOps Cell must take all necessary measures to **promptly** remedy the cause of the Data Security Incident (e.g. deleting malware from an infected computer or device, correcting security weaknesses, deleting compromised access credentials or restoring production data from backup systems) and prevent similar incidents.
- **Exceptional Circumstances:** In exceptional circumstances (determined by the CTO or the TechOps Cell Leader) it might be appropriate to **not** perform certain remedial activities in order to not compromise the investigation of the Data Security Incident. Only the CTO or the TechOps Cell Leader (after consultation with the CTO) can determine that exceptional circumstances apply and can give appropriate instructions.

- **Evidence and Record Keeping:** Each TechOps Cell member must collect, protect and preserve all evidence of the Data Security Incident in accordance with the Evidence and Record Keeping Protocol. Team members must be careful to not inadvertently modify or destroy evidence (e.g. log files) that might be important to the investigation and assessment of the Data Security Incident. Each Team member must create records (in accordance with the Evidence and Record Keeping Protocol) of their remedy/recovery activities as they perform the activities.

- **Reporting:** The TechOps Cell members must immediately report to the TechOps Cell Leader the results of their remedy/recovery activities and any additional information about the Data Security Incident that might challenge the then-current assessment of the cause, nature, extent or severity of the Data Security Incident.

- **Reassessment:** During the remedy/recovery activities, the TechOps Cell Leader and/or CTO must reassess the Data Security Incident based on information reported by the TechOps Cell, and working with the Legal & Comms Cell take appropriate action (e.g. internal escalation, notifications/inquiries and changes to Team composition) if there is a material change in the assessment of the cause, nature, extent or severity of the Data Security Incident.

- **Reporting/Notifications:** During the remedy/recovery activities, the CTO, Legal & Comms Cell and Legal Representative must begin considering whether Dialogue should report or give notice of the Data Security Incident as set out in section 3.6.

- **Monitoring:** If the Data Security Incident involves a compromised IT system or equipment (e.g. network, server, personal computer/laptop or mobile device), then after the remedy/recovery is completed the TechOps Cell must continue to monitor the IT system or equipment, and related systems and equipment, until the investigation of the Data Security Incident (section 3.4) is completed.

3.4 Investigation

Timing: As soon as possible after the Data Security Incident is contained.

This step involves an investigation to verify the root cause and consequences of the Data Security Incident, to confirm that the Data Security Incident was properly contained and remedied, and to enable an assessment of the risks presented by the Data Security Incident. The nature and scope of the investigation will depend on the particular circumstances of the Data Security Incident, including whether the Data Security Incident resulted from a systemic problem or an isolated event.

- **Investigation Team:** The CTO or the TechOps Cell Leader must appoint Team members, other Dialogue employees and external consultants and advisors (if necessary) to an investigation team to investigate the Data Security Incident. (External consultants and advisors must be engaged with the assistance of the Legal Representative in accordance with section 2.6.)

- **Scope of Investigation:** Before the investigation begins, the CTO and the TechOps Cell Leader must determine the initial scope of the investigation. As the investigation proceeds, the CTO and the TechOps Cell Leader may agree to change the scope of the investigation.

- **Investigation and Report:** The investigation team must promptly investigate the Data Security Incident and deliver to the CTO a written report regarding factual circumstances (e.g. who, what, when, where, why and how) of the Data Security Incident and confirming that the Data Security Incident was properly contained and remedied.

- **Reporting:** During the investigation, the TechOps Cell Leader must provide periodic (at least daily) updates regarding the status and findings of the investigation to the CTO, and must immediately report to the CTO and the Legal Representative any information that might challenge the then-current assessment of the cause, nature, extent or severity of the Data Security Incident or the adequacy of the initial containment activities.

- **Reassessment:** During the investigation and after the investigation is completed, the CTO and the TechOps Cell Leader must reassess the Data Security Incident based on information reported by the investigation team, and working with the Legal & Comms Cell take appropriate action (e.g. internal

escalation and changes/additions to Team composition) if there is a material change in the then-current assessment of the cause, nature, extent or severity of the Data Security Incident.

- **Evidence and Record Keeping:** Each Team member must collect, protect and preserve all evidence of the Data Security Incident in accordance with the Evidence and Record Keeping Protocol. Team members must be careful to not inadvertently modify or destroy evidence (e.g. log files) that might be important to the investigation and assessment of the Data Security Incident. Each Team member must create records (in accordance with the Evidence and Record Keeping Protocol) of their investigation activities and findings as they perform the activities and make the findings.

3.5 Risk Assessment

Timing: Within 14 days after the investigation of the Data Security Incident is completed.

This step involves a formal assessment of the risks presented by the Data Security Incident, so that Dialogue can determine whether additional actions are necessary or appropriate. The formal risk assessment is in addition to the informal risk assessments made throughout the incident response process.

- **Risk Assessment Team:** The risk assessment team must be composed of the CTO, the Cell Leader(s), the Legal Representative and other individuals designated by the CTO. Also, in the event of a Security Incident involving health information of individuals residing in Alberta, the Custodian(s) who reported this incident to Dialogue must be part of the Risk Assessment Team.
- **General:** The risk assessment team must assess the risks presented by the Data Security Incident and prepare one or more reports to Dialogue's Executive Leadership Team and Board, if appropriate.
- **Scope of Assessment:** The risk assessment must consider all actual and potential risks presented by the Data Security Incident to Dialogue, its employees, members/clients and service delivery partners, other individuals and organizations and the general public. The risk assessment must consider the cause, nature, extent and severity of the Data Security Incident, the Data involved, the individuals and entities that might be affected, the foreseeable harm and applicable legal obligations (e.g. reporting and notifications).
- **Legal Report:** The assessment of legal risks and obligations (including compliance with statutory, common law and contractual obligations regarding Personal Information or other kinds of regulated, protected or confidential Data) must be conducted by the Legal Representative and set out in a separate, privileged and confidential written report to the CTO and Dialogue Executive Leadership Team.
- **Personal Information Risk Assessment:** If the Data Security Incident involves Personal Information, then the risk assessment team must include Dialogue's Privacy Officer and/or delegate and must include consideration of the Privacy Breach Assessment Guidelines (see Attachment G).
- **Internal Escalation:** The CTO, based on the results of the risk assessment and after consultation with the Legal Representative, must determine whether to immediately report the Data Security Incident to the Executive Leadership Team and the Board (if appropriate) in accordance with the Escalation Response - IT Incident Preparedness Protocol. If immediate reporting is not necessary, then the CTO and Legal Representative will deliver the risk assessment reports to the Executive Leadership Team for consideration in due course.
- **Mandatory reporting to Sun Life:** For significant matters, sunlife must be informed based on the following details

Type of incident	Reporting guideline	Contact at SL
Privacy incidents	Material privacy incidents : **within 48 hours** after incident was identified for Level 1 and Level 2 incidents (to be assessed by Privacy officer)	email details to Privacyofficer@sunlife.com. Informed in cc: John Delangen

	After the dialogue privacy breach process is initiated, The Privacy Officer and the R&C teams will confirm the need to report to Sun Life. Other privacy incidents to be included in the quarterly reporting.	
Security/Cyber Incidents at Dialogue	All P0 and P1 incidents, **within 12hrs** The CISO will confirm the need to report these events to sunlife after an incident is detected.	Sun Life Service Desk is the main intake for all Security Incidents. Phone number for Canada is 1-800-263-4053. Erik Walsh – Associate Director (erik.walsh@sunlife.com) Is also responsible as part of the Security Incident process for all Cyber Security related OSFI notifications. 353 51 336 533 Ext 3076533 Barry Kelly - AVP Threat and Vulnerability Management team SIRT (barry.kelly@sunlife.com) and manages the Blue Team, Security Incident , Red team , Vuln Management, Threat Intel team and Pen testing team. 353 51 336 537 Ext 3076537 Informed in cc: John Delangen (john.Delangen@sunlife.com)
Security/Cyber Incidents at 3rd party	All P0 and P1 incidents **within 12hrs** of event detection The CISO will confirm the need to report these events to sunlife after an incident is detected.	
System outage / Disruption	Report outages that extend beyond our RTO **within 12hrs** after incident is detected Refer to the Business continuity plan	Ayoub Jivraj (ayoub.jivraj@sunlife.com) is the AVP within the Canadian business technology support team who oversees system outage incidents. Ali Kassam ali.kassam@sunlife.com, from corporate technology team oversees the reporting of incidents to OSFI

		Informed in cc: John Delangen (john.Delangen@sunlife.com)
Crisis event	Need to notify Sun Life **within 12hrs** A crisis is an unexpected event that significantly and adversely impacts or threatens to impact the people, assets, reputation and/or business operations of the company. Crises require rapid response beyond the scope of normal business operations. Level 1 Crisis: - Significant event impacting safety, loss of life, or reputation; or a disruption that impacts multiple business groups. High severity and/or global impact. Level 2 Crisis: - Event that poses a risk to safety or loss of life, or a region-wide disruption of business. Moderate Severity and/or regional impact.	Incident Reporting Centre, North America, 1-888-224-8110 The Incident Reporting Centre (IRC) is a central intake point and repository for all incidents and events that may impact Sun Life operations. to be informed at Sun Life (cc) : Anna Cloutier (Anna.Cloutier@sunlife.com) John Delangen (john.Delangen@sunlife.com)

.

3.6 **Reporting/Notifications and Communications**

Timing: Commencing as soon as possible after the initial assessment of the Data Security Incident.

This step sets out the procedure for issuing internal notifications, external reports and notifications (including to members/clients, service delivery partners, insurers, law enforcement and regulators) and media statements regarding a Data Security Incident.

□ **Application:** The procedure set out in this step applies to all internal notifications and external reports, notifications and statements regarding a Data Security Incident.

□ **Required Approvals:** Any internal or external report, notification or communication (including method, form, content and timing) regarding a Data Security Incident must be approved by each of the CTO, the Privacy Officer (if the Data Security Incident involves Personal Information) and the Legal Representative, and by all other persons (e.g. Dialogue's Executive Leadership Team or Board) determined by the Legal Representative.

□ **Mandatory Legal Advice:** The Legal Representative must review and provide legal advice regarding each proposed internal or external report, notification or communication. All written (including electronic) communications with the Legal Representative regarding those issues must be identified as "Privileged and Confidential".

□ **Reporting/Notification Guidelines:** Decisions regarding external reporting, notification and communications must be made after consideration of the General Communications Protocol and the Guidance on reporting breaches to privacy commissioners and notifying Affected Individuals.

3.7 Post-Incident Review (Lessons Learned)

Timing: Within 90 days after the investigation of the Data Security Incident is completed.

This step requires a post-incident review to identify areas for improvement and lessons learned to prevent the same or similar Data Security Incidents and to improve Dialogue's resilience.

□ **General:** Within a reasonable period after a Data Security Incident is resolved (including completion of the related investigation), the CTO must designate a small multidisciplinary team (e.g. risk, technical, business and the Legal Representative) (the "**Post Incident Review Team**") to conduct a post-incident review of the Data Security Incident to identify areas for improvement and lessons learned from the Data Security Incident, including opportunities for improvement to: this Plan and related policies/procedures; Dialogue's execution of this Plan and related policies/procedures; Dialogue's execution of this Plan and related policies/procedures; Dialogue's people, processes, technologies and systems; and Dialogue's technical, physical and administrative data security practices and procedures. Certain aspects of the review might be conducted by the Legal Representative for the purpose of providing legal advice.

□ **External Consultants/Advisors:** If the Post Incident Review Team requires the assistance of an external consultant or advisor, then the consultant/advisor must be engaged with the assistance of the Legal Representative in accordance with section 2.6.

□ **Report:** The Post Incident Review Team must prepare a written report to the CTO and the Executive Leadership Team setting out the team's findings and recommendations. All legal advice from the Legal Representative must be set out in a separate, privileged report.

□ **Implementation:** The CTO or a delegate must be accountable for the implementation of the recommendations of the post-incident review team.

□ **Notification of individuals residing in Alberta affected by the Privacy Breach:** The PO or a delegate must send a notification to the affected individuals upon receiving an instruction to do so from the OIPC, in the case where the Privacy Commissioner doesn't agree with Dialogue's decision to not notify the individuals affected by the Privacy Breach.

3.8 Final Reports and Records

Timing: Within 30 days after the post-incident review of the Data Security Incident is completed.

This step confirms the completion of the Data Security Incident response.

□ **Final Report:** After completion of the response to a Data Security Incident (including completion of all post-incident review activities), the Team must complete, sign and submit to the CTO a form of Data Security Incident Final Report. The Data Security Incident Final Report must not include any legal advice or attach any reports prepared by the Legal Representative.

□ **Legal Report:** After completion of the response to a Data Security Incident (including the completion of all post-incident review activities), the Legal Representative must submit to the CTO a privileged report providing legal advice regarding the Data Security Incident. The legal report must confirm that Dialogue, including its custodians when applicable, have complied with all legal reporting/notification obligations and created all legally required records of the Data Security Incident.

□ **Records:** After completion of the response to a Data Security Incident (including the completion of all post-incident review activities), the CTO must ensure that all documents and data regarding the Data Security Incident are consolidated and retained for the applicable retention periods.

A. Incident Management Program Requirements

Dialogue takes its data protection and security incident response obligations seriously. The list of Incident Management Program Requirements below form the framework of Dialogue's incident response efforts and shall be integrated into the Information Security Policy so that it accurately represents Dialogue's Incident Management Program for external stakeholders.

	Requirements	Included
1.	Dialogue has an established Incident Management Program that has been approved by management, communicated to appropriate constituents and an owner to maintain and review the program.	●
2.	Incident Response Team available 24x7x365.	●
3.	Formal Incident Response Plan has been adopted and includes: ● Guidance for escalation procedure; ● Procedures to collect and maintain a chain of custody for evidence during incident investigation; ● Actions to be taken in the event of a Data Security Incident; ● A process for identifying and mitigating all vulnerabilities that were exploited, removing all malware, inappropriate materials and other components, and remediating any affected systems discovered after incident closure; ● A process for returning systems to an operationally ready state, confirming that the affected systems are functioning normally and, if necessary, implementing additional monitoring to look for future related activity; ● A process for assessing and executing client and third party notification requirements (legal, regulatory and contractual); ● Events relevant to supporting incident investigation regularly reviewed using a specific methodology to uncover potential incidents; ● Feedback process to ensure those reporting Data Security Incidents are notified of the results after the issue has been dealt with and closed; ● Formal disciplinary process for dealing with those who commit a privacy breach.	●
4.	Incident Response Plan and changes to the Plan distributed to stakeholders.	●
5.	Monitoring and Logging: ● Events on scoped systems or systems containing scoped Data relevant to supporting incident investigation regularly reviewed using a specific methodology to uncover potential incidents ● There is an automated system to review and correlate log and/or behavioral events (e.g., SIEM) ● Personnel monitors security alerts related to scoped systems and Data at least daily ● All changes to user access rights logged on scoped systems and Data ● Regular security monitoring include all changes to privileged user access rights on all scoped systems and systems with scoped Data ● Regular security monitoring includes: ○ Network IDS events ○ behavioral activity indicating botnet traffic ○ network device security events ○ server security events ○ application, Web Server, and Database security events ○ malware activity alerts such as uncleaned infections and suspicious activity ○ 24x7x365 security monitoring of the hosting environment	●

B. Incident Reporting and Plan Activation Guidelines

<u>Incident Reporting</u>

1. What to report. All employees, agents and contractors must report all problems and concerns that relate to a possible or potential breach of privacy and/or information security.
2. When to report. Promptly. Employees, agents and contractors must not attempt to assess or remedy a problem or concern themselves. Any possible breach or vulnerability must be reported right away.
3. How to report. Incident reports must be received and assessed by a clearly identified person or small team who is qualified to: (a) gather the basic facts, (b) assess whether any response is warranted (i.e., validate the existence of an incident), and (c) determine whether the incident should be escalated to a full Incident Response Team.
    1. Clinical Quality (CQ): Dialogue's MedOps and CQ team have implemented an internal reporting tool for all MedOps personnel (including all health professionals, case managers, care coordinators, etc.) who become aware of a possible or potential breach of privacy and/or information security. CQ will evaluate and investigate any reported incidents and escalate to the broader Incident Response Team where warranted. Where Personal Health Information is involved but the breach does not require the input of the entire Team, a subset of the Team will be activated including, at a minimum, the Privacy Officer and/or delegate, Legal Representative, certain TechOps Cell Members (where applicable), and the Medical Director.
    2. Information Security (InfoSec): Anyone else at Dialogue that gains knowledge about a possible or potential breach of information security must escalate to the Incident Response Team via Slack on #security channel or via Guarduty or text message to the Exec Cell and Legal & Comm Cell 778-321-7449. The reporter must make sure the message is received and acknowledged.

*Reports must provide the basic facts only. What happened? When? Who was involved? CQ or InfoSec Support may ask follow-up questions in order to assess the situation.

I

C. Incident Response Team Contact List

Executive cell (Exec Cell)

Exec Cell Leader: Alexis Smirnov (Chief Technology Officer)

1.	Primary C-level Executive Sponsor	Alexis Smirnov
2.	CISO	Darryl Campbell

The Exec Cell makes strategic decisions such as issuing notices, changing the service levels, including making decisions to shut down the whole or part of the service.

Technical operations cell (TechOps Cell):

TechOps Cell Leader: Steve Mercier (VP Platform Engineering), Vincent Deschênes as Backup

1.	IT & Security	Souheil Soueidan
2.	DevOps	Edouard Lavery-Plante
3.	Platform Engineering	Maxime Belanger

The TechOps Cell is responsible for providing an accurate assessment of the exposure, performing mitigation actions and preventing/reducing vulnerability.

Legal and external communications cell (Legal & Comms Cell)

Legal & Comms Cell Leader: Dominique Payette (Senior Privacy Counsel and Privacy Officer)

1.	Legal	Melissa Azuelos
2.	Risk & Compliance	Aiham Zawahreh
3.	Privacy	Dominique Payette
4.	Public Relations	Jean-Christophe de Le Rue
5.	Medical Director	Dr. Marc Robin
6.	Clinical Quality	Suong Phan
7.	Customer Success	Melissa Trottier
8.	Social Media	Simrat Barring
9.	Internal Communications	Jean-Christophe de Le Rue

The Legal & Comms Cell is responsible for assessing legal exposure, assessing any actual or potential privacy breaches (if so, the appropriate privacy breach process must be followed), executing

communication actions such as public notices, impacted entities, law enforcement and other external parties and stakeholders.

Dialogue retains external legal counsel specialized in cyber-crime:

Osler	Eloise Gratton; EGratton@blg.com, 416-367-6225 or 514-954-3106
	Daniel Michaluk; DMichaluk@blg.com, 416-367-6097

Dialogue retains external legal counsel specialized in privacy:

Osler	Francois Joli-Coeur; FJolicoeur@blg.com 514-954-3144 or 416-367-6178

Dialogue Tech E&O Insurance Coverage

Broker can provide guidance on notification requirements, or to obtain additional support during an incident. Compliance lead is responsible for coordinating conversations with insurance broker and Legal and Comms Cell. The below note shall provide guidance on notification requirements that apply to the policy.

GPL Assurance	Paige Cheasley; pcheasley@gplassurance.com 514-788 -4933 or 514-914-3065

Reporting a Notice of Circumstances in any Liability Coverage:

(i) If during the policy period you first become aware of circumstances that may give rise to a claim, you may elect to submit a written notice of circumstance to us. Such written notice must contain a description of the circumstances, the nature of the wrongful act, persons involved and the nature of the relief sought.

(ii) Any subsequent claim that is based upon or arises out of a noticed matter will be deemed to have first been made in the policy period in which we accepted the notice of circumstances.

*Team members can delegate their responsibilities to other members of the Team or seek assistance from anyone at Dialogue (on a need-to-know basis) and use external resources, subject to Section 2 of the Plan.

D. Team Communications Protocol

1. **Application:**

This Protocol applies to all communications regarding a Data Security Incident among Team members (including external consultants/advisors) and between Team members and other Dialogue personnel assisting the Team to execute the Plan.

2. **Purpose:**

This Protocol is designed to help ensure the security, confidentiality and legal privilege (if applicable) of all communications regarding a Data Security Incident.

3. **Confidentiality**

(a) General: All information about a Data Security Incident (including the fact that a Data Security Incident has occurred) must be treated as strictly confidential, and must not be disclosed to any person (other than Team members) except as otherwise authorized by this Protocol or the Incident Response Plan.

(b) Dialogue Personnel Assisting Team: Information about a Data Security Incident may be disclosed to other Dialogue personnel assisting the Team to respond to the Data Security Incident provided that: the information is disclosed on a need-to-know basis only; and the personnel are clearly warned that the information is strictly confidential and must not be disclosed to any other person.

(c) Other Disclosures: Information about a Data Security Incident must not be disclosed to any other person (e.g. Dialogue personnel not involved in Incident response activities, Dialogue members/clients or news media) except in accordance with the Plan and related protocols (i.e. General Communications Protocol).

4. **Security**

(a) General: All communications among Team members and with other Dialogue personnel assisting the Team must be made either in person (face-to-face meetings) or using secure communications channels.

- #war-room channel is used for ongoing communication.
- Cell Leaders may elect to create a private channel for restricted ongoing communication. If so, the existence of such a channel and its members are communicated to #war-room and #wg-infosec-response.
- The Legal&Comms Cell Leader will make Team members aware that, unless legal privilege applies, all communications may be discoverable in a legal proceeding. The Legal&Comms Cell Leader is responsible for determining whether litigation is a reasonably foreseeable consequence of an incident and, if so, invoking a communication protocol meant to establish a legal privilege that protects Team communications and documents.

(b) Telephone: Telephone calls should be made using landlines or mobile phones in private places. Care should be taken to ensure that conversations are not overheard by unauthorized persons.

(c) Other Technologies: Communications using other technologies (Slack, email, text messaging, or other Google Workspace services) must be sent/received using work accounts (or other secure accounts expressly approved by the CTO) that are protected using robust credentials.

(d) Prohibited Systems/Services: If a Data Security Incident has affected, or might have affected, an information technology system or service (e.g. Dialogue's Slack, email, text messaging, or other Google Workspace service), then the system/service and any connected system/service must not be used for any communications about the Incident unless and until the CTO expressly approves the use of the system/service. In addition, Team Members must not use a communication system/service that is prohibited by the Cell Leader(s).

5. **Marking:**
All written communications with Team members and other persons about a Data Security Incident must be prominently marked “Privileged and Confidential”.

6. **Questions:**
If you have any questions or concerns regarding this Protocol, please contact the CTO or the Legal Representative.

E. General Communications Protocol

All communications outside of the Team will be planned and authorized jointly by the Exec and Legal & Comms Cells and, when appropriate, vetted by the Legal Representative. Timing is critical. Although perfect knowledge cannot be expected, the Team will strive for well-timed communication that is accurate and appropriately qualified in light of the uncertainties. The following are potential internal and external audiences to consider in responding to every Incident.

Internal	External
Affected employees Board of directors Sunlife (see section 3.6)	Insurers Law enforcement Regulators / government Other organizations (threat information) Affected individuals Media and public at large Clients and/or partners Investors

Dialogue has pre-selected a public relations firm, Media Profile, who will be notified and engaged.

Legal & Comms Cell are responsible for assessing and executing client and third-party notification requirements (legal, regulatory and contractual). Notification procedures include any customer/client-specific notification requirements. In cases where PHI of individuals is breached, the Medical Director (Dr. Marc Robin) or his delegate(s) is in charge of notifying the patients, subject to Attachment G4: Guidance on reporting breaches to privacy commissioners and notifying Affected Individuals.

Legal & Comms Cell and Customer Success representative, Gabriella Baciu) is responsible for identifying a security contact for our clients, stored in Salesforce. Lacking a security contact explicitly identified by the client, the client's main contact is the first contact. Everyone in the Legal & Comms Cell has access and has instructions on how to find the client contact. Standard contacts are used to communicate with them.

For tactical back-and-forth communication, Legal & Comms Cell (PO, Public Relations representative, , and Legal Representative) are responsible for communicating with a threat actor, with support of TechOps Cell and Dialogue's engaged incident response vendor (where applicable).

Third-Party Reporting and Notification Duties to Consider:

1. Is there a duty to notify individuals and report to the privacy regulators (see Attachment G4).
2. Is there a duty to notify other organizations under privacy regulation (see Attachment G4).
3. Do we have contractual notification obligations that may apply (consult with Legal).
4. Should we share threat information with other organizations?
5. Should we report to law enforcement because they are likely to assist?

Communication principles

1. **Acknowledgement**. Laying out the facts as they are known will reinforce that you are dealing with the issue and taking charge. It will also present an opportunity to correct any misinformation that a reporter may already have.
2. **Empathize**. Demonstrating that you understand all sides of an issue and its importance is a critical step in convincing audiences to listen to what you have to say. Empathy is not an apology; it is a demonstration of feeling and understanding.
3. **Action**. Once acknowledgement and empathy have been expressed, then the audience is more open to hearing about the steps a company is taking to address the issue. This is an opportunity to explain context and process and demonstrate leadership.
4. **Advocacy**. The final step in messaging is communicating the organization's values, approach or track record. Too often organizations start with this step, which comes across as disingenuous given that the company is in a crisis. Only by providing the above context first will the audience be willing to hear about the values or history of the organization. During a crisis, including advocacy messages is not always necessary, and should not be forced.

Possible communication materials

- News release
- Media statement
- Key messages (for interviews)
- QA and fact sheets for media
- Social media posts
- Statements to staff
- Phone and email scripts for front line staff
- Statements for other stakeholders including: government, regulators, investors, etc.

i. Tracking and reporting

The Legal & Comms Cell, with the support of external PR agency, will track media and social media coverage of any incident and report to the Team on a schedule of Dialogue's choosing. For severe incidents, this reporting should be at least once per day.

Once an incident has passed, Legal & Comms Cell will issue the post-mortem report on the success of the communications efforts and any lessons learned, including recommendations for improving the Plan.

F. Evidence and Record Keeping Protocol

A. Evidence

1. **Application**: This Protocol applies to all activities by Team members when executing the Discovery, Containment, Remedy/Recovery and Investigation steps of the Plan.

2. **Purpose**: This Protocol is designed to help Team members collect and securely retain all available evidence regarding a Data Security Incident (including the cause, nature, extent and severity of the Incident) for use in legal and regulatory investigations and proceedings (e.g. investigations by regulators and law enforcement).

3. **Kinds of Evidence**: Evidence of a Data Security Incident may include all kinds of physical objects and paper and electronic documents and records that are collected or created by a Team member while performing activities relating to the Incident. For example: physical storage devices; paper and electronic correspondence, documents and records; downloaded computer logs and telephone logs; and screen shots. If you are uncertain whether an item should be treated as evidence, please contact the Legal Representative.

4. **Collection**: If evidence is in paper format, then to the extent possible Team members should collect and retain the original item rather than a copy of the item. If evidence is in electronic format, then Team members should ensure that they collect and retain a complete and accurate electronic copy of the item.

5. **Temporary Storage**: A Team member who creates or collects an item of evidence must store the item in a secure manner (e.g. paper and physical items kept in a locked drawer, and electronic items stored in a secure, password-protected computer that is not affected by the Data Security Incident) so that the item is protected against loss, damage, deletion and unauthorized access.

6. **Delivery to Legal Representative:** All evidence must be delivered promptly to the Legal Representative. A Team member who creates or collects an item of evidence must personally deliver the item (and the related Chain of Custody Record, described below) to the Legal Representative as soon as reasonably practicable. If use of the item by the Team member (or other persons) is necessary for responding to the Incident, then the Team member may create and retain a copy of the item before delivering the original item to the Legal Representative.

7. **Chain of Custody Record**: A Team member who collects or creates an item of evidence must also contemporaneously create a written, dated and signed "Chain of Custody Record" describing each step (including date and time) in the process used to collect/create the item and to store the item until it is delivered to the Legal Representative. A Chain of Custody Record can be simple (e.g. a handwritten note), but it must be accurate and complete, because it might be useful to the investigation of the Incident and necessary for the item to be used in a legal proceeding. The Chain of Custody Record for an item of evidence must be delivered to the Legal Representative along with the item of evidence.

8. **Chain of custody evidence** may impact both Exec Cell decision making and Legal&Comms Cell activities. As a result, material updates to the chain of custody should be shared with those Cells immediately and on an ongoing basis, until the Data Security Incident has concluded.

- All communications between stakeholders are recorded. Slack, Email, Text may be used. Slack channels are #security #war-room and #wg-infosec-response
- The incident is logged in Jira as P0 priority item for tracking purposes.
- A Notion page may be created for long-form documentation.
- Post-Mortem notes are recorded in Notion or in equivalent information storage medium.

- Events relevant to supporting incident investigation are regularly reviewed to uncover other potential incidents. TechOps Cell is responsible for this; TechOps Cell Leader is accountable for this happening.
- The information collected may be shared with the insurer, subject to approval from the Legal Representative.

9. **Confidentiality:** All evidence regarding a Data Security Incident must be treated as strictly confidential, and must not be disclosed to any person (other than Team members) except as otherwise authorized by this Protocol or the Plan.

B. Record-Keeping

1. **Application:** This Protocol applies to all activities by Team members when executing the Discovery, Containment, Remedy/Recovery and Investigation steps of the Plan.

2. **Purpose**: This Protocol is designed to help Team members create and retain records of their activities in response to a Data Security Incident, so that the recorded information is available for use by other Team members in responding to the Incident and by other persons authorized by Dialogue.

3. **General**: Each Team member must create accurate and complete records of all of their activities when executing the Discovery, Containment, Remedy/Recovery and Investigation steps of the Plan. Each record must be dated and clearly indicate the name of the Team member who created it. If the record is hand written, then it should be signed by the Team member who created it.

4. **Timing**: Each Team member must create records of their activities on a daily basis and more frequently to the extent practicable. If a Data Security Incident involves a potentially compromised information technology system, then all technical activities (e.g. copying logs, isolating systems, suspending credentials) must be recorded contemporaneously and if possible indicate the time of each activity.

5. **Confidentiality**: All records and the information they contain about a Data Security Incident and steps taken in response to the Incident must be treated as strictly confidential, and must not be disclosed to any person (other than Team members) except as otherwise authorized by this Protocol or the Plan. All records should be prominently marked "Confidential".

6. Record-Keeping System

a. General: Each Team member must create and store their records using the record-keeping system specified by the CTO (see Chain of Custody above). If the CTO has not specified a record-keeping system, then Team members must create and store their records in a secure manner (e.g. paper notes kept in a locked drawer, and electronic records stored on a secure, password-protected computer), so that the records are protected against loss, damage and unauthorized access, use or disclosure.

b. Prohibited Systems/Services: If a Data Security Incident has affected, or might have affected, an information technology system or service (e.g. Dialogue's Google Suite solution), then the system/service and any connected system/service must not be used to create or store records unless and until the Incident has been fully resolved and the system/service has been verified to be secure. In addition, Team Members must not use a record-keeping system prohibited by the Team Leader.

7. **Collection of Records:** Each Team member must deliver their records to the Cell Leader(s) when the Team member completes their participation in the Data Security Incident response process and at any other time on request by the Cell Leader(s). The Cell Leader(s) must securely retain the records and make them available for use and retention in accordance with the Plan.

8. **Retention of Records**: Records shall be retained for a minimum of 2 years after the day on which Dialogue determined that the Data Security Incident has occurred.

9. **Exceptions**: This protocol does not apply to Legal Representatives and privacy officers.

10. **Questions**: If you have any questions or concerns regarding this Protocol, please contact the CTO or the Legal Representative.

G. Privacy Breach Assessment Guidelines

a. G1. Guidelines for the Identification of Privacy Breaches

Definitions:

- "**Applicable Privacy Legislation**": Refer to Appendix A of the Internal Privacy Policy for the Glossary of Terms.

- "**Custodian**": Refer to Appendix A of the Internal Privacy Policy for the Glossary of Terms.

- "**Privacy Breach**" means a confirmed loss of, unauthorized access to, or unauthorized disclosure of Personal Information resulting from a breach of Dialogue's security safeguards (i.e. physical, organization and technological measures meant to protect Personal Information against the loss or theft as well as unauthorized access, disclosure, copying, use, or modification of Personal Information) or from a failure to establish those safeguards. Security safeguards shall also include those measures included in clause 4.7 of Schedule 1 of PIPEDA or in substantially similar provincial laws and health information laws. The term "Privacy Breach" may also be referred to as a "Privacy Incident," and these terms may be used interchangeably in this document and others.

  A Privacy Breach always requires mitigation, but depending on its severity may also include reporting to regulators and notification to Affected Individuals (as defined below). Refer to Attachment G2 for guidance on assessing the severity of a Privacy Breach, Attachment G3 for the appropriate Privacy Breach Response Procedure, and to Attachment G4 for guidance on whether reporting to regulators and notifying Affected Individuals (as defined below) is required.

- "**Privacy Policy**": Refer to Appendix A of the Internal Privacy Policy for the Glossary of Terms.

- **"Affected Individual"** means an individual whose Personal Information has been involved in a Privacy Breach (in Dialogue's case this could mean our employees, subcontractors, or patients (i.e. end users of our Integrated Health Platform).

- "**Suspected Privacy Breach**" means a situation that may affect Personal Information under the control or custody of Dialogue. Suspected Privacy Breaches must be escalated to the Privacy Officer or their delegate for qualification, and if required, severity assessment. Following this qualification and severity assessment, the "Suspected Privacy Breach" might be classified as a "Privacy Breach".

  The sooner a breach is identified, the sooner actions can be taken to contain the incident and mitigate the potential harm. Every time you suspect a Privacy Breach, you should immediately use the Clinical Quality Reporting Tool or escalate to InfoSec in accordance with Incident Reporting and Plan Activation Guidelines.

  In order to reduce the risk of harm resulting from a Privacy Breach, it is important to ensure that every Dialogue employee can quickly identify a Suspected Privacy Breach and report it immediately. This is particularly relevant for Dialogue employees monitoring emails sent to privacy@dialogue.co or support@dialogue.co. Raising awareness around information confidentiality and security is the first step. The following are guidelines to help employees identify a Suspected Privacy Breach threat that may arise.

  A Privacy Breach occurs when there is a loss of, unauthorized access to or unauthorized disclosure of Personal Information resulting from a breach of Dialogue's security safeguards that are referred to in clause 4.7 of Schedule 1 of PIPEDA or in substantially similar provincial laws and health information laws (i.e. physical, organization and technological measures meant to protect Personal Information against the loss or theft as well as unauthorized access, disclosure, copying, use, or modification of Personal

Information) or from a failure to establish those safeguards. Such activity is ''unauthorized'' if it occurs in contravention of Dialogue's Privacy Policies or Applicable Privacy Legislation.

The following are some common examples of Privacy Breaches:

- Personal Information is stolen or misplaced;
- Personal Information is sent to another person through unsecured means (unsecured email);
- Personal Information has been accessed by an employee that should not have access thereto;
- A letter is inadvertently mailed to an incorrect address or faxed to the wrong person;
- An electronic device (e.g. computer, handheld electronic device, USB storage device) is lost or stolen where appropriate security controls such as passwords and encryption have not been implemented;
- Inappropriate access to Personal Information stored in an electronic system;
- Personal Information is not disposed of appropriately;
- A person who legitimately accesses records gains unintended access to personal information that he or she is not authorized to see.

Privacy Breaches usually fall into three broad types:

- **Accidental disclosure:** involves incidents where Dialogue discloses Personal Information to unintended recipients by accident
    - For example: member information sent to the wrong recipient through mechanical or human error;
- **Loss:** refers to incidents where Personal Information in the hands of Dialogue goes missing
    - For example: a laptop, CD or paper documents are lost;
- **Unauthorized access, use or disclosure** encompasses any incident in which Personal Information is accessed, used or disclosed without authorization or in contravention of the Dialogue Privacy Policy or Applicable Privacy Legislation.
    - For example: a laptop is stolen, database is hacked into, or an employee accesses Personal Information for unauthorized purposes.

The Privacy Breach must be related to Personal Information under the custody or control of Dialogue.

Suspected or real Privacy Breaches can come to Dialogue's attention through (i) report by one of Dialogue employees or subcontractors; (ii) through a complaint by a Dialogue member (end user) or member of the public; (iii) through a formal complaint to a regulatory or legal authority; or (iv) through compliance monitoring mechanisms such as audit trails in electronic systems.

What should I do if I am not sure whether an incident I became aware of is a Privacy Breach or not?

The Privacy Officer or their delegate will evaluate the Suspected Privacy Breach and will get back to you if the incident is considered a Privacy Breach.

G2. Breach Severity Evaluation Grid

Not all Privacy Breaches are equal or necessarily entail the same level of risk exposure and remediation measures. Several criteria must be considered when evaluating the severity of a Privacy Breach. The level of severity goes hand in hand with the level of risk exposure and dictates the approach to follow when addressing the Privacy Breach.

Dialogue has established two sets of criteria to comply with law and react to Privacy Breaches. Accordingly, even if a Privacy Breach does not meet the risk of harm[1] criteria set out in Data Protection Laws, but the breach meets our internal criteria, the breach will be managed following the high severity response procedure.

This Attachment provides a framework to guide the evaluation of a Privacy Breach and assess breach severity and the course of action to be taken. The examples provided below are for illustration only. The assessment should be based on the best available facts as known at the time of the assessment. If any criteria in the "High" or "Very High" column is met, then the high severity process should be followed.

In case of a risk of harm to an Alberta resident: to comply with mandatory reporting of a privacy breach under the Alberta HIA and regulations, Custodians and Dialogue as their Information Manager must assess the risk of harm to an individual when their health information has been lost or inappropriately accessed or disclosed by considering each of the factors set out in *s. 8.1(1) of the Alberta Health Information Regulation* in addition to any other relevant factors described hereunder:

Severity Assessment Grid				
Criteria	**4: Low**	**3: Moderate**	**2: High**	**1: Very High**
Risk of harm (Data Protection Laws) Criteria				
Sensitivity of the information	Phone number publicly available	Name and Address only	Date of birth Amount due Salary	Member health information Financial information, unique identifiers (SIN, driver's license number) Behavioral information Geolocation Account credentials
Presumed intention	Self-reported by a Dialogue employee who has been debriefed	Self-reported by the only external party in possession of information	Lost information Signs of unauthorized access from inside Dialogue	Stolen information Signs of unauthorized access from outside Dialogue
Potential harm to the Affected Individuals involved, including risk of	Unique set of information was found and there is little risk	Only one identifier (name, address, email address), and	Lost information is not to be found	Financial information Health information Information belonging to public figure

[1] The definition of "risk of harm" varies by province. Refer to Attachment G4 for details on the thresholds applicable in each province.

Monetary loss **Identity theft** **Body injury** **Reputational damage** **Humiliation, embarrassment**	of it been accessed/ or misused	non-sensitive information An information media was lost within Dialogue's premises	Information is for sale and/or sold online (i.e. dark web)	
Dialogue Internal Criteria				
Number of Affected Individuals involved	Less than 10	10 or more	50 or more	100 or more
Dialogue's financial risks	Little development needed to address system issue Low potential harm	Costs associated with termination of a business associate contract	Lawsuits possible High development costs	Class-action possible Risk of identity theft for affected individuals
Dialogue's reputational risks	Self-reported by the involved individual	Breach contained soon after identification	Breach identification occurred more than 2 months after the breach Breach was detected by outside parties (including clients) Breach is getting growing social media coverage	Likeliness of class-action Information belonging to public figure Loss of market value
Number of systems involved	None	System of a business associate	System with sensitive information and identifiers	Multiple systems containing sensitive info
Efforts required to address the breach	Further training Process only	Little development needed to address system issue Temporary fix possible	Potential disruption to other projects agendas	Development needed No easy, temporary fix

Course of actions	
Rating	**Path**
One of the Data Privacy Laws criteria is 1 or 2	Follow high severity breach response
All other situations	Assess whether to follow high or low severity breach response

G3. Privacy Breach Response Procedure

Upon becoming aware of a Suspected Privacy Breach, the following steps must be followed immediately. These steps are not meant to augment the Security Incident Response protocols as illustrated above. The CTO and PO shall make determination on whether the Full Security Incident Response Plan is to be initiated, or whether only the Privacy Breach Response Procedure is appropriate given the nature of the incident.

1.1 REPORT SUSPECTED PRIVACY BREACH AND CONDUCT PRELIMINARY ASSESSMENT

In order to properly identify and report a Suspected Privacy Breach, all employees that manage or handle Personal Information must have an understanding of privacy issues that might arise at Dialogue and receive appropriate training.

All employees are responsible for identifying Suspected Privacy Breaches in accordance with the Guidelines included in Attachment G1 above. Once identified, employees must report them to Clinical Quality via the Clinical Quality Reporting Tool who will, in turn, notify the PO (or delegate). The confirmation of whether the Suspected Privacy Breach is actually a Privacy Breach is the Responsibility of the PO.

1.1.1 CONDUCT PRELIMINARY ASSESSMENT

Once a Suspected Privacy Breach has been brought to the attention of the PO, it must be investigated. A high level assessment of the situation shall immediately be carried out by the PO who shall determine if the Suspected Privacy Breach is a Privacy Breach (i.e. confirmed) and assign a severity level determined in accordance with the criteria attached in Attachment G2, which shall trigger an appropriate organizational response.

Attachment G2 contains detailed guidelines on how to determine the appropriate severity level that may apply to a confirmed Privacy Breach as well as the appropriate response procedure to follow.

If an incident concerns the health information of individuals residing in Alberta, the Custodian(s) in charge in part or in whole of the care of this individual must be notified and be part of the investigation and the preliminary assessment as well as becoming a member of the Breach Response Team. If an incident qualifies as a high severity Privacy Breach, the PO must assemble a Breach Response Team (consisting of CQ, Legal, Privacy and others as appropriate) or engage the Incident Response Team to discuss risks to Dialogue and follow the high severity Privacy Breach response procedure described in Section 1.2 to ensure all required actions are taken in compliance with legal and regulatory requirements.

The Breach Response Team, led by the PO, shall guide and oversee all steps of the high severity Privacy Breach response procedure and action plan.

If the Privacy Breach is considered to be of low severity, the PO (or their delegate(s)) may address and document the breach, or may decide to form a team to complete this task. A minor Privacy Breach does not require legal notification to the Affected Individuals or a privacy regulator.

The Breach Response Team shall follow the low severity Privacy Breach response procedure described in Section 1.3 and resolve the issue(s).

1.2 HIGH SEVERITY PRIVACY BREACH RESPONSE PROCEDURE

1.2.1 CONTAIN HIGH SEVERITY PRIVACY BREACH

Once it has been determined that a high severity Privacy Breach has occurred, steps must be taken immediately to contain the Privacy Breach.

The Breach or Incident Response Team shall ensure the Privacy Breach is immediately contained by:

(a) **Closing the Breach:** Put an end to the unauthorized practice, recover all relevant records, shut down the system (or access to the system) that relates to the Privacy Breach, revoke or change computer access codes, correct vulnerabilities in physical or electronic security, or undertake any other corrective action as appropriate;

(b) **Protect the Investigation**: Protect and preserve all evidence that could be valuable in determining the cause of the Privacy Breach. This may include cloning electronic devices, preserving emails, and the Legal Department sending a litigation hold / document preservation notice to relevant employees.

1.2.2 INVESTIGATE HIGH SEVERITY PRIVACY BREACH AND IMPLEMENT CORRECTIVE ACTIONS

The Breach Response Team and relevant stakeholders shall meet to discuss the Privacy Breach. This meeting will be held at the outset of the investigation to agree on the scope and requirements of the investigation.

The Breach Response Team shall:

(a) Coordinate the investigation and confirm the risks posed by the Privacy Breach;

(b) Define an action plan to investigate the Privacy Breach;

(c) Coordinate the implementation of the action plan;

(d) Oversee the completion of an Investigation Report as described in Attachment G5.

While confirming the risks posed by a Privacy Breach, the following factors described in detail in Attachment G2 should be considered:

(a) The sensitivity of the Personal Information involved in the Privacy Breach; and

(b) The probability that the Personal Information has been, is being, or will be misused.

The Breach Response Team shall:

(a) Oversee the Privacy Breach resolution process and ensure that all relevant risks are properly addressed;

(b) Review the Privacy Breach Investigation Report and ensure the breach is thoroughly investigated, documented and properly resolved.

1.2.3 IDENTIFY PARTIES TO NOTIFY

The PO (or delegate(s)) shall:

(a) **Regulators**: Determine whether there is a legal obligation to send a declaration to the federal and/or provincial privacy regulator(s) and a notice to Affected Individuals, based on whether there is a risk of harm to Affected Individuals, using the Breach Severity Assessment Grid (see Attachment G2) and the guidance provided in Attachment G4 on breach reporting.

(b) **Third Parties**: Determine whether there is a legal obligation to send a notice to external parties, including third party contractors. Notice to external parties may have to be sent to:

- Business Partners: if required by contract;
- Law enforcement: if theft or other crime is suspected;
- Insurers or others: if required by contract or if the Privacy Breach may be insurable;
- Professional or other regulatory bodies (if applicable); and
- Financial institutions if their assistance is necessary for contacting Affected Individuals or assisting with mitigating harm.

(c) **Internal Parties**: Determine the opportunity to notify other impacted internal parties, such as Business Units or Custodian(s) concerned by the Privacy Breach, if not previously notified. In case of a privacy breach occurs when there is a violation of the duties of the HIA, it is very important that the PO notifies the Custodian of the Security Incident as soon as practicable and, to the extent necessary, work with the Custodian with a view to ensuring an expeditious response to the Security Incident, including, without limitation, remediating the Security Incident, notifying affected individuals, regulators and other organizations, ensuring that all factors relating to a risk of harm assessment are appropriately considered, and otherwise complying with obligations under Applicable Privacy Legislation.

1.2.4 REPORT TO PRIVACY REGULATOR OR OTHER GOVERNMENT AUTHORITIES

The PO (or delegate(s)) in collaboration with the Breach Response Team shall report to privacy regulator(s) as soon as possible, once the Privacy Breach has occurred and the requirement/decision to notify has been confirmed by the PO (or delegate(s)) (unless cooperation with law enforcement necessitates a delay to protect the investigation). See Attachment G4 for guidance on when to report a Privacy Breach to privacy regulator(s) or other government authorities as required by Applicable Privacy Legislation.

Except if a Privacy Breach concerns the health information of individuals residing in Alberta, the declaration to a privacy regulator should be in writing and include:

- A description of the circumstances of the Privacy Breach and, if known, the cause;
- The day on which, or the period during which, the Privacy Breach occurred (if neither is known, the approximate period);
- A description of the Personal Information that is the subject of the Privacy Breach;
- The number of Affected Individuals by the breach or, if unknown, the approximate number;
- A description of the steps that Dialogue has taken to reduce the risk of harm to each Affected Individual resulting from the Privacy Breach or to mitigate that harm;
- A description of the steps that Dialogue has taken or intends to take to notify each Affected Individual of the Privacy Breach if it is reasonable in the circumstances to believe that the breach creates a risk of harm to the Affected Individual; and
- The name and contact information of the PO or any other person who can answer, on behalf of Dialogue, the privacy regulator's questions about the Privacy Breach.

The Privacy Breach Investigation Report Template in Attachment G5 should be used for internal record-keeping and may also be used as a basis to create incident reports to privacy regulators, when required.

If a Privacy Breach concerns the health information of individuals residing in Alberta and it is concluded that there is a risk of harm for this individual, notice must be given to Office of the Information and Privacy Commissioner ("**Alberta OIPC**") and also be given to the Minister of Health as follows:

- **Notice to Alberta OIPC** must be given in writing in a form approved by the Commissioner and must include the information listed at 8.2(2) HIA Regulation as follows:

    (a) the name of the custodian who had custody or control of the information at the time of the loss or unauthorized access or disclosure,

    (b) a description of the circumstances of the loss or unauthorized access or disclosure,

    (c) the date on which or period of time within which the loss or unauthorized access or disclosure occurred,

    (d) the date on which the loss or unauthorized access or disclosure was discovered,

    (e) a non-identifying description of the type of information that was lost or that was the subject of the unauthorized access or disclosure,

    (f) a non-identifying description of the risk of harm to an individual as a result of the loss or unauthorized access or disclosure, including a description of the type of harm and an explanation of how the risk of harm was assessed that includes a non-identifying description of the custodian's consideration of the factors referred to in section 8.1(1), including any relevant factors not detailed in that section,

    (g) the number, or if the number cannot be determined, an estimate of the number, of individuals to whom there is a risk of harm as a result of the loss or unauthorized access or disclosure,

    (h) a description of any steps that the custodian has taken or is intending to take, as of the date of the notice, to reduce the risk of harm to an individual as a result of the loss or unauthorized access or disclosure,

    (i) a description of any steps that the custodian has taken or is intending to take, as of the date of the notice, to reduce the risk of a future loss or unauthorized access or disclosure,

    (j) a non-identifying copy of the information that has been or will be provided in the notice to the individual who is the subject of the individually identifying health information referred to in subsection (4), if applicable, together with a statement indicating the method referred to in section 103 of the Act that has been or will be used to give notice to the individual, if applicable,

    (k) if the custodian is requesting the authorization of the Commissioner to give notice to an individual by substitutional service under section 103(c) of the Act, the request together with a statement of the reasons for the request,

    (l) the name and contact information for a person who is able to answer questions on behalf of the custodian about the loss or unauthorized access or disclosure, and

    (m) any other information that the custodian considers relevant.

- **Notice to the Minister of Health** in the form prescribed at 8.2(3): (3) A notice to the Minister of a loss of or an unauthorized access to or disclosure of individually identifying health information under section 60.1(2) of the Act must be in writing in a form approved by the Minister and must include the information set out in subsection 8.2(2)(a), (b), (e), (f), (g), (h), (l) and (m) as follows:

(a) the name of the custodian who had custody or control of the information at the time of the loss or unauthorized access or disclosure,

(b) a description of the circumstances of the loss or unauthorized access or disclosure,

(e) a non-identifying description of the type of information that was lost or that was the subject of the unauthorized access or disclosure,

(f) a non-identifying description of the risk of harm to an individual as a result of the loss or unauthorized access or disclosure, including a description of the type of harm and an explanation of how the risk of harm was assessed that includes a non-identifying description of the custodian's consideration of the factors referred to in section 8.1(1), including any relevant factors not detailed in that section,

(g) the number, or if the number cannot be determined, an estimate of the number, of individuals to whom there is a risk of harm as a result of the loss or unauthorized access or disclosure,

(h) a description of any steps that the custodian has taken or is intending to take, as of the date of the notice, to reduce the risk of harm to an individual as a result of the loss or unauthorized access or disclosure,

(l) the name and contact information for a person who is able to answer questions on behalf of the custodian about the loss or unauthorized access or disclosure, and

(m) any other information that the custodian considers relevant.

1.2.5 NOTIFICATION TO AFFECTED INDIVIDUALS

The PO (or delegate(s)) in collaboration with the Breach Response Team shall deliver notification to Affected Individuals in a manner that will reasonably ensure receipt. Delivery of notification should be direct (i.e. by App, phone, letter, email or in person), unless such delivery could cause further harm to the Affected Individuals, is likely to cause undue hardship for Dialogue (e.g. is prohibitive in cost), or the contact information for Affected Individuals is not known. In such cases, delivery may be indirect (i.e. by website information, posted notices, or through the media), provided the communication is likely to reach the Affected Individuals. See Attachment G4 for guidance on when to notify Affected Individuals of a Privacy Breach.

Except if a Privacy Breach concerns the health information of individuals residing in Alberta, the notice to Affected Individuals should contain enough information to allow the Affected Individuals to understand the significance of the Privacy Breach and take steps to mitigate the harm. At a minimum, it must include:

- A description of the circumstances of the Privacy Breach;
- The day on which, or period during which, the Privacy Breach occurred or, if neither is known, the approximate period;
- A description of the Personal Information that is the subject of the Privacy Breach to the extent that the information is known;
- A description of the steps that Dialogue has taken to reduce the risk of harm / injury, including a description of how Dialogue plans to assist the Affected Individuals, if there is any such plan;
- A description of the steps that Affected Individuals could take to reduce the risk of harm that could result from the breach or to mitigate that harm. This may include arranging for credit monitoring, identity theft insurance, terminating credit card or bank accounts, or raising awareness of phishing

emails, text message or phone scams. If relevant, the notice should include information to assist Affected Individuals in protecting themselves against identity theft;

- Contact information (a toll-free number or email address) for Customer Success or another appropriate department or individual(s) at Dialogue that can answer questions, provide further information, or address privacy concerns. Dialogue must take reasonable steps to ensure that the department or person is prepared to address Affected Individuals' concerns, including by providing prior training and reference material, such as a script (Q&As) for Customer Success.

If a Privacy Breach concerns the health information of individuals residing in Alberta, the Custodian must also provide notice to the individual who was subject to the improper use, unauthorized access, or disclosure of their health information; **and report to the Alberta OIPC when and why there has been a determination to not report a privacy breach to an individual** (s. 60.1 HIA)**.** In such a case, according to the *Information Management Program for Custodians* ("IMPC"), Dialogue undertakes to notify the Commissioner on Custodians' behalf of this, and to let Custodians know if Dialogue decides not to give notice.

- **Notice to an individual of a loss of or unauthorized access to or disclosure of individually identifying health information under section 60.1(2) of the Act must be in writing and must include the information listed at 8.2(4) HIA Regulation as follows:**

  (a) a description of the circumstances of the loss or unauthorized access or disclosure,

  (b) the date on which or period of time within which the loss or unauthorized access or disclosure occurred,

  (c) the name of the custodian who had custody or control of the health information at the time of the loss or unauthorized access or disclosure,

  (d) a non-identifying description of the type of information that was lost or that was the subject of the unauthorized access or disclosure,

  (e) a description of the risk of harm to the individual as a result of the loss or unauthorized access or disclosure, including a description of the type of harm and an explanation of how the risk of harm was assessed,

  (f) a description of any steps that the custodian has taken or is intending to take, as of the date of the notice, to reduce the risk of harm to the individual as a result of the loss or unauthorized access or disclosure,

  (g) a description of any steps that the custodian has taken or is intending to take, as of the date of the notice, to reduce the risk of a future loss or unauthorized access or disclosure,

  (h) a description of any steps that the custodian believes the individual may be able to take to reduce the risk of harm to the individual,

  (i) a statement that the individual may ask the Commissioner to investigate the loss or unauthorized access or disclosure that includes contact information for the Office of the Information and Privacy Commissioner,

  (j) the name and contact information for a person who is able to answer questions on behalf of the custodian about the loss or unauthorized access or disclosure, and

  (k) any other information that the custodian considers relevant.

- **Notice to Commissioner of decision not to give notice to an individual must :**

  (a) be in writing in a form approved by the Commissioner,

  (b) have attached as an appendix the notice required to be provided to the Commissioner in respect of the matter under section 60.1(2) of the Act, and

  (c) set out the total number, or if the number cannot be determined, an estimate of the total number, of individuals that the custodian expects not to give notice to on the basis set out in section 60.1(5) of the Act.

THE PO SHALL APPROVE ALL REPORTS TO PRIVACY REGULATORS AND OTHER REGULATORS, ALL NOTIFICATIONS TO AFFECTED INDIVIDUALS, AS WELL AS ANY INTERNAL/EXTERNAL COMMUNICATIONS ABOUT THE PRIVACY BREACH.

1.3 LOW SEVERITY PRIVACY BREACH RESPONSE PROCEDURE

1.3.1 CONTAIN LOW SEVERITY PRIVACY BREACH

Once it has been determined that a low severity Privacy Breach has occurred, the containment of the breach must be undertaken. The PO (or delegate(s)) or Breach Response Team shall ensure the Privacy Breach is immediately contained by:

(a) **Closing the Breach:** Put an end to the unauthorized practice, recover all relevant records, shut down the system (or access to the system) that relates to the Privacy Breach, revoke or change computer access codes, correct vulnerabilities in physical or electronic security, or undertake any other corrective action as appropriate;

(b) **Protecting the Investigation**: Protect and preserve all evidence that could be valuable in determining the cause of the Privacy Breach. This may include cloning electronic devices, preserving emails, and the Legal Department sending a litigation hold / document preservation notice to relevant employees.

1.3.2 INVESTIGATE LOW SEVERITY PRIVACY BREACH AND IMPLEMENT CORRECTIVE ACTIONS

Relevant stakeholders affected by the Privacy Breach shall be consulted to fully understand the nature of the Privacy Breach and its potential impact.

The PO (or delegate(s)) or Breach Response Team shall then:

(a) Investigate the cause of the Privacy Breach;

(b) Assess whether the investigation reveals evidence that may have an impact on the severity of the breach and may result in a high severity Privacy Breach – the PO (or delegate(s)) will then decide whether the investigation will proceed according to the high severity Privacy Breach procedure;

(c) Confirm with the PO (or delegate(s)) (if applicable) if internal or external notification is required;

(d) Address the breach;

(e) Complete a Privacy Breach Investigation Report as described in Attachment G5 and, if applicable, submit to the PO (or delegate(s).

THE PO SHALL APPROVE ALL INTERNAL/EXTERNAL NOTIFICATIONS.

1.4 BREACH POST-MORTEM AND PREVENTIVE MEASURES

Once the Privacy Breach, whether low or high severity, has been handled, it needs to be reviewed to identify process improvement and the necessary actions that may be required to prevent future Privacy Breaches to occur. The PO (or delegate(s)) shall:

(a) Conduct a debrief session with key contributors who were actively involved in the privacy breach response process to identify potential process improvement;

(b) Determine if additional action is required to prevent future breaches and whether a prevention plan is warranted. As part of this assessment, the PO (or delegate(s)) and relevant stakeholders should consider the significance of the Privacy Breach and whether it was systemic or an isolated occurrence;

(c) Coordinate the development of a prevention plan (as required) while taking into consideration the recommendations outlined in the Privacy Breach Investigation Report. The prevention plan may include, but is not limited to, the following:

- An assessment of both physical and informational security practices;
- Privacy breach response process improvement;
- A review of policies and procedures and any changes to reflect the lessons learned from the Privacy Breach investigation;
- A review of relevant / applicable employee training practices;
- The requirement for employee disciplinary measures;
- A review of service delivery/outsourcing partners.

1.5 RECORDKEEPING

The PO (or delegate(s)) shall ensure that Suspected Privacy Breaches and Privacy Breaches have been properly documented and that the Privacy Breach Investigation Report has been stored for future reference.

Records of all Privacy Breaches (whether high or low severity), must be retained for a minimum of 2 years after the day on which Dialogue determined that the breach has occurred.

1.5.1 INFORMATION TO BE INCLUDED IN RECORD

Information allowing Dialogue to assess whether the Privacy Breach created a risk of harm to the Affected Individuals shall be documented in the Privacy Breach Investigation Report (see Attachment G5).

1.5.2 MODIFICATIONS TO SYSTEMS AND PROCEDURES

Any modification to Dialogue systems or procedures to prevent future Privacy Breaches should be documented in the records, including:

(a) The results of any assessment of physical or informational security;

(b) Any changes to policies and procedures to reflect lessons learned from the Privacy Breach and investigation;

(c) Any review or modification of employee training practices;

(d) Whether employee discipline was administered;

(e) Any changes to contractual arrangements with business partners or others;

(f) The date and result of any internal or external audit to ensure that a prevention plan has been fully implemented.

2 ADDITIONAL INFORMATION

2.1 COMPLIANCE

Non-compliance by employees with this Procedure could result in disciplinary measures, up to and including termination.

2.2 INTERPRETATION

Responsibility for the interpretation of this Procedure rests with the PO (or delegate(s)).

2.3 REVIEW

This Procedure will be reviewed every two (2) years or whenever warranted by a Privacy Breach, new regulatory requirements, or other compelling reasons.

b. G4. Guidance on reporting breaches to privacy commissioners and notifying Affected Individuals

LAW	IS REPORTING/ NOTIFICATION MANDATORY?	DETAILS
PIPEDA Applies if affected individuals are not Dialogue employees (i.e. they are clients/members); and are residing in a province other than Alberta, BC and Quebec	**Yes** (Starting November 1, 2018) Reporting to regulator and notification to affected individuals is mandatory.	**Threshold:** Organizations must notify individuals in cases of breaches if it is "reasonable in the circumstances to believe that the breach creates a real risk of significant harm to an individual" and report to the Office of the Privacy Commissioner of Canada ("**OPC**"). The definition of "significant harm" is an open-ended definition that includes bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on the credit record and damage to or loss of property. The factors for identifying whether there is a real risk of significant harm are "the sensitivity of the personal information involved in the breach" and "the probability that the personal information has been, is being or will be misused". **Content of report to OPC:** The report to the OPC must include: ● a description of the circumstances of the breach and, if known, the cause; ● the day on which, or the period during which, the breach occurred or, if neither is known, the approximate period; ● a description of the personal information that is the subject of the breach to the extent that the information is known; ● the number of individuals affected by the breach or, if unknown, the approximate number; ● a description of the steps that the organization has taken to reduce the risk of harm to affected individuals that could result from the breach or to mitigate that harm; ● a description of the steps that the organization has taken or intends to take to notify affected individuals of the breach; ● and the name and contact information of a person who can answer, on behalf of the organization, the OPC's questions about the breach. **Content of notification to affected individuals**: The notification to affected individuals must include: ● a description of the circumstances of the breach; ● the day on which, or period during which, the breach occurred or, if neither is known, the approximate period; ● a description of the personal information that is the subject of the breach to the extent that the information is known; ● a description of the steps that the organization has taken to reduce the risk of harm that could result from the breach; ● a description of the steps that affected individuals could take to reduce the risk of harm that could result from the breach or to mitigate that harm; ● and contact information that the affected individual can use to obtain further information about the breach. **Form and manner of the notification to affected individuals**: Direct notification must be given to the affected individual in person, by telephone, mail, email or any other form of communication that a reasonable person would consider appropriate in the circumstances. Indirect notification is acceptable if: direct notification would be likely to cause further harm to the affected individual; direct notification would be likely to cause undue hardship for the organization; or the organization does not have contact information for the affected individual.

		Timing: Report to the OPC and notification to affected individuals must be given as soon as feasible after the organization determines that the breach has occurred. **Penalty:** An organization who knowingly contravenes the obligation to report the breach to OPC and to notify the affected individuals may be guilty of an offence punishable on summary conviction and liable to a fine not exceeding $10,000 or an indictable offence and liable to a fine not exceeding $100,000.
Alberta PIPA Applies if affected individuals are residing in Alberta (they may be employees) **Alberta HIA** Applies if affected individuals	**Yes** Reporting to regulator is mandatory and regulatory may instruct organization to notify individuals (if not already done by the organization - in practice, businesses usually notify the Alberta OIPC at the same time as affected individuals)	**Threshold:** An organization having Personal Information under its control must provide notice to the Office of the Information and Privacy Commissioner ("**Alberta OIPC**") of any incident involving the loss of or unauthorized access to or disclosure of the Personal Information where a reasonable person would consider that there exists a "real risk of significant harm" to an individual as a result of the loss or unauthorized access or disclosure. **Content of notice to the Alberta OIPC**: A notice to the Alberta OIPC must include: ● a description of the circumstances of the loss or unauthorized access or disclosure; ● the date on which or time period during which the loss or unauthorized access or disclosure occurred; ● a description of the personal information involved in the loss or unauthorized access or disclosure; ● an assessment of the risk of harm to individuals as a result of the loss or unauthorized access or disclosure; ● an estimate of the number of individuals to whom there is a real risk of significant harm as a result of the loss or unauthorized access or disclosure; ● a description of any steps the organization has taken to reduce the risk of harm to individuals; ● a description of any steps the organization has taken to notify individuals of the loss or unauthorized access or disclosure; ● the name of and contact information for a person who can answer, on behalf of the organization, the Alberta OIPC's questions about the loss or unauthorized access or disclosure. **Content of notification to affected individuals**: A notification to affected individuals must include: ● a description of the circumstances of the loss or unauthorized access or disclosure, ● the date on which or time period during which the loss or unauthorized access or disclosure occurred, ● a description of the personal information involved in the loss or unauthorized access or disclosure, ● a description of any steps the organization has taken to reduce the risk of harm, and ● contact information for a person who can answer, on behalf of the organization, questions about the loss or unauthorized access or disclosure. **Form and manner of the notification to affected individuals**: Notification must be given directly, but may be given to the individual indirectly if the Commissioner determines that direct notification would be unreasonable in the circumstances. **Timing**: Notice to the Alberta OIPC must be given without unreasonable delay. Notification to individuals must be given within a time period determined by the Alberta OIPC (if not already done by the organization). **Penalty:** Failure to report the breach to the Alberta OIPC – when it should have been reported – is an offence under the Alberta PIPA, for which an organization is liable to a fine of not more than $100,000 **Threshold**: when any individually identifying health information under the custody or control of a custodian is lost, or there is an unauthorized access to or disclosure of individually identifying health information, the Custodian (or Information Manager, where designated) must evaluate the **risk of harm** to the individual who is the subject of that information in determining whether or not to proceed with notification to that individual, the Information and Privacy Commissioner, and the Minister of Health (section 8.1 and 60.1 HIA).

are residing in Alberta and their health information are affected.	**Yes** Reporting to the regulator (OIPC), the Minister of Health and notification to affected individuals is mandatory.	As part of its Information Management Program, Dialogue undertakes to provide notice to the appropriate bodies and individuals, when notice is required by Applicable Privacy Legislation. To enable Dialogue to fulfil this requirement, Custodians undertake to immediately inform Dialogue's Privacy Officer of any known or suspected loss or theft of, or unauthorized access to, use or disclosure of, Health Information. In the other way, if Dialogue becomes aware of a security incident concerning the health information of an individual under the care of the Custodian, Dialogue must as soon as possible notify the Custodian. Section 8.2 of the Health Information Regulation sets out the factors that custodians must consider when determining if the breach created any risk of harm to any individual. The assessment of harm must be done by the custodian and Dialogue as Information Manager. When the custodian determines that there is a risk of harm due to a breach, notice is to be given in writing to the affected individual(s), the Information and Privacy Commissioner of Alberta, and the Minister of Health. **Form and content of Notice to the individual, the Information and Privacy Commissioner, and the Minister of Health** are explained in this document under the section "HIGH SEVERITY PRIVACY BREACH RESPONSE PROCEDURE". For more information, it is advised to consult the following guideline: *Health information act guidelines and practices manual | chapter 14 duty to notify* (pages 86-91.) **Timing:** The HIA requires a custodian to, **as soon as practicable,** give notice in accordance with the regulations of a loss of, unauthorized access to, or disclosure of individually identifying health information in the custody or control of the custodian if there is a risk of harm to an individual as a result of the loss or unauthorized access or disclosure.
BC PIPA Applies if affected individuals are residing in BC (they may be employees)	**No (although recommended)**	The BC Office of the Information and Privacy Commissioner has adopted guidelines for managing security breaches, recommending the notification to individuals and the privacy commissioners in the event that there is a risk of harm for affected individuals.[2] When dealing with a Privacy Breach affecting individuals in BC, Dialogue may consider notifying the regulator of such a province for strategic reasons. The larger the breach and the more likely affected individuals in BC are to find out of the breach, Dialogue may consider reporting to the BC regulator and affected individuals in the province, also taking into account the following factors: ● Regulators exchange information about breach reports with each other, therefore the BC regulator will learn of the breach and contact the organization for more information. ● The breach may be publicized if a certain number of customers are notified, which may inform customers in other provinces or the media. ● The Alberta OIPC will eventually publish on its website its findings with respect to the breach report it has received.
Quebec Private Sector Act Applies if		**Definition**. New section 3.6 defines a "confidentiality incident" as an unauthorized access, use or disclosure of personal information, loss of personal information, or other breach in the protection of such information. As such, any breach, violation or incident involving personal information will fall under the application of section 3.6. Some of the different types of confidentiality incidents include

[2] It should also be noted that under the common law regime, there is a general obligation for an organization to mitigate the consequences of an organization's failure to use appropriate security safeguards to protect Personal Information. Depending on the severity of the incident, notifying affected individuals may mitigate eventual damages.

affected individuals are residing in QC (they may be employees)		phishing, malware deployment, ransomware attacks, botnets, brute force attacks, sending personal information to the wrong email address, etc. It is interesting to note that Québec is the only jurisdiction in Canada to include unauthorized use of personal information in its definition of confidentiality incident. This inclusion could lead to uncertainties as to whether the use of personal information without consent for marketing purposes, for example, could be considered a "confidentiality incident". While such an interpretation could lead to an overabundance of incident notifications to the CAI and to the individuals involved, companies will need to exercise judgment in assessing the risk of injury, as explained in the following sections. **Mitigation of risk.** Section 3.5 requires businesses that have "cause to believe" that a confidentiality incident has occurred to take "reasonable measures to reduce the risk of injury and to prevent new incidents of the same nature". This requirement applies to any entity or third party that has custody or control of personal information, such as a service provider or subcontractor. In practice, this means that organizations will need to take all appropriate and reasonable steps to prevent injury to individuals as a result of the incident. The steps to be taken will depend on the type of incident and the applicable context, but could include, for example, thorough investigations and any security measures to contain and eradicate the incident. We note that this obligation applies regardless of the seriousness of the risk. A good way to mitigate the risk of injury is to have a robust security program based on industry best practices, and to have the organization's incident response plan tested by incident response experts. **Risk of serious injury assessment.** All confidentiality incidents will be subject to a "risk of serious injury" assessment process to determine whether the incident in question should be notified to the CAI and the individuals involved. The notion of "risk of serious injury" proposed by the Québec legislator is subtly distinguished from the notion of "real risk of significant injury" provided for in PIPEDA and Alberta's PIPA, as the word "real" has been omitted. In addition, unlike PIPEDA, Bill 64 does not provide a definition or examples of serious injury, but does set out key factors to be considered in assessing the level of seriousness of the risk of injury: (i) **The sensitivity of the information involved.** Information that, because of its nature (e.g., medical, biometric or otherwise intimate) or the context of its use, entails a high level of reasonable expectation of privacy will increase the risk of injury; (ii) **The anticipated consequences of its use.** For example, whether the compromised information is likely to be used to commit fraud or identity theft; (iii) **The likelihood that it will be used for injurious purposes.** If, for example, the information has been exfiltrated from the organization's servers or published on the Dark Web, it is likely to be used for injurious purposes. Although the assessment criteria for PIPEDA and PIPA are superficially similar to Bill 64 test, we do not rule out the possibility that the CAI will interpret the notification requirements more narrowly, particularly given the omission of the word "real" in its definition of "risk of serious injury". In any event, the Privacy Officer should be consulted in making this assessment (section 3.7 in fine). **Notification of incidents.** If the organization determines that the incident poses a risk of serious injury, it will be required to notify the CAI and any individual affected by the incident, failing which the CAI may order the organization to do so. It is also provided that the organization may, at its discretion, notify any person or organization that may be able to reduce the risk of injury, but with only the

		personal information necessary to do so (without the consent of the individual concerned). In the latter case, the Privacy Officer shall record the disclosure. There is no time limit for reporting incidents, but reporting must be done "promptly", according to section 3.5. By comparison, PIPEDA and PIPA require notification as soon as possible to the OPC in the event that a breach of security measures presents a "real risk of significant harm". In Europe, the GDPR requires disclosure of a breach to the country's supervisory authority no later than 72 hours after the breach when it poses a risk of injury. If a confidentiality incident occurs at a third party service provider or subcontractor to whom personal information has been outsourced, there may be contractual requirements for notification of incidents. However, since the notification obligations of Bill 64 apply to any organization regardless of their role in the processing of personal information, a service provider or subcontractor may be required to report the incident since reporting the obligation applies to "any person carrying on an enterprise who has cause to believe that a confidentiality incident involving personal information the person holds has occurred." At the federal level, PIPEDA requires an organization to report a breach involving personal information under its control. It is unclear if the Québec legislator voluntarily omitted to mention the notion of control and whether the CAI would expect both the organization acting as the data controller and its service provider (and subcontractor) to report the incident which may require some type of coordination between these organizations. Notwithstanding the foregoing, it should be noted that an individual affected by a confidentiality incident will not have to be notified if such notification would impede an investigation by a person or body that, by law, is responsible for preventing, detecting or suppressing crime or offences under section 3.5. **Formalities.** Bill 64 does not impose any particular form on the notices that organizations must send to the CAI and to the individuals concerned in order to fulfil their notification obligations. However, section 3.5 para. 4 gives the government the power to determine, by regulation, the content and manner of such notices. Until such a regulation is adopted, organizations can use the confidentiality incident reporting form available on the CAI website (in French only), which sets out the various information to be disclosed about the context of the incident and the steps to be taken. Finally, organizations will have to keep a register of confidentiality incidents, a copy of which must be sent to the CAI upon request, pursuant to section 3.8. A government regulation may determine the content of this register as well as the time limits for its retention. By way of comparison, the Breach of Security Safeguards Regulations provide that organizations must keep a record of all security breaches for twenty-four months after the date on which the organization concludes that a breach has occurred, regardless of the risk of injury.

c. G5. Privacy Breach Investigation Report Template

A Dialogue Privacy Investigation Report needs to be completed for all Privacy Breaches and Suspected Privacy Breaches.

The Dialogue Privacy Investigation Report template provides guidance on how to complete the investigation report and the level of detail expected.

Glossary

- Detection - The method by which the incident was detected.
- Mitigation - The method by which we removed the wrongful access to the breached data.
- Diagnosis - The method by which we figured out what was causing the impact.
- Direct Cause - The event that triggered the failure. This might be human error.
- Root Cause - The underlying cause(s) of the failure. This is never human error.

d. Part I: Post-Mortem

(To be filled during the Post-Mortem meeting or as soon as possible by the designated Dialogue employee)

At Dialogue, we conduct Post-Mortems upon discovery of a Privacy Breach. This Post-Mortem is generally led by IT, Security and sometimes Privacy. The post mortems are stored on Notion.

The Post-Mortem includes the following elements:

■ **Timeline**

A detailed timeline of events. Talk about what happened and at what time, including events before the incident if they are relevant.

■ **Data**

Include images, logs, graphs that demonstrate the problem and the impact. Do not forget to add the impact on the SLO error budget if SLOs were impacted.

■ **Customer Impact**

How and when did our customers experience the problem?

How and when did they experience the recovery?

■ **Trigger**

What was the trigger of the problem?

What could we have done differently to prevent the trigger of the failure? Could we have prevented it before it had any impact?

What did we do well and how did we get lucky?

■ **Detection**

How and when did our automated systems detect the problem?

How and when did our people become aware of the problem?

What could we have done differently to detect this failure sooner? Could we have detected it before it had any impact?

What did we do well and how did we get lucky?

- **Mitigation**

  How and when did we mitigate the impact?

  What could we have done differently to mitigate the impact of this failure faster?

  What did we do well and how did we get lucky?

- **Diagnosis**

  How and when did we diagnose the direct cause of the problem?

  What could we have done differently to diagnose the direct cause of the failure faster?

  What did we do well and how did we get lucky?

- **Resolution**

  How and when did we permanently fix the problem?

  What did we do well and how did we get lucky?

- **Customer and Member Experience**

  What could we have done differently to improve the customer's experience during the incident?

  Could we have informed them before they experienced the problem?

  What did we do well and how did we get lucky?

  What could we have done to reduce the number of people affected by the impact of this incident?

- **Further Analysis**

  How did the engineering culture/process at Dialogue contribute in any stage of the incident? What changes would you propose?

  Could automation of any existing process have helped lessen the impact in any stage of the incident?

- **Summary**

  When did the incident begin and when was it mitigated?

  What happened?

  What was the impact for our users?

  What was the impact for our clients?

  What did or will we do to ensure this doesn’t happen again?

- **Action Items**

Part II: Legal Analysis
(To be prepared by a member of the P&SC, the PO or any of its designate)

Author(s): *list authors*

To be completed only after the other sections have been filled and reviewed by the individuals involved in the incident. Shall contain:

- **Overview of the Incident**

Include the date and summary of the event. Refer to Post-Mortem for more details.

- **Information about the individual(s) affected by the incident**

Identification of the Applicable Privacy Legislation (refer to Attachment G4: Guidance on reporting breaches to privacy commissioners and notifying Affected Individuals)

Analysis regarding whether incident meets the applicable risk threshold (consider the factors detailed in Attachment G2)
Has the applicable threshold been reached?

- **Analysis on who to notify**

Decision about whether to notify Affected Individual(s), privacy regulator(s) and/or client(s).

- **Examination of Dialogue Processes**

Review the Dialogue processes to see whether they caused or contributed to the incident.

- **Summary of corrective actions**

Explanation of the actions taken to promptly address the incident.

- **Action items**

Describe any action items needed.

- **Determination for escalation to Sun Life**

Evaluate whether the privacy incident meets the threshold for notification to Sun Life. Consider the following three factors to determine the incident level:

(i) Intention/Motivation
(ii) Sensitivity of Personal Data
(iii) Number of Impacted Individuals

The Privacy Officer is responsible for making this determination in accordance with applicable policies and procedures.

Version Control:

Version Number	Effective Date	Revision Date	Approval
1	December 5, 2021	December 5, 2021	Alexis Smirnov, Chief Technology Officer
2	April 15, 2022	April 15, 2022	Alexis Smirnov, Chief Technology Officer
2.1	March 10, 2023	March 10, 2023	Alexis Smirnov, Chief Technology Officer
2.2	April 18, 2023	Apr 18, 2023	Alexis Smirnov, Chief Technology Officer
2.3	October 3, 2023	October 3, 2023	Darryl Campbell, CISO
2.4	August 1, 2024	August 1, 2024	Darryl Campbell, CISO
2.5	October 3, 2024	October 3, 2024	Darryl Campbell, CISO