Dialogue

Deloitte.

System and Organization Controls SOC2—Type 2

Report on Dialogue's Description of its Virtual Health Care system and on the suitability of the design and implementation of its controls, to meet the criteria for the Security principle throughout the period from April 1, 2023, to March 31, 2024.

Prepared in accordance with CPA Canada Handbook—Assurance (Section 3000)

September 19, 2024—**CONFIDENTIAL**

Table of contents

Table des matières

Notice of confidentiality

This report, including the description of tests of controls and results thereof in Section IV is intended solely for the information and use of the Service Organization, user entities of the Service Organization's system, prospective user entities, independent auditors and practitioners providing services to such user entities and regulators who have a sufficient understanding to consider it. This report is not intended to be and should not be used by anyone other than these specified parties. Except for these specified parties, this document may not be reproduced in any form or by whatever mechanical or electronic process whatsoever, including electronic archiving systems, without the written permission. The receiving party is exempt from this restriction for its internal use only.

If you have received this document by error, be advised herewith that reading, reproducing, or distributing it is prohibited. Consequently, we ask that you inform us by email if you have received the document by contacting security@dialogue.co. We also ask that you return the document, along with any copies, to us by regular mail, or, where you have received it electronically, that you destroy all electronic copies. In either case, please provide a written attestation that you have returned or destroyed the copies, as applicable.

Deloitte.

Deloitte LLP
La Tour Deloitte
1190 avenue des
Canadiens-de-Montréal
Suite 500
Montréal QC-H3B 0M7
Canada

Tel: 514-393-7115
Fax: 514-390-4115
www.deloitte.ca

Section 1 – Independent Service Auditor's Report

To: The management of Dialogue Health Technologies Inc.

Scope

We have been engaged to report on Dialogue Health Technologies Inc.'s ("service organization", "Dialogue") accompanying description of the Virtual Health Care system titled "Dialogue Health Technologies Inc.'s Description of the Virtual Health Care System" throughout the period April 1, 2023 to March 31, 2024 ("description") based on the criteria for a description of a service organization's system in DC section 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (AICPA, Description Criteria), ("description criteria") and the suitability of the design and operating effectiveness of controls stated in the description throughout the period April 1, 2023 to March 31, 2024, to provide reasonable assurance that Dialogue's service commitments and system requirements were achieved based on the trust services criteria relevant to security ("applicable trust services criteria") set forth in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria).

The information included in Section V, "Other Information Provided by Dialogue Health Technologies Inc. That is Not Covered by the Service Auditor's Report", is presented by management of Dialogue to provide additional information and is not a part of the description. Information about Dialogue's responses to Deloitte's exception has not been subjected to the procedures applied in the engagement to report on the description and the suitability of the design and operating effectiveness of controls to achieve Dialogue's service commitments and system requirements based on the applicable trust services criteria, and accordingly, we express no opinion on it.

As indicated in the description (see pages 29 and 30), Dialogue uses subservice organizations to provide cloud hosting, source code management, account management and authentication services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Dialogue, to achieve Dialogue's service commitments and system requirements based on the applicable trust services criteria. The description presents Dialogue's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Dialogue's controls. The description does not disclose the actual controls at the subservice organizations. Our engagement did not include the services provided by the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Dialogue, to achieve Dialogue's service commitments and system requirements based on the applicable trust services criteria. The description presents Dialogue's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Dialogue's

Deloitte.

controls. Our engagement did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

Service Organization's Responsibilities

Dialogue Health Technologies Inc. is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Dialogue Health Technologies Inc's service commitments and system requirements were achieved. Dialogue Health Technologies Inc. has provided the accompanying statement titled “Management of Dialogue Health Technologies Inc.’s Statement” (“statement”) about the description and the suitability of design and operating effectiveness of controls stated therein. Dialogue Health Technologies Inc. is also responsible for preparing the description and statement, including the completeness, accuracy, and method of presentation of the description and statement; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Our Independence and Quality Management

We have complied with the relevant rules of professional conduct / code of ethics applicable to the practice of public accounting and related to assurance engagements, issued by various professional accounting bodies, which are founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality, and professional behavior.

The firm applies Canadian Standard on Quality Management 1, *Quality Management for Firms that Perform Audits or Reviews of Financial Statements*, or Other Assurance or Related Services Engagements, which requires the firm to design, implement and operate a system of quality management, including policies or procedures regarding compliance with ethical requirements, professional standards, and applicable legal and regulatory requirements.

Service Auditor's Responsibilities

Our responsibility, under this engagement, is to express an opinion on the description and on the suitability of design and operating effectiveness of controls stated in the description based on the evidence we have obtained.

Our engagement was conducted in accordance with Canadian Standard on Assurance Engagements 3000, Attestation Engagements Other than Audits or Reviews of Historical Financial Information, set out in the CPA Canada Handbook - Assurance. This standard requires that we plan and perform our engagement to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed and operated effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

A reasonable assurance engagement to report on the description of a service organization's system and the suitability of the design and operating effectiveness of controls involves the following:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements.
- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed and did not operate effectively.
- Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria.

Deloitte.

- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria.
- Testing the operating effectiveness of controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria.
- Evaluating the overall presentation of the description.
- Performing such other procedures as we considered necessary in the circumstances.

Inherent Limitations

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual report users may consider important to meet their informational needs.

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design and operating effectiveness of controls is subject to the risk that controls may become ineffective because of changes in conditions or that the degree of compliance with policies or procedures may deteriorate.

Description of Tests of Controls

The specific controls we tested, and the nature, timing, and results of those tests are listed in *Section 4* of this report.

Opinion

In our opinion, in all material respects,

- the description presents Dialogue Health Technologies Inc.'s IT systems that was designed and implemented throughout the period April 1, 2023, to March 31, 2024, in accordance with the description criteria.
- the controls stated in the description were suitably designed throughout the period April 1, 2023 to March 31, 2024, to provide reasonable assurance that Dialogue Health Technologies Inc.'s service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period and if the subservice organization and user entities applied the complementary controls assumed in the design of Dialogue Health Technologies Inc.'s controls throughout the period April 1, 2023 to March 31, 2024.
- the controls stated in the description operated effectively throughout the period April 1, 2023 to March 31, 2024, to provide reasonable assurance that Dialogue Health Technologies Inc.'s service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of Dialogue Health Technologies Inc.'s controls operated effectively throughout the period April 1, 2023 to March 31, 2024.

Deloitte.

Restricted use

This report, including the description of tests of controls and results thereof in Section 4, is intended solely for the information and use of Dialogue, user entities of Dialogue's virtual health care system during some or all of the period April 1, 2023 to March 31, 2024, business partners of Dialogue subject to risks arising from interactions with the virtual health care system, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization.
- How the service organization's system interacts with user entities, business partners, subservice organizations, and other parties.
- Internal control and its limitations.
- Complementary user entity controls and complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's commitments and system requirements.
- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services.
- The applicable trust services criteria.
- The risks that may threaten the achievement of the service organization's service commitments and system requirements and how controls address those risks.

This report is not intended to be, and should not be, used by anyone other than these specific users.

Deloitte LLP

Chartered Professional Accountants
Montreal, Québec
September 19, 2024

[1] CPA auditor, public accountancy permit N° A131397

Section 2 – Statement by Management of Dialogue Health Technologies Inc.

September 19, 2024

We have prepared the accompanying description of Dialogue Health Technologies Inc 's ("service organization", "Dialogue") virtual health care system titled "Dialogue Health Technologies Inc.'s Description of the Virtual Health Care System" throughout the period April 1, 2023 to March 31, 2024 ("description") based on the criteria for a description of a service organization's system in DC section 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (AICPA, Description Criteria) ("description criteria"). The description is intended to provide report users with information about the virtual health care system that may be useful when assessing the risks arising from interactions with Dialogue's system, particularly information about system controls that Dialogue has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to security ("applicable trust services criteria") set forth in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria).

Dialogue uses subservice organizations to provide cloud hosting, source code management, account management and authentication services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Dialogue, to achieve Dialogue's service commitments and system requirements based on the applicable trust services criteria. The description presents Dialogue's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Dialogue's controls. The description does not disclose the actual controls at the subservice organizations.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Dialogue, to achieve Dialogue's service commitments and system requirements based on the applicable trust services criteria. The description presents Dialogue's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Dialogue's controls.

We confirm, to our knowledge and belief, that:

a. The description presents Dialogue's virtual health care system that was designed and implemented throughout the period April 1, 2023, to March 31, 2024, in accordance with the description criteria.

b. The controls stated in the description were suitably designed throughout the period April 1, 2023 to March 31, 2024, to provide reasonable assurance that Dialogue's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and if the subservice organizations and user entities applied the complementary controls assumed in the design of Dialogue's controls throughout the period April 1, 2023 to March 31, 2024.

c. The controls stated in the description operated effectively throughout the period April 1, 2023, to March 31, 2024, to provide reasonable assurance that Dialogue's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of Dialogue's controls operated effectively throughout the period April 1, 2023, to March 31, 2024.

Name: Darryl Campbell

Title: Chief Information Security Officer

Dialogue Health Technologies Inc.

Section 3 – Dialogue Health Technologies Inc. – Description of its Virtual Health Care System

Introduction

The control environment is a fundamental and critical part of Dialogue Health Technologies Inc.'s ("Dialogue") activities. It defines the mindset for the entire organization and influences the control awareness of its team. The components of the control environment support Dialogue's corporate values and are as follows:

- Management's commitment to excellence
- Dialogue's organizational structure
- Assignment of authority and responsibility
- Oversight and direction provided by Senior Management and the Board of Directors
- Risk management process with mitigation plan
- Communication of relevant information through various channels
- Monitoring the effectiveness of controls and their enhancement

3.1. Overview of Operations

3.1.1 Company Background

Dialogue was founded in 2016 by Cherif Habib, Anna Chif and Alexis Smirnov, who had the vision to deliver personalized quality health care to everyone.

Dialogue was founded with the strong conviction that technology would play a pivotal role in improving health care and lives. Initially, Dialogue focused exclusively on employers (i.e., plan sponsors) as its main clients, as its founders believe that this approach is the most complementary to the current Canadian healthcare system and existing regulations.

Dialogue is fully vertically integrated. The company has developed its own technology, controlled all operations, and had a dedicated network of nurses, physicians and other healthcare professionals who have been formally vetted and trained to deliver the highest quality of service. Management strongly believes that this tight integration of technology and services creates the best experience for its Clients and Members (see definition on next page).

Dialogue is headquartered at 390 Notre-Dame West #200, Montreal, Quebec. Dialogue's office is protected by locking mechanisms, 24-hour video surveillance and an alarm system (C.6.4.1).

On October 3rd, 2023, Sun Life indirectly acquired all the issued and outstanding common shares in the capital of Dialogue, other than those already owned indirectly by Sun Life and certain common shares owned by members of Dialogue's management.

Dialogue will remain headquartered in Montreal and intends to continue to operate as a standalone entity. This change is not expected to negatively impact the control environment in which Dialogue operates. Dialogue intends to continue executing its business plan and serving its partners and customers, each of which continues to have access to Dialogue's services and capabilities and benefits from the continued innovation resulting from the combined strengths of both organizations.

3.1.2 Description of Services Provided

Dialogue provides access to virtual health and wellness services to employers, associations, insurers, and other organizations (collectively "Clients") for use by their employees, customers, participants and/or members ("Users") respectively. The Users and their families (if applicable), collectively defined as "Members", are all eligible to use these services, for a fee paid by the Clients. The services are provided by medical personnel employed or contracted by Dialogue through the virtual healthcare system on a Dialogue-owned technology platform.

Through the virtual care service, Members have access to an Integrated Health Platform, which can include one or many of the following services:

- **Primary Care Services**
  - Unlimited consultations via multiple channels such as video, messaging, and phone with service providers (care managers, registered nurses, nurse practitioners or physicians)
  - Prescriptions and renewals when medically indicated.
  - Referrals to specialists or other healthcare providers, when medically indicated.
  - Care navigation
  - Access by end- user to all details of their care plan, health history, physician recommendations and completed forms.
  - Physician evaluations
- **Mental Health+**
  - Questionnaire-based screening
  - Habit-forming coaching sessions
  - Mental Health evaluations
  - Psychotherapy sessions and follow-ups
  - iCBT Program
- **Employee Assistance Program**
  - Mental Health services (questionnaire-based screening, habit-forming coaching sessions)
  - Family, marital and relationship services (questionnaire-based screening, counseling sessions)
  - Child and elder care services (general guidance and information services, Ortho pedagogy, occupational therapy, referral services)
  - Work and career advisory services (general guidance and information services provided by case managers and career counselors)
  - Manager consultation services (coaching of employees by mental health specialist and career counselors)
  - Access to allied health professionals via the virtual platform (pay per service)
  - Additional services provided by external partners:
    - Legal services (civil, family, criminal, property, and will/estate law counseling)
    - Financial services (counseling with a financial professional)
    - Critical incident response service (support consultations, action plan development, consultation of employees with trauma specialists, coaching services)
- **Wellness Program**
  - Library of expert-backed content, grouped into healthy habits and other wellness topics.
  - Wellness communication campaigns aligned to client awareness initiatives.
  - Wellness Progress tracker and personalized content
  - Recurring and custom activity challenges

- Client Reporting on key organizational wellness metrics
- Integration with wearables and activity trackers

Dialogue also operates physical clinics for Clients that require this service. Controls specific to the operation of physical clinics are not included in the scope of this report.

This report covers the services provided by Dialogue's Canadian operations. However, although this report does not specifically cover infrastructures outside of Canada, Optima, Tictrac and eHH operations, those operations do benefit from certain common controls covered by this report.

3.2 Components of the system used to provide the DPOI services.

3.2.1 Infrastructure

The system production environment is hosted by Amazon AWS, an infrastructure cloud service provider. The controls related to the subservice organization's responsibilities are not included in the scope of this report ('carve-out' method). The subservice organization issues a separate SOC 2 Type II audit report.

3.2.2 Software

Dialogue utilizes various applications and tools to support their services. These applications and tools include:

- **Applications**

Member App (iOS, Android, Web): This application is designed to provide Members with access to Dialogue's services. It offers messaging and video capabilities, allowing Members to communicate with healthcare professionals and access the necessary healthcare support.

Care Platform (Web, Mac OS, and Windows): The Care Platform is designed to be used by care professionals who provide medical services to the Members. It includes messaging, video capabilities, Member record management and clinic management capabilities.

Presto (a.k.a. HR Administrator Console) (Web): Presto is an application designed for Dialogue's Clients, enabling them to manage the services within their organizations. It provides Clients with the ability to manage the list of Users who have access to the services. This application streamlines the administrative tasks related to managing the service.

- **Tools**

Dialogue relies on several key tools to support their service commitments and system requirements. These tools include:

GitHub: Dialogue utilizes GitHub as a source control and source code repository. It allows for efficient version control and collaboration among developers working on the Dialogue platform.

Okta: Okta is an Identity and Access Management (IAM) tool that allows for the secure management of user access to various applications, while offering several features such as Single Sign-On (SSO) and Multi-Factor Authentication (MFA).

Sentinel One: Sentinel One is an Endpoint Detection and Response (EDR) tool that provides threat detection and response capabilities. By utilizing artificial intelligence and machine learning, Sentinel One offers real-time protection against a wide range of threats, including malware, ransomware, and zero-day attacks.

Kandji: Kandji is a Mobile Device Management (MDM) tool specifically designed for Apple environments. It enables businesses to manage, secure, and deploy macOS, iOS, iPadOS, and tvOS devices.

Cloudflare : Cloudflare is an advanced Web Application Firewall (WAF) that protects websites against various types of online attacks, including SQL injection attacks, attempts to execute malicious code, brute force attacks, and many others.

AWS: Amazon Web Services (AWS) is a comprehensive and market-leading cloud services platform provided by Amazon. It offers a global infrastructure of data centers, allowing businesses to deploy and manage their applications and services without the need for local physical infrastructure.

UltiPro: UltiPro is an integrated human resources management platform developed by UKG, which offers comprehensive solutions for managing payroll, talent, benefits, as well as employee time and attendance. UltiPro also enables benefits enrollment management and workforce scheduling.

PagerDuty: PagerDuty is an on-call scheduling and incident management system used by Dialogue. It helps in effectively managing and resolving any incidents or issues that may arise in the system.

CircleCI: Dialogue employs CircleCI as a continuous integration tool. It automates the process of building, testing, and deploying software, ensuring a smooth and efficient development workflow.

Terraform: Terraform is an automated deployment framework used by Dialogue for network configuration deployment (VPC, Route53), database deployment (RDS), storage volume deployment (EBS), and virtual machine cluster deployment (EKS). It simplifies the process of provisioning and managing infrastructure resources within the Dialogue system.

3.2.3 Principal Service Commitments and System Requirements

Dialogue has designed its policies and processes to provide a secure environment for its systems and for the data that is processed, in line with its objectives, based on commitments to customers, laws and regulations, and any operational requirements Dialogue has established for its services. These commitments may include service levels related to system uptime and issue response and resolution times. As applicable, Dialogue's service and security commitments are documented and communicated in service agreements and contracts with customers.

Internal controls in place to support Dialogue's service and security commitments may include but are not limited to the following:

- Logical access security policies, designed to prevent unauthorized persons or systems from gaining access to systems used to process customer data.
- Technical and organizational measures to protect customer data against loss, alteration, and unauthorized disclosure or access — these measures include data encryption and other protective security controls.
- Change management standards applied during the development, deployment, and maintenance of applications and systems.
- Hiring practices that require background checks, confidentiality agreements, and a commitment to Dialogue's code of conduct upon hire.
- System monitoring to detect and alert on potential security incidents, with an incident response policy and process to respond to incidents.
- Security tests and assessments of systems (e.g., penetration tests and vulnerability scans).
- Reviews of key vendors to evaluate their security posture, measures and/or control conformance.

3.3. Overview of Internal Controls

Dialogue's internal controls are encompassed in a set of policies and procedures, with oversight by the Senior Executive Management team ("SEMT"), the Executive Management Team ("EMT") and other personnel in order to provide reasonable assurance regarding the achievement of its objectives in the following categories:

- Quality care
- Efficiency of operations

- Compliance with established policies and procedures
- Compliance with applicable laws and regulations
- High Client and Member satisfaction with service and support
- Growth

The Chief Executive Officer ("CEO"), the Chief Technology Officer ("CTO"), the Chief Operations Officer ("COO"), the Chief Financial Officer ("CFO"), the Senior VP Commercial and the Senior VP of Operations compose the SEMT. In addition to the SEMT members, the EMT also includes the Chief Medical Officer ("CMO"), the General Counsel, the Chief Information Security Officer ("CISO"), and a number of Vice-Presidents and Directors.

The description is presented in accordance with the five components of internal control of Dialogue, as established by the COSO Framework:

- Control Environment
- Risk Assessment
- Control Activities
- Information and Communications
- Monitoring

3.3.1 Control Environment

This section discusses Dialogue's culture and its core values, Management's philosophy and operating style, the structure and allocation of authority and responsibilities, Dialogue's policies and procedures, the risk management process and monitoring, and the role of control groups. Dialogue's SEMT & EMT have established and maintain a number of control activities outlined in the dedicated section below, designed to ensure compliance with established policies and procedures.

3.3.1.1 Code of Conduct Core Values

Integrity and ethical values are essential elements of Dialogue's control environment, and they are translated into the design, administration and monitoring of key processes. Integrity and ethical behavior are the products of Dialogue's culture and ethical and behavioral standards, how they are communicated, and how they are monitored and enforced in its business activities.

The Dialogue team shares the following values:

- Core Value #1 - We deeply care.
- Core Value #2 - We are humbly confident.
- Core Value #3 - We are Shackletons.
- Core Value #4 - We have a burning desire to make an impact.
- Core Value #5 - We exude positive energy.

The SEMT communicates Dialogue's core values and behavioral standards to personnel through its actions, ongoing company-wide communications and, formally, through Dialogue's HR Policies and the HR portal. The core values are reviewed and updated by the SEMT as needed (C.1.1.1). The SEMT & EMT highlights the behaviors of those employees who embody those values and behaviours, and the examples set by the SEMT & EMT.

Dialogue's SEMT recognizes its responsibility to foster a strong ethical environment within the organization and to determine that Dialogue's business affairs are conducted with integrity and in accordance with high standards of personal and corporate conduct.

This responsibility is indeed characterized and reflected in Dialogue's HR Policies, which are distributed to all employees of the organization. More specifically, employees are prohibited from misusing information (including personal health information and personally identifiable information), infringing intellectual property rights,

disclosing confidential information of Dialogue's Clients and Members, or from taking any action that is not in the best interest of Dialogue's Clients and Members.

Beyond the standards set by the HR Policies, employees are also required to maintain ongoing compliance with all statements of policies and procedures, and with lawful and ethical business practices, whether or not they are specifically mentioned in the HR Policies. Violations of these policies or other forms of misconduct may lead to disciplinary action up to and including dismissal.

The SEMT monitors employee's compliance with the core values outlined above through the monitoring of internal and external feedback (C.1.1.3).

As well, employee compliance with core values is assessed within the employee performance review process as explicit evaluation criteria evaluated by their manager. Managers monitor employee behaviour and performance throughout the year and assess employee compliance on each of the values in their performance review. This ensures employees are acting in accordance with Dialogue's core values.

3.3.1.2 Executive management participation

SEMT and EMT

Dialogue's Chief Executive Officer ("CEO") manages Dialogue's activities on a daily basis with assistance from the SEMT and EMT, representing all functions of the business. Members of the SEMT draw experience from their former senior roles in other organizations, specializing in software technology, health care, customer service, and management consulting.

The SEMT assigns and, at least annually, evaluates authority, responsibility for operating activities and establishes reporting relationships and authorization hierarchies as part of the ongoing risk assessment and business planning processes including financial and security risks (C.1.3.2).

The SEMT defines corporate objectives that are reviewed by the Board of Directors and communicated across the organization so that all personnel know how their individual actions interrelate and contribute to those objectives and recognize how and for what they will be held accountable. Performance is presented to the Board of Directors every quarter (C.2.2.3).

Lines of authority and responsibility under the CEO are clearly established throughout the organization. These lines of authority and the associated responsibilities are communicated through:

- Job descriptions and role scorecards
- Organizational structure
- Policies and procedures

Managers are responsible to lead employees in complying with Dialogue's policies and procedures. The SEMT holds the following recurring meetings:

- Weekly meetings to address top issues across business functions and monitor KPIs.
- Quarterly meetings (or more as needed) to plan the next quarter(s) and discuss strategy and policy updates.
- Ad hoc meetings for important updates

The SEMT holds weekly meetings (or more as needed) to provide an update on key performance indicators ("KPIs") and functions (C.2.1.2).

During the SEMT meetings, management also evaluates the need for additional tools and resources in order to achieve business objectives, while assessing risks involved (C.3.1.1).

Board of Directors

Dialogue's control environment is influenced by the Board, which provides corporate governance. The Board has 7 members and consists of 2 Dialogue executives and 5 Sun Life Executives. Each member of the Board possesses adequate and relevant experience. The Board is actively involved in and follows the activities of Dialogue's functional groups. Under by-laws and a Board Charter, the responsibilities of the Board of Directors are defined, documented and available to employees and include oversight of the development and performance of internal controls (C.1.2.1).

Management's philosophy and operating style

The CEO, together with the SEMT and EMT, is responsible for directing and controlling operations; establishing, communicating, and monitoring control policies and procedures; and setting the tone for the organization. The importance is placed on adherence to core values, maintaining and evolving business processes and procedures, security, and privacy, and establishing and maintaining sound internal controls over all functional aspects of operations.

Management's philosophy and operating style affect the way Dialogue is managed, including the kinds of business risks that are considered acceptable. Dialogue places a great deal of importance on working to ensure that the integrity and security of its system and related data — including personal health information — are a primary focus and that controls are optimized to mitigate risk in daily operations. Management and specific teams are structured to ensure the highest level of integrity, security and efficiency in Member support and processing.

Formal job descriptions and team meetings and inter-team interactions ensure communication of organizational values, ethics, and behavioural standards. Personnel operate under Dialogue's HR Policies and its Information Security Policy, as well as individual employment and contractor agreements, which include expectation with respect to confidentiality and data protection. The annual security awareness training and other training are conducted to communicate regulations and the importance of privacy and security.

Management is committed to being aware of regulatory and market and economic changes that impact the business, and to closely monitoring and analyzing Member satisfaction, usage patterns, trends, changes, and anomalies.

Organizational structure and assignment of authority and responsibility

Dialogue's organization and distribution of responsibilities and authority provide the framework within which its activities for achieving company-wide objectives are planned, executed, controlled, and monitored.

The assignment of authority and responsibilities includes factors such as how authority and responsibility for operating activities are assigned and how reporting relationships and authorization hierarchies are established. This includes factors relating to business practices, required skill sets and experience, resources and operating licenses (such as licenses to provide medical care). In addition, Dialogue's policies and communications are directed at ensuring that personnel understand company objectives, know how their individual actions impact, and contribute to those objectives, and recognize how and for what they will be held accountable.

Dialogue's SEMT and function leads assign authority and responsibility to key personnel with the skills and experience necessary to carry out their assignments. Those assignments help in achieving corporate objectives, oversight of operating functions and any compliance with applicable regulatory and contractual requirements.

Dialogue's EMT encourages collaboration and individual initiatives in addressing issues and resolving problems.

Roles and responsibilities

Led by the C-level roles and the SEMT, Dialogue's organization includes the following functions:

- Finance
  - Finance – Responsible for managing accounting functions, preparing reports and statistics that detail financial results, and for establishing and maintaining accounting practices to ensure that accurate and

reliable data necessary for business operations is provided and safeguarded. Finance oversees accounts receivable, accounts payable, payroll, budget, forecasting, financing, investor relations and corporate development activities (mergers and acquisitions), as well as corporate and regulatory reporting. Finance is also responsible for billing Clients.
  - Legal – Responsible for providing all legal support to Dialogue's activities, the organization, the CEO, and the Board, on topics such as corporate governance, regulatory compliance, contracts, business development, legal liability assessment, etc.
  - Risk & Compliance - Responsible for designing and deploying risk & compliance policies and processes in support of business objectives and operations and monitoring compliance with those policies.
  - Corporate Development - Responsible for carrying out transactions such as mergers and acquisitions, joint ventures, divestitures, disinvestments, and strategic partnerships.

- Technology
  - IT & Information Security – Responsible for identifying and providing IT needs to Dialogue's entire organization, including office network setup, hardware procurement, IT account administration and management, office productivity tools and services, and internal IT support. The team is also responsible for information security of corporate IT systems and related processes; the corporate IT infrastructure system design; and implementation, maintenance, and lifecycle management of IT systems. The team must maintain the availability and disaster recovery of corporate IT systems. The team is responsible for Level 2 technical Support for Care Platform and coordination of post-mortems for incidents.
  - Software Engineering – Responsible for the software architecture, development and maintenance of all Dialogue systems and applications. Software Engineering interacts with Product Management and other teams to gain a detailed understanding of software requirements, and to validate the results for conformance with expectations and requirements. The development process covers all disciplines of project management, software development and software quality assurance.
  - Quality Assurance – Responsible for assuring that the software releases comply with the functional requirements (including security and privacy), non-functional requirements and usability expectations. Quality Assurance is responsible for tracking software defects across all systems and applications. Quality Assurance is also responsible for maintaining up-to-date and accurate reports on software quality.
  - Site Reliability (DevOps) – Responsible for operational processes; system reliability; selection, setup, and budgeting of third-party services; operational on-call support coverage (including service providers and subservice organizations management); and monitoring and alerting security compliance and penetration testing schedules. Moreover, Site Reliability has the responsibility for applying the Incident Management Process when a security breach occurs. In addition, the team has to manage all issues regarding information security defined by Dialogue's Information Security Policy.
  - Data Analytics – Responsible for collecting, analyzing, reporting, and interpreting data stemming from the operations of all Dialogue functions. The team is also responsible for providing data-based business insights to help define business strategy, evolve Dialogue products and services, and optimize Dialogue's operational activities.
  - Product Support – Responsible for Dialogue's Support Services, helping all Clients in need of assistance with any Dialogue usage, and implementation, upgrades and various "how to" questions. Responsible for technical support for all Dialogue users across all Dialogue products.

- Operations
  - Medical Operations – Responsible for provision of the safe and effective telemedicine service to Dialogue Members (patients); for developing medical processes and care pathways optimized for telemedicine and for maintaining compliance with all applicable medical regulations. Medical Operations is also responsible for operating physical clinics as part of Dialogue's accounts that require this service. As mentioned at the beginning of Section 3, controls specific to the operation of physical clinics are not included in the scope of this report.
  - Strategy – Responsible for vision and objective setting, allocation of corporate resources, portfolio management and prioritization. The strategy team identifies new service opportunities and client and

member requirements by developing and validating service models, testing new service models and launching pilot projects. The team supports evaluation of international market opportunities, building business cases, supporting, and monitoring expansion, and evaluating expansion needs in the markets where Dialogue is active or planning to expand.
  - Compliance - Monitors clinical regulations in the geographies where dialogue operates or is planning to expand and ensures Dialogue policies and practices are in compliance with relevant regulations and standards.
  - Public Policy & Communications – Responsible for publishing company press releases, press & media kits, and ensuring efficient relationships with applicable government bodies. Monitors provincial and federal regulations in the markets where Dialogue is active that could impact Dialogue's operations.
  - Talent & Culture (referred to as "HR" in this document) – Responsible for defining Dialogue's people strategy, and for sourcing, recruiting, onboarding, hiring, and retaining employees, as well as providing a safe and energizing work environment for all Dialogue employees.
  - General Admin – Responsible for administrative support to the SEMT.

- Product
  - Product Management – Responsible for identifying business requirements, prototyping, interpreting, and communicating the results of prototype testing, developing detailed product specifications, and developing and maintaining the product road map in accordance with business objectives.
  - Product Design – Responsible for identifying quantitative and qualitative user profiles (i.e., "personas"); creating effective user experience; testing and evolving designs with representative users; and supporting Software Engineering by defining and designing specifications alongside them.

- Commercial
  - Direct Sales – Responsible for identifying and calling on prospects with the objective of getting them on board as Clients, and for growing our pipeline and maintaining good relationships with current and new Clients.
  - Account Executives and Enterprise Account Executives – Account Executives are responsible for selling into the small and medium size businesses (250 Lives to 2000 Lives) and the Enterprise Account Executives are responsible for sales to the large enterprise clients. Objective is to drive a growing and sustainable pipeline and convert this business into net new and add on business. The team is responsible for maintaining good relationships with such new Clients and ensuring Client's retention and account expansion.
  - Partnership & Business Development – Responsible for identifying, setting up and developing partnership relationships. The team is also responsible for building partnership strategies to support Dialogue's business objectives, managing partner channels, and equipping partners with necessary resources to grow sales and ensure Partner and Client satisfaction.
  - Marketing – Responsible for the brand development, marketing strategy and execution of such strategy supporting Dialogue's activities and the promotion of its products and services.
  - Customer Success – Responsible for the overall Dialogue relationship with its Direct Clients and Members. This includes participating with initial contact, managing Dialogue's onboarding process, reporting, Clients and Members training, continuous education, engagement, managing Clients and Member satisfaction, and renewals etc.
  - Commercial Operations – Management of commercial projects to ensure efficiencies and streamlined processes to drive effective engagement in Sales, Customer Success, Marketing, Commercial Operation, Revenue Operations, and Partnerships. This includes RFP management, training, project management and growth initiatives such as clients' insights and exception trackers.
  - Revenue Operations - Responsible for unifying and optimizing the end-to-end processes across marketing, sales, partnerships, and customer success to drive growth and maximize revenue. This includes CRM management, enabling data driven decision making, automating processes, sales enablement, and managing the overall GTM tech stack.

Commitment to competence

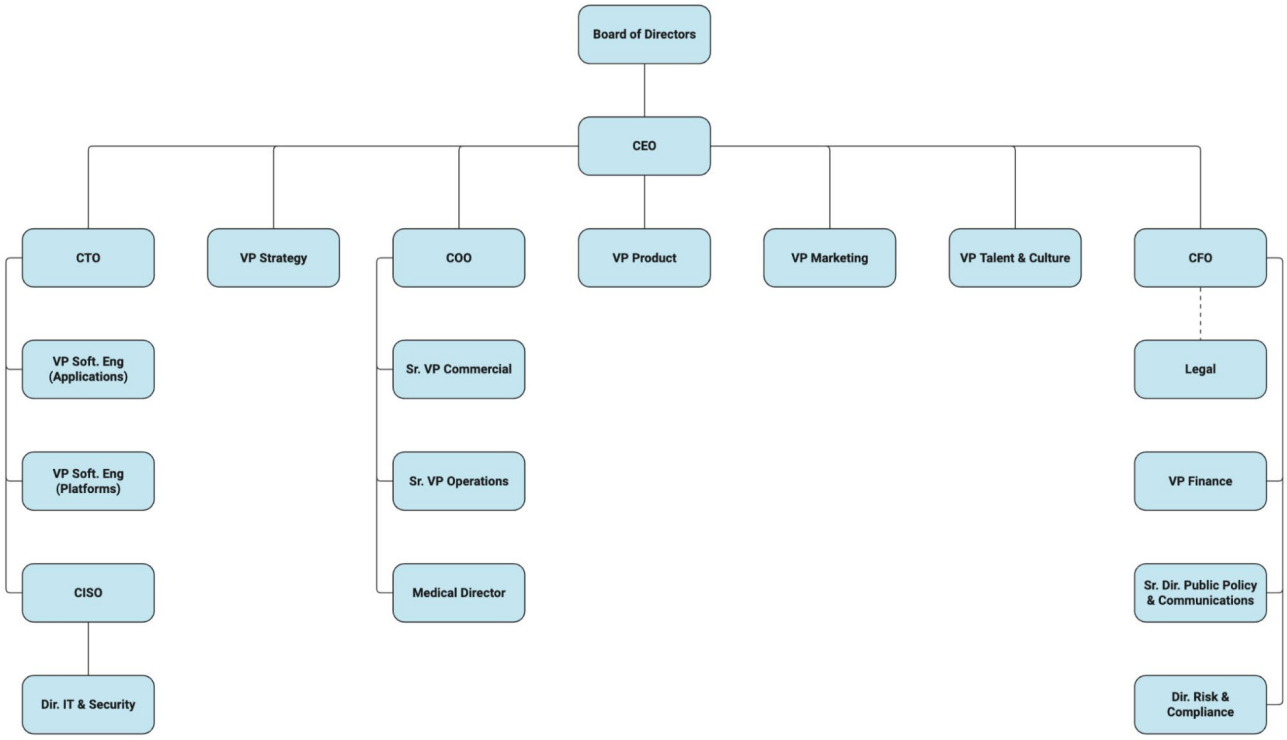
Dialogue has formal job descriptions that define the roles and responsibilities, experience, knowledge, and background required to perform each job and related tasks in a professional and competent fashion. Through a formal process, Dialogue determines the knowledge and skills needed to perform a particular job's duties and responsibilities and hires for that skillset and job requirements.

Examples of specific activities that Dialogue has implemented in this area are described below:

- A hiring procedure that is designed to check that the candidate has the required skills and competencies.
- Monitoring of employees' performance on a periodic basis through formal assessment, sets of objectives and KPIs, to determine that performance meets or exceeds Dialogue's standards.
- A professional development framework deployed across each function, and an employee training program.

3.3.1.3 Accountability

Dialogue has defined lines of Management authority, which are outlined in the following organizational chart. (A complete organizational chart is kept up to date in the HR Management tool and is available to all employees.)



On an as needed basis, the SEMT reports any issues with the potential to impact specific functions of the organization to the Board. Management maintains an open-door policy to encourage personnel to bring forth questions or concerns.

Dialogue has established T&C Policies to guide its employees with the handling of a vast array of situations and issues. As part of the onboarding process, new employees receive the T&C Policies as well as the Information Security Policy, Code of Conduct and Whistleblower Policy. Additionally, employees are required to sign a labour agreement, which includes standard employment terms including requirements to conform to Dialogue's standards.

Employees receive annual performance evaluations. Each employee is evaluated based on performance objectives and KPI criteria, in addition to behaviors and adherence to company values, and Management provides each employee with feedback. Salary increases and incentives are determined on the basis of the annual performance evaluation.

Direct managers conduct regular one-on-one meetings with employees to review ongoing progress toward objectives and display of behaviors and provide feedback and solicit suggestions about improving business processes.

3.3.1.4 Vendors and business partners

To manage risks associated with vendors and business partners' who are involved in the provisioning of virtual health care services or have access to Dialogue's systems, Dialogue obtains signed contracts or agreements which include a confidentiality clause (C.9.2.1).

3.3.1.5 Information Security Policy

An Information Security policy is in place and is made available to all employees and contractors. The policy includes a description of the roles and responsibilities assigned to individuals within the organization regarding security (including access control, incident handling and change requests). The Information Security policy and related procedures are reviewed annually. Changes are approved by the EMT (C.2.2.1).

Dialogue's security-related policies, standards and requirements communicated to employees further encompass the following topics:

- Intellectual property
- Confidentiality, data protection and privacy
- Tools usage
- Business practices

3.3.2 Risk Assessment

Dialogue has several processes for identifying and managing risks associated with its key services and has a formal management process that includes risk identification, assessment, and mitigation. Risk and fraud assessments are documented, updated quarterly by the SEMT, and includes risk and fraud identification, assessment, and mitigation plans (C.3.1.2). This process is a critical component of Dialogue's internal controls system. The purpose of Dialogue's risk assessment process is to identify, assess and manage risks that affect Dialogue's ability to achieve its objectives.

Dialogue has considered risks that could affect the organization's ability to operate and provide reliable services to its Clients and Members (including operational, reputational and fraud). In managing risks, Management uses a standard risk assessment matrix to evaluate and provide guidance to determine its mitigation strategy. Risks associated with tickets, whether they have been raised by customers or internally, are assigned a priority rating using a formal risk assessment formula (C.2.1.3):

Risk Matrix	Impact		
Likelihood	Low	Medium	High
High	Medium	High	High
Medium	Low	Medium	High
Low	Low	Low	Medium

Risk mitigation strategies are established via a risk assessment process that involves the SEMT, EMT as well as employees, to identify risks that could affect Dialogue's ability to operate, meet its objectives and/or meet its obligations. Risk assessment efforts include analysis of risk, probability of occurrence, impacts and associated mitigation plans.

Dialogue has put in place an Incident Management Process to manage, respond to, mitigate, and suppress potential incidents in a timely manner (same day resolution or mitigation for Priority 0, 2 days for Priority 1 and 10 days for Priority 2 incidents) (C.7.2.1).

An Incident Response Plan is documented, updated, and approved by management annually (C.7.4.1).

Dialogue strives to identify and prevent risks at an early stage through its policy, analysis, and procedure adherence in addition to mitigating relevant risks as discovered either through team structure, meetings, or notifications. Dialogue maintains security policies and communicates them to staff to ensure that individuals utilizing Dialogue resources understand their responsibility in reducing the risk of compromise and exercise appropriate security measures to protect systems and data.

As part of assessing security risks, Dialogue:

- Identifies threat actors.
- Establishes classification of assets which is included in its Information Security Policy; and
- Uses CVEs (Common Vulnerabilities and Exposures) and risk evaluation as a formal prioritization of software weaknesses applied to third party dependencies included in Dialogue's systems.

Dialogue's Business Continuity and Disaster Recovery Plan is documented and tested annually using a variety of industry standard techniques. (C.9.1.2).

Dialogue also subscribes to cyber and error and omission insurance policies to offset the financial impact in the event of a breach (C.9.1.1).

3.3.3 Control Activities

3.3.3.1 Organizational Controls

People who make up part of the Dialogue team are the most critical element of the company. This section describes the controls related to aspects of human resources management. In this section, the terms "employee" also refers to care professionals and contractors.

- Human resources (Talent & Culture) policies and practices

Dialogue's HR policies and processes are designed to (1) identify and hire competent personnel; (2) provide employees with the training and information they need to perform their jobs; (3) evaluate the performance of employees to verify their ability to perform job assignments; and (4) through performance evaluation, identify opportunities for growth and job performance improvement.

- Hiring procedures

Formal job descriptions are developed and maintained for each position. Job descriptions are reviewed as part of the annual performance evaluation as the job evaluation framework defines the expectation of each level (C.1.3.3). Dialogue uses documented hiring practices to ensure that new employees are qualified for their job responsibilities (C.1.4.2). The hiring process requires prospective candidates to be interviewed by personnel with whom the candidate will work and by members of the EMT.

Hiring policies and procedures include confirmation of prior work experience and criminal background checks prior to hiring.

- Recruitment

Dialogue applies the WHO methodology for hiring. The process starts with the hiring manager creating a scorecard for the position. The scorecard defines the role, its mission, accountability, responsibilities, objectives, KPIs, qualifications, experience and behaviours of the person who would occupy the position. The scorecard is approved

by the hiring manager and the EMT. The hiring manager works closely with the HR department throughout the recruitment process. The job description is drafted and reviewed. Most job descriptions are posted across several channels, and some of the job descriptions are filled with available candidates.

The HR team uses an application tracking system ("ATS"), to track job postings, applications and the entire recruitment process up to the offer acceptance stage.

The next phase of recruitment is sourcing candidates. A variety of sourcing channels are used to ensure the best candidate flow (e.g., LinkedIn, industry groups, universities, etc.). Internal referrals are encouraged with a recruitment bonus.

The first contact with the candidate is generally a presentation of Dialogue, its mission, core values and the position the company is seeking to fill. The next phase is the screening interview, generally performed by the recruiter, who uses a standard set of high-level questions to evaluate the candidate. After a successful screening call, technical interviews are scheduled with members/colleagues of the function. Depending on the nature of the role, this second call might contain a challenge to be completed by the potential candidate (for example, in Engineering or Sales). A Software Engineering candidate would meet with several engineers and cover topics such as secure coding, security standards for storage and networking, as well as best practices of software development. Following the technical interview is a practical "case study" or a "challenge" where the applicant must demonstrate their ability to perform the tasks related to their role to the highest standards. The challenges are adapted to each job position. The hiring manager is responsible for selecting the appropriate challenge. Use of the same challenge across several candidates is encouraged to allow Dialogue to make an objective assessment of each candidate. The case study/challenge is presented and discussed in person or virtually.

The next step is the "top grading" interview – a non-technical interview that focuses on the candidate's professional career, highlights, lowlights, learnings, values, and behaviours. C-suite are not typically present in top grading interviews unless hiring for a VP and above .

Pre-hiring verification procedures that include criminal background checks and work experience checks are performed prior to hiring (C.1.4.3).

The offer letter is drafted by HR (i.e., Head of Talent or delegate), reviewed by the hiring manager and at least one C-level executive and sent to the candidate. When the candidate accepts the offer, HR sends an employment contract for signing, via digital signature service HelloSign.

- Onboarding

Upon hire, employees (including care professionals and contractors) sign a formal non-disclosure/confidentiality agreement to protect proprietary information by prohibiting disclosure of proprietary or third-party confidential information, including Member information, to unauthorized parties (C.1.1.4).

Once the contract is signed, the onboarding process starts. The employee information is collected and recorded into the HR management system, tracking time off, benefits, etc.

Employee, care professional and contractor user IDs are created only after being approved by management or human resources (C.6.2.1).

Team communications mainly take place in Slack, a collaboration hub, so employees are placed in the right Slack channels as part of onboarding. Employees also join Notion, an internal cloud-based documentation and collaboration system (i.e., knowledge base).

There is a bi-weekly HR onboarding session for all new hires that is hosted by the Talent & Culture Coordinator. Part of this presentation is an overview of the core values, HR tools and general employee benefits.

Employees also get onboarding presentations by the leads of various functions (product, data, tech, medical) – attendance is role-specific.

Upon hire, employees (including care professionals and contractors) are shown where to find the security policy referred to in the HR Policies and are asked to acknowledge them in UKG.

Employees receive information on Dialogue's shared information repository. This information includes an overview of Dialogue's HR policies and procedures — these policies and procedures being also accessible by employees at all times — the offer letter or employment contract, relevant compensation information, the HR Policies, and the Information Security Policy.

Dialogue has also established an onboarding procedure including on-the-job employee training for critical functions. Programs include position-specific training and orientation on the basics of the functional teams' operations and activities. Employees are also encouraged to actively participate in available self-training, webinars, etc. to maintain their knowledge and develop an awareness of technology developments (specifically for Software Engineering and others when needed), trends and issues facing Dialogue.

The onboarding process continues according to an individual's onboarding plan. The plan stems from a common onboarding checklist and is adapted to the role and specific needs of each individual.

- Continuous training

Employees are required to maintain a high degree of competence surrounding data security and privacy. A security awareness training program is in place. Dialogue uses an online learning management system ("LMS") that allows management to track the progress of each employee and enables the company to run the training on an annual schedule.

Each function has a specific training program. The medical team has an extensive training program that covers medical, privacy and technology processes.

The company encourages employees to leverage the continuous training program that is in place. Work-related training is funded by the company to cover 100% of the costs (dependent on budget per team). More specifically, a defined budget is made available for the Software Engineering team for training needs related to evolving requirements (C.1.4.4). After the training, employees are encouraged to present and share their knowledge with the rest of the team.

- Security awareness

Dialogue conducts regular security training programs for all employees and contractors in the areas of system security, safety, and privacy. Each employee and contractor of Dialogue is made aware of the security implications that revolve around their functions and actions. This process begins with providing individuals with the understanding and knowledge needed to help secure Dialogue's system and its Clients and Members and their data within established policies. Security awareness programs include the message that individuals can have a significant impact on the overall security of an organization. Dialogue's employees and contractors are required to complete security awareness training on an annual basis, a record of security awareness training attendance is maintained and follow-up with the individuals is made in case of nonattendance (C.1.4.5).

- Employee Performance Monitoring and Development

Twice per year, employees are required to undergo a formal performance evaluation. Results of the evaluations are submitted in the HR management platform (C.1.4.6). During the mid-year review process, employees write their self-assessment and managers write their employee's performance review, including a description of how the employee's performance compares to the responsibilities outlined in their job description and goals assigned to them, areas for improvement, and an evaluation against the organization's values. During the year-end process,

this is completed as well in addition to employees receiving an aggregate 360 feedback from their peers and direct subordinates (if applicable) and managers providing an overall 4-point scale rating of performance. The formal assessment of employees via the rating scale is then calibrated in various sessions across the organization including all managers from the organization to ensure fairness. Results are communicated to the SEMT.

Dialogue has implemented a structured performance appraisal process. The SEMT establishes performance measures that are aligned with objectives and are reviewed at least annually (C.1.5.2). Managers are asked to discuss performance expectations and goals with each employee, reporting to them at least annually. These objectives and development goals are documented in a formal annual assessment sheet. Incentives are related to the performance measures and corrective or disciplinary actions are taken if performance is below expected performance standards.

- Offboarding Procedure

Managers, in coordination and collaboration with Human Resources, the Legal team, IT and the EMT, are responsible for managing voluntary and non-voluntary terminations. Managers and the assigned Human Resources stakeholder communicate with the employee to identify the employee's final day of employment and to inform the employee of his or her rights and responsibilities. The employee (including care professionals and contractors) is asked to return any of Dialogue's assets in his or her possession, including, if any, computers, accessories, office keys, etc.

Non-voluntary off boarding (termination) takes place in cases where an employee fails to successfully complete a Performance Improvement Plan, when appropriate.

The decision to terminate is discussed between the appropriate manager, the head of HR, the Legal team, and the C level executives. When the decision is made, a termination letter is drafted.

The manager, a member of the HR team and the employee meet, and the letter is delivered to the employee. During or immediately after the meeting, an off-boarding procedure is executed:

- The head of HR or a delegate collects the keys and any access cards; and
- The CTO or a delegate disables all access to applications and accounts.

In the case of a voluntary termination of the employment contract, the off-boarding checklist is performed at the mutually agreed date. Contractors must give at least 10 days' notice. When appropriate, a member of the HR team performs an exit interview.

In accordance with the off-boarding procedure, employee, care professional and contractor user IDs are removed according to the date of termination and physical assets including, if any, computers, accessories, and office keys, are returned (C.6.2.5).

3.3.3.2 Information security controls

- Applications

Dialogue's services are presented to the Clients and Users and supported via several applications.

Member App (iOS, Android, Web) is designed to provide Members access to the service. It includes messaging and video capabilities.

Care Platform (Web, Mac OS, and Windows) is designed to be used by care professionals who provide medical services to the Members. It includes messaging, video capabilities, Member record management and clinic management capabilities.

Presto (a.k.a. HR Administrator Console) (Web) is designed to enable Dialogue's Clients to manage the service within their organizations. It includes the ability to manage the list of their Users who have access to the service. Dialogue creates the organization accounts and Presto Administrators (HR administrators at the Clients, when requested) are assigned by Dialogue's Presto Super Administrator (C.6.2.2). Upon request from an authorized Client representative, Member accounts are created by Dialogue's Presto Super Administrator (C.6.2.3). Upon request from the Client, Member accounts are deactivated by Dialogue's Presto Super administrator in a timely manner (C.6.2.4). Upon contract termination, or within 7 days, all Presto Administrators are deactivated (C.6.2.7).

- Services

For the design, development, deployment, and support of the applications used for its services, Dialogue applies the Twelve-Factor App methodology. This methodology, which is widely used for building software-as-a-service (SaaS) applications, comprise the following 12 principles:

I.	Codebase	One codebase per deployed service tracked in revision control: many deployments
II.	Dependencies	Explicitly declare and isolate dependencies.
III.	Config	Store configuration in the environment
IV.	Backing services	Treat backing services as attached resources.
V.	Build, release, run	Strictly separate build and run stages
VI.	Process	Execute the app as one or more stateless processes.
VII.	Port binding	Expose services via port binding
VIII.	Concurrency	Scale out via the process model.
IX.	Disposability	Maximize robustness with fast start-up and graceful shutdown.
X.	Dev/Prod parity	Keep development, staging and production as similar as possible
XI.	Logs	Treat logs at event streams
XII.	Admin Processes	Run admin/management tasks as one-off processes.

Dialogue uses a micro-services architecture. In addition to the key services listed above, there are several microservices designed to enable a narrow functionality and control access to a narrower data set, in addition to increased agility in the development, maintenance, deployment and isolation of system components. An up-to-date high-level architecture of Dialogue's system components is maintained, accounting for additions and removals and is posted on Dialogue's intranet and is available to its internal users (C.3.4.1).

For example, one such microservice is the geolocation service. This service tracks the location of the Member in order to ensure that Dialogue treats residents of each province with resources who have the corresponding license to be able to do so, when applicable (and also to prevent providing regulated healthcare services to people who are outside of a specific region). This microservice has access to the geolocation of the Member at the time of the consultation but does not have access to the rest of the Member's records.

- Infrastructure

Dialogue uses cloud provider Amazon AWS data centers that are physically located in Canada. Several AWS services such as EKS, EC2, Relational Database Service, Route53, Cloud Watch, Key Management Service, DynamoDB, Lambda, Guard Duty, Security Hub, SNS, SQS, Pinpoint, SES, Backup and Kinesis are used in Dialogue's system.

The identity provider of the platform is Okta CIC (Formerly Auth0). Okta CIC is responsible for secure storage of users' password hashes, as well as authentication and authorization services. It is also responsible for multi factor authentication for member access.

The identity provider of Dialogue employees is Okta. Okta is responsible for secure storage of employee credentials and is responsible for managing access to various systems including access to Care Platform and Presto. Okta has SSO SAML integration capability with various tools used at Dialogue including Okta CIC, Google Workspace, NetSuite, Ironclad and GitHub, etc. All users are provisioned/deprovisioned in Okta via automated

import of employees and contractors list from UltiPro. All communication between Okta and the Dialogue is protected by TLS 1.2 supporting Perfect Forward Secrecy (PFS).

The firewall provider is Cloudflare. 100% of dialogue services are protected by Cloudflare firewall and network traffic flowing into AWS is enforced through Cloudflare. Cloudflare ensures the traffic is secured with TLS v1.2 minimally or v1.3 when the client browser supports it.

Two kinds of databases are used: relational databases (PostgreSQL) are used for Member information, billing and messaging and NoSQL databases (DynamoDB) are used for microservice-specific data. All databases have backups in place, managed by AWS Backup. Failover configuration is also in place. Files are stored in Amazon S3. All the data is encrypted in transit and at rest.

- Development and deployment

Production and test environments are monitored, and logs from both environments are aggregated, indexed, and made available via a flexible search and filtering tool (Datadog). The alerts generated by both environments are communicated via real-time notifications and messaging system (Slack) and on-call scheduling system (PagerDuty). The health of the overall system is visualized via a set of dashboards (Datadog).

A unique build number is created, and every modification to the code is tracked in GitHub with a unique version which is attributed to the person who made the change.

For mobile app updates, an Over the Air ("OTA") update mechanism is used to allow fast deployment of the updates, without having to wait for app store approval cycles for most of the updates of the applications. This method of deployment of mobile apps allows instant application updates without having to require Users to manually keep their mobile apps up to date. Many changes to Dialogue's mobile apps are done via the OTA update method, while some updates that use the new features of mobile operating systems (iOS or Android) are deployed through the app stores.

- Authentication and Authorization

Each access to a Dialogue service or microservice is authenticated.

For Members, the authentication requires the creation of Member identities. Each Member receives their unique identity during online sign-up. Upon Member sign-up, the account is activated if the Member is on the eligibility list (C.6.2.5). Systems are configured to authenticate internal and external Users with a unique user account and to enforce user account and password requirements (C.6.1.2). Internal and external users must meet password complexity and entropy standards (C.6.1.3). Okta CIC (Formerly Auth0) is the identity provider for Member identities.

All physicians must also be authenticated in order to access Dialogue's applications. Physician identities are provided and managed by Okta that powers Dialogue employees' identity. Okta automatically associates roles of Dialogue employees in Okta CIC (Formerly Auth0). The roles of those identities are managed with Okta CIC (Formerly Auth0).

Access rights are assigned to security roles based on the requirements for the job function. User IDs are assigned security roles based on the individual's job responsibilities (C.6.1.1).

Once the user is authenticated at login, Auth0 generates an authorization token that encodes the identity's role. Accesses are granted based on the role assigned to the user ID. There are several different users with different roles:

- Patient (Member)
- Physician (physician, care coordinator or nurse, Call Center agent, restricted-practitioner a.k.a contractors)

- Clinician (Medical Quality Assurance)
- Non-Medical Professionals (eap-practitioner)
- Administrator (Presto Administrator, HR Administrator, Clients Administrator)
- Read-only super administrator (Presto Administrator)
- External Partner Organization HR Administrator (Presto Administrator, HR Administrator)
- Super Administrator (Presto Super Administrator, Dialogue System administrator)

Administrative access privileges to infrastructure systems are restricted to authorized System Administrators. System Administrators have an account in which they can assume different roles to perform the necessary activity they have to.

Access to the production environment is restricted to authorized personnel and is only permitted through an encrypted connection (SSH) to the database private network managed and secured by a virtual private cloud (VPC) (C.6.1.4).

The assignment of a specific role to an identity is documented and approved by System Administrators. Two-factor authentication is supported by the identities provided by Okta. All Tech team members and care professionals use two-factor authentication which is enforced by the system (C.6.1.8).

For employees and contractors, operating systems are configured to accept updates automatically (C.6.7.1).

For our servers, the secure disposal of informational physical assets is under the responsibility of AWS. Dialogue employees' laptops are encrypted to ensure the protection and confidentiality of all information stored on local disks (C.6.5.1).

At least annually, user access rights reviews are performed on employees, care professionals and contractors, including system administrators, and corrections are applied when necessary (C.6.2.8).

3.3.3.3 Change management controls

- Design and planning

All major changes to the product or a service go through several review phases. A monthly road map review with all of the EMT members validates that planned changes are aligned with the business strategy. The road map is then communicated to the SEMT and is kept up to date. Additionally, we hold weekly Solution Design review meetings where product designers and Product Managers present the evolution of specific feature designs and proposed changes and solicit feedback from interested stakeholders, especially leadership across Tech, Product, Ops, and the CEO.

An independent technical review led by developers in Software Engineering focuses on the architecture and the implementation details including a risk assessment of the proposed changes (including architectural, security and data risk). Approval via a pull request process is required prior to release of changes to production (C.8.1.2). The technical designs and test plans are documented in documentation repositories (Notion, GitHub) accessible to all engineers. The ability to push changes to the production environment is restricted to Software Engineering personnel only via a GitHub pull request and can never be pushed directly to the main code branch without bypassing the process. (C.8.1.3).

Dialogue's development process follows the Scrum methodology. A sprint planning meeting held every two weeks is used to detail the exact implementation plan. A sprint plan includes features and defects the team is planning to resolve. All work done by the team is defined via a detailed work item (GitHub issues). The progress is tracked and monitored with a project management tool (JIRA) that integrates with GitHub. JIRA visually shows the progression of the work through stages.

- Software development

The source code is controlled by GitHub. Dialogue's source code is stored in several code repositories. Each repository includes the code that logically belongs together, e.g., implements a particular service. Dialogue employees and contractors that need access to the source code are placed into appropriate GitHub "teams". Each team has access to a specified set of code repositories. The access level (Read, Write) is assigned to the GitHub team and the admin access level is assigned to a subset of key employees which are maintaining and operating the system e.g., DevOps team.

All code development takes place in separate branches. Once the code is complete, it is committed into the branch. CircleCI automatically performs the following sequence of automated continuous integration testing prior to deployment to the production environment, as applicable (C.8.1.4). The steps below happen within CircleCI:

1. The code is analyzed via various static code and security code analysis tools to help prevent common security vulnerabilities and ensure adherence to code standards.
2. A build is produced by CircleCI.
3. A set of automated tests (unit, integration, system or end-to-end) is run on the code and CodeCov is used to calculate the percentage of code covered by automated testing.

In order to contribute to the code update to the system, a developer needs to submit the code for a peer review via a pull request. A pull request can only be integrated into the main code branch if the build and the test sequences pass.

A pull request is reviewed by one or more engineers, who are selected by the original author of the change on the basis of their expertise with the system being changed. Code review comments are integrated, and the pull request is updated. Once the pull request is accepted, it can be integrated into the main code branch. This act triggers another sequence of build, test, and deployment to the production environment. The entire process is automated and does not require manual intervention.

Quality Assurance performs comprehensive functional and regression tests. In cases where no defects are found and the implementation matches the requirements, the change is promoted by software developers from staging to a main branch, and the automated sequence of build, test, and deployment to production is repeated.

The system maintains full traceability of changes. Each build carries a unique version. Each version is mapped to the commit. Each commit identifies the exact changes that were made to the code.

Rollback procedures are established for application and configuration changes. The Software Engineering team monitors the deployment post-deployment for any impairment or degradation of production. The monitoring system will alert the team owning the system being deployed for any error that will impact the service operation of the Dialogue platform.

- Staged Deployment

Back-end systems are tested in isolation before being deployed on a test environment. The test environment is a replica of the production environment. It has all the capabilities of the production system. Test environments are logically separated from production environments (C.8.1.1).

Care Platform

Once the Care Platform testing is completed in the test environment, the application is deployed to a beta "channel" within the production environment. This release allows the care professional team to test the product in the context of the production environment. This is done by a limited set of practitioners. In the event of any issues, the care professional team can switch back to the stable version. This approach allows Dialogue to test the product prior to release without having access to the production environment (developers do not have access to production).

When the beta testing is successful, the product is promoted to production.

Admin Portal (Presto)
Once the HR Admin testing is completed in the test environment, the application is deployed to a staging environment where it can be used by internal users such as the Customer Success team. Once the test phase is completed, the application is deployed to production.

Member App
Mobile apps are configured to work within the test environment and are installed on mobile devices for testing. When the test is successful, the new build is produced automatically with the configuration pointing to the production environment. This build is submitted to the app stores for review if it cannot be updated via OTA.

- Release Announcements

The internal communication of releases is performed via an all-hands meeting, road map updates and release notes sent to the users of affected systems. External Users are informed of new releases and customer impacting changes as well as corrective measures, when necessary, via Dialogue's public website (C.2.3.1).

- Support

Support is provided for three sets of users:

- Care professionals (physicians, care coordinators, nurses, heap practitioners)
- Members
- Clients, HR Administrators.

The care professional support is initiated via an instant message on a dedicated Slack channel (#support). Whenever the issue is clarified, it is recorded by a tech support specialist in JIRA, a ticketing system.

When the Member or a Client's HR Administrator experiences an issue, they can reach out for support over email.

Software defects created in JIRA are prioritized via a formal methodology that defines an issue's priority based on the scale measuring severity and the impact of the issue. The performance of the tech support function is monitored via reports. High severity incidents are analyzed in post-mortem reviews (C.7.2.2).

3.3.4 Information and Communication

3.3.4.1 Relevant information and communication

Dialogue has implemented an internal knowledge base to disseminate information to employees ("Notion"). The information includes responses to clients and member inquiries, "how-to" and training, applicable dialogue.

Policies and processes – including security policies and processes. Individual functions are charged with maintaining their relevant information in the knowledge base. The information is generally published to the knowledge base for company-wide access.

Restrictive access controls are also applied if the material being published is not intended for general viewing.

Dialogue has also implemented various methods of communication to help ensure that employees understand their individual roles and responsibilities, and that significant events are communicated. Those methods include the following: new hire onboarding, training, policy and process updates, biweekly meetings summarizing events and changes, 1:1 meeting, team meetings, use of email and slack (encrypted messaging app) to communicate time-sensitive information, and the documentation and storage of historical and reference data and documentation in internal repositories for business and support activities. Significant changes such as changes in senior

management, VP or C-level roles and responsibilities are communicated internally and externally following communication methods stated above (C.2.2.2).

An anonymous communication (whistleblower) policy is in place to allow employees to identify and report on concerns and other complaints related to various topics of interest, including satisfaction, ethics, and social responsibility, through a dedicated tool. Automatic reminders are sent to all employees on a bimonthly basis (C.1.1.5).

Security is reinforced by training and through awareness programs. In addition, communication is encouraged at all levels to promote a security first mindset that contributes to the operating efficiency of dialogue. The information security policy prohibits the transmission of sensitive information over the internet or other public communication paths (e.g., email) unless it is encrypted (C.6.1.5). Communications use secure transports such as SSL and HTTPS (C.6.1.7).

Clients' responsibilities, which include reporting operational failures, incidents, problems, concerns and complaints, and the process of doing so, are described in Dialogue's public website (C.2.3.4).

Dialogue security commitments are also communicated to our clients via the master service agreements. In addition, a summary of these commitments is available on Dialogue's public website (C.2.3.2). Documentation of system operations is available to Dialogue Members and Clients on Dialogue's public website (C.2.3.3).

3.3.5 Monitoring

- Monitoring activities

Ongoing monitoring procedures are built into the normal recurring activities of dialogue and include regular management and supervisory activities.

The compliance team reviews control activities annually. Senior management is deeply involved in the day-to-day operations of the organization. Senior management and managers are regularly in touch with personnel, whether on an ad hoc basis or through recurring teams and one-on-one meetings and may question the accuracy of information that differs significantly from their knowledge of operations.

  - Dialogue has established a risk assessment process and an Incident Management Process in order to manage certain risks and threats.
  - Dialogue further monitors regulatory changes in an ever-more complex and rapidly changing legal environment, to ensure operational processes adapt as needed in order to be legally compliant.
  - The Privacy Officer and Privacy Council, General Counsel and Compliance Manager are responsible for ensuring that dialogue complies with applicable laws, regulations, and standards (C.3.1.3).
  - Dialogue uses dedicated systems to track user and client's requests and incidents (Jira), errors and alerts (Datadog, Slack), which are tracked until completion. Management performs regular reviews of tasks assigned to their staff. Tasks that are not completed in a timely manner are escalated and resolved.
  - Dialogue also undergoes periodic external scans and assessments to evaluate systems security, and, in some cases, receives recommendations for improvement.
  - Dialogue engages third-party security specialists to conduct internal and external vulnerability assessments at least annually. Findings are assessed, communicated, and acted upon as needed (C.3.2.2).
  - Identified internal control deficiencies are monitored and followed up until resolution by the compliance manager (C.4.2.1).

- Security Incident and Event Management (SIEM)

Another component of Dialogue's monitoring activities is the SIEM. Typically, a SIEM system centralizes the storage and interpretation of logs and allows near real-time analysis, which enables security personnel to take defensive actions more quickly. A SIEM system collects data into a central repository for trend analysis and provides

automated reporting for compliance and centralized reporting. By bringing these two functions together, SIEM systems provide quicker identification, analysis, and recovery of security events.

The SIEM system deployed by Dialogue is Datadog, a software-as-a-service (SaaS) monitoring solution that centralizes threat detection, incident response and compliance management for Amazon's AWS.

Datadog integrates with AWS cloud services; SIEM sensors are deployed on Dialogue services and capture all logs and sensitive information. That data is then moved to the SIEM third party cloud services to be analyzed and correlated. Finally, automatic alerts are configured through the SIEM monitoring console (Web) and communicated to Dialogues people in charge of information security.

Monitoring software is used to identify and evaluate ongoing system performance, security threats, changing resource utilization needs and unusual system activity. This software sends a message automatically to the operations center (C.2.1.1).

- Evaluating and communicating problems and complaints

Client/member requests and complaints are tracked in JIRA and reviewed for resolution in compliance with service level agreements with clients, and for consideration on how to improve Dialogue's systems.

3.4. Complementary User Entity Controls

Management has determined that certain applicable trust services criteria can be met only if complementary user entity controls ("CUEC") are suitably designed and operating effectively, at the clients. Therefore, each user entity's internal control must be evaluated in conjunction with Dialogue's controls, considering the related complementary user entity controls identified in the table below, where applicable.

For user entities to rely on the controls reported herein, each user entity must evaluate its own internal control to determine if the identified complementary user entity controls have been implemented and are operating effectively.

User Entity Control	Associated Criteria
Providing Dialogue with, and keeping up to date, a list of the individuals (Client HR Administrators) having authority to act on its behalf and updating Dialogue's system promptly of any departure of employees on that list.	CC6.2, CC6.3
Ensuring that creation, modification, and removal of Dialogue Member accounts are authorized and performed in a timely manner.	CC6.2, CC6.3
Restricting access to services provided by Dialogue to authorized client personnel.	CC6.2, CC6.3
Ensuring that user access credentials remain confidential.	CC6.2, CC6.3
Reporting to Dialogue in a timely manner any known or suspected incidents or problems with systems operation.	CC6.8, CC7.2, CC7.4

3.5. Subservice Organization Monitoring and Complementary Subservice Organization Controls (CSOCs)

To deliver services to Dialogues Clients, the following subservience organizations are used:

AWS

AWS is the main cloud provider where dialogue hosts most of the components that power its platform and data. Dialogue uses AWS ca-central-1 region to ensure that Canadian member personal health information and personal identification information data stay in Canadian data centers.

Okta C.I.C. (Formerly Auth0):
Okta C.I.C. provides customer identity management, authentication and authorization services used by all our members to access the Dialogue app and by all our practitioners to connect to the Care-Platform to serve members.

Circle Internet Services Inc. (CircleCI):
CircleCI is a continuous integration and continuous delivery platform that is used to build, test, validate and deploy any software changes to production environments.

Kandji:
Kandji is the mobile device management tool used to manage Apple end users compute devices owned by Dialogue, their operating systems, and their security features.

Cloudflare:
Cloudflare is a global cloud platform designed to make everything you connect to the Internet secure, private, fast, and reliable. Cloudflare offers, among other services, a content delivery network, domain name server, firewall and zero trust tunneling system which Dialogue uses.

GitHub:
GitHub is a source code management system and is used by Dialogue to host all proprietary software source code and configuration required to build its platform. Dialogue uses the cloud-hosted GitHub enterprise version.

Datadog
Data dog provides monitoring, alerting, error tracking and performance as a service platform based on a public cloud.

Input Health:
Input Health provides the software used for Electronic Medical Records interface and management.

Google Workspace:
Google provides email services, cloud storage, virtual meeting rooms, and various cloud computing, productivity, and collaboration tools.

Okta:
Okta provides identity account management, authentication, and authorization services.

UKG – Ultipro:
Ultimate Kronos Group (UKG) - Ultipro provides a Human Resources Information Management (HRIS) system.

SentinelOne:
SentinelOne provides data security protection and monitoring service.

Sentry:
Sentry provides frontend application logs monitoring and error tracking system.

In the design of its internal control, Management has determined that specific criteria can be achieved only if the subservience organizations implement complementary controls. Each user entity's internal controls must be evaluated in conjunction with Dialogue's controls, and the related tests and results described in this report, considering the related complementary subservice organizations controls ("CSOC") expected to be implemented at the subservice organization as described below:

Subservice Organization controls	Associated Criteria
Logical access controls are implemented to protect relevant software and infrastructure.	CC6.1

Subservice Organization controls	Associated Criteria
User access is created only when authorized and removed when no longer required.	CC6.2, CC6.3
User access rights reviews are performed regularly.	CC6.2, CC6.3
Access granted is based on user responsibilities and monitored accordingly.	CC6.2, CC6.3
Physical access mechanisms are in place to prevent unauthorized access to information assets.	CC6.4
Disposed and unused media are securely destroyed or disposed of to prevent any recovery of sensitive information assets.	CC6.5
Network security mechanisms are in place to prevent outside threats.	CC6.6
Transmission of information assets are adequately protected against unauthorized use and disclosure.	CC6.7
Protection mechanisms against malicious software for software and infrastructure are in place.	CC6.8
Firewall and other external perimeter protection controls are in place and monitored.	CC7.1
Review of changes made to systems and infrastructures are performed to prevent the introduction of unauthorized changes.	CC7.1
Systems are monitored to ensure compliance with the subservice organization standards.	CC7.1
System performance and security monitoring is in place to detect anomalies.	CC7.2
Security incidents are assessed to determine necessary corrective actions.	CC7.3
Procedures are in place for the execution of a defined response and recovery plan in case of significant security incidents.	CC7.4, CC7.5
Systems and procedures are in place to ensure that regular backups are performed as per service agreement.	CC7.5
System changes are documented, tested, and approved before they are migrated into production.	CC8.1
Procedures are in place to manage business disruption risks.	CC9.1
Procedures are in place to identify and manage risks related to vendors and business partners.	CC9.2

Dialogue service providers (AWS, Auth0, CircleCI, CloudFlare, GitHub, Datadog, Input Health, Google, Okta, U.K.G. - Ultipro, SentinelOne and Sentry) produce Service Organization Controls (SOC) report making them reliable partners for Dialogue. Annually, management obtains, and reviews reports on controls provided by subservience organizations and evaluates the impact on Dialogue's internal controls (C.3.2.3).

3.6. Changes since the last report

There were no major changes that would affect the security of the technical or logical environment in the past year.

Dialogue was required to change the auditor responsible for conducting the SOC 2 type 2 audit following the acquisition by Sun Life, in order to comply with independence requirements.

Section 4 – Trust Services Category, Criteria, Related Controls, and Tests of Controls

Information Provided by the Service Auditor

Tests of Operating Effectiveness

This report on the description of dialogue systems, and on the suitability of the design and operating effectiveness of controls, when combined with an understanding of the controls at subservience organizations and user entities, is intended to provide reasonable assurance that Dialogue service commitments and system requirements were achieved based on the AICPA Trust Services Criteria relevant to security ("applicable trust services criteria") set forth in the TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria).

This section presents the following information provided by dialogue:

- The applicable trust services criteria.
- The controls established and specified by dialogue to achieve the applicable trust services criteria.

Also included in this section is the following information provided by us:

- A description of the tests performed by us to determine whether Dialogue controls were operating with sufficient effectiveness to achieve the applicable trust services criteria. We determined the nature, timing, and extent of the testing performed.
- The results of our tests of controls.

Our engagement was limited to the applicable trust services criteria and related controls specified by Dialogue Service Organization in Sections 3 and 4 of the report and did not extend to controls in effect at subservience organizations and user entities.

It is each user's responsibility to evaluate the information included in this report in relation to internal control in place at individual user entities to obtain an understanding and to assess control risk at the user entities. The controls at the subservience organizations, user entities and dialogue controls should be evaluated together. If effective subservience organization controls and user entity controls are not in place, dialogue controls may not compensate for such weaknesses.

Dialogue's internal control represents the collective effect of various factors in establishing or enhancing the effectiveness of the controls specified by Dialogue. In planning the nature, timing, and extent of our testing of the controls to achieve the applicable trust services criteria, we considered aspects of Dialogue's control environment, risk assessment process, monitoring activities, and information and communications.

The following table clarifies certain terms used in this section to describe the nature of the tests performed. In addition to the tests listed below, ascertained through multiple inquiries with management and the control owner that each control activity listed below operated as described throughout the period.

Test Description	Description of testing procedures performed
Inquiry	Inquiry of appropriate personnel and corroboration with management
Observation	Observation of the application, performance, or existence of control
Inspection	Inspection of documents and reports indicating performance of the control
Re-performance	Re-performed in the control

In addition, when using information produced (or provided) by the service organization, we evaluated whether the information was sufficiently reliable for our purposes by obtaining evidence about the accuracy and completeness of such information and evaluating whether the information was sufficiently precise and detailed for our purposes.

Tests of Operating Effectiveness

Our tests of controls were designed to cover a representative number of transactions throughout the period from April 1, 2023, to March 31, 2024. In determining the nature, timing, and extent of tests we considered, (a) the nature and frequency of the controls being tested, (b) the types of available evidential matter, (c) the nature of the control criteria to be achieved, (d) the assessed level of control risk, (e) the expected effectiveness of the test, and (f) the results of our tests of the control environment.

Testing the accuracy and completeness of information provided by dialogue is also a component of the testing procedures performed. Information we utilized as evidence may have included, but was not limited to:

- Standard “out of the box” reports as configured within the system.
- Parameter-driven reports generated by dialogue systems.
- Custom-developed reports that are not standard to the application such as scripts, report writers, and queries.
- Spreadsheets that include relevant information utilized for the performance or testing of control.
- Dialogue prepared analyses, schedules, or other evidence manually prepared and utilized by Dialogue.

While these procedures were not specifically called out in the test procedures listed in this section, they were completed as a component of our testing to support the evaluation of whether the information is sufficiently precise and detailed for purposes of fully testing the controls identified by dialogue.

Our tests of the controls were designed to cover a representative number of transactions throughout the period from April 1, 2023, to March 31, 2024. In determining the nature, timing, and extent of tests we considered, (a) the nature and frequency of the controls being tested, (b) the types of available evidential matter, (c) the nature of the control objectives to be achieved, (d) the assessed level of control risk, (e) the expected effectiveness of the test, and (f) the results of our tests of the control environment.

Our test of the operating effectiveness of controls included such tests as we considered necessary in the circumstances to evaluate whether the controls and the extent of compliance with them is sufficient to provide reasonable, but not absolute, assurance that the applicable trust services criteria were achieved during the period from April 1, 2023, to March 31, 2024.

In cases where the key controls were standardized, test samples were selected across locations and platforms. Testing samples were selected in accordance with accepted auditing standards.

Reporting on Results of Testing

The concept of materiality is not applied when reporting the results of tests of controls for which exceptions have been identified because we do not have the ability to determine whether an exception will be relevant to a particular user entity. Consequently, we report all exceptions.

In the description of our test results, if any exceptions were noted, a response from management may be included to provide additional information related to the exceptions. Unless otherwise indicated, we did not apply any audit procedures to the information provided in the management response.

Control testing matrix

Security Criteria and Control Activities

This section contains a description of the relevant criteria under the security (applicable trust services criteria) set forth in the AICPA, Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality and Privacy. It also contains a description of Dialogue's control activities designed and implemented to meet each criterion throughout the period April 1, 2023, to March 31, 2024. The controls to meet the applicable trust services criteria have been specified by and are the responsibility of dialogue.

SOC2 Criteria	SOC 2 Common Criteria Description	Control Number	Control description	Testing procedure	Criteria Conclusion
CC1.0 - Control Environment					
CC:1.1	COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.	C.1.1.1	Dialogue has documented the code of conduct and core values which are reviewed and updated by the SEMT as needed.	Inspected the HR portal to ascertain that Dialogue's core values had been communicated to all employees via the HR portal.	No exception
		C.1.1.2	The code of conduct and core values outline potential disciplinary sanctions, including termination of employment, for employee violation or misconduct.	Inspected the code of conduct and core values to ascertain that it outlines potential disciplinary sanctions, including termination of employment, for employee violation or misconduct.	No exception
		C.1.1.3	The SEMT monitors employees' compliance with Dialogue's core values and the HR Policies through the monitoring of Dialogue's Members, Clients, and employees' feedback.	Inspected the reports used by the SEMT to ascertain that they had monitored members, clients, and employees' feedback.	No exception
		C.1.1.4	Upon hire, Dialogue's employees (including care professionals and contractors) are required to acknowledge and sign confidentiality / nondisclosure agreement.	For a sample of new employees, care professionals and contractors, inspected evidence of the signed formal nondisclosure/confidentiality agreement to ascertain that it had been acknowledged.	No exception
		C.1.1.5	Management has established separate communication channels in support of the functioning of the internal control components, including anonymous third-party administered whistle-blower hotlines available to internal and external users. Automatic reminders are sent to all employees on a bimonthly basis.	Inspected anonymous communication (whistleblower) policy in place to ascertain that it directed employees to identify and report on concerns and other complaints related to various topics of interest, including satisfaction, ethics, and social responsibility, through a dedicated tool. Inspected automatic reminder configuration to ascertain that it had been configured to send reminders to all employees on a bimonthly basis.	No exception

SOC2 Criteria	SOC 2 Common Criteria Description	Control Number	Control description	Testing procedure	Criteria Conclusion
CC:1.2	COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	C.1.2.1	The responsibilities of the Board of Directors, which includes a majority of independent members, are defined, documented and available to employees and include oversight of the development and performance of internal controls. Board members meet on a quarterly basis.	Inspected the Board of Directors' charter to ascertain that they had been appropriately defined, documented, and made available to employees and to ascertain that it included the development and performance of internal controls. For a sample of quarter, inspected the board of directors' minutes to ascertain that board members meet on a quarterly basis.	No exception
CC:1.3	COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	C.1.3.1	The organization structure allows for a clear distinction of functions and responsibilities.	Inspected the organizational Chart and Dialogue Accountability Chart, to ascertain that the charts allowed for a clear distinction of functions and responsibilities.	No exception
		C.1.3.2	Dialogue management has established an organizational structure, reporting lines, authority, and responsibilities as part of its ongoing risk assessment and business planning processes. These structures are evaluated at least annually.	Inspected Dialogue's Accountability Chart to ascertain that organizational structure, as well as roles and responsibilities, are clearly defined and documented. Inspected evidence of the annual evaluation of the organizational structure to ascertain the structures are reviewed annually.	No exception
		C.1.3.3	Formal job descriptions are developed and maintained for each position. Job evaluation framework defines the expectation of each level.	For a sample of positions, inspected the formal job description to ascertain that they had been developed, maintained and that a job evaluation framework defined the expectations for this position.	No exception
CC:1.4	COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in	C.1.3.3	Formal job descriptions are developed and maintained for each position. Job evaluation framework defines the expectation of each level.	For a sample of positions, inspected the formal job description to ascertain that they had been developed, maintained and that a job evaluation framework defined the expectations for this position.	No exception

SOC2 Criteria	SOC 2 Common Criteria Description	Control Number	Control description	Testing procedure	Criteria Conclusion
	alignment with objectives.	C.1.4.2	New employee hiring procedures are in place to guide the hiring process and include verification that candidates possess the required qualifications to perform the duties as outlined in the job description.	Inspected the hiring procedure in place to ascertain that the hiring process had included a verification that the candidate possessed the required qualifications to perform the duties as outlined in the job description.	No exception
		C.1.4.3	As a component of the hiring process, pre-hiring verification procedures that include criminal background checks and work experience checks are performed prior to hiring.	Inspected a sample of new hires to ascertain that verification procedures that include criminal background checks and work experience checks had been performed prior to hiring.	No exception
		C.1.4.4	A defined budget is set aside for continuous training and is made available to the Software Engineering team to keep them up to date with evolving requirements.	Inspected the budget for the year to ascertain that a portion had been aside for continuous training and was made available to the Software Engineering team to keep them up to date with evolving requirements.	No exception
		C.1.4.5	Employees and contractors are required to complete security awareness training on an annual basis, a record of attendance is maintained and follow-up with the individuals is made in case of nonattendance.	Inspected evidence of training completion for a sample of active employees and contractors to ascertain that they had completed their security awareness training on an annual basis as required.	No exception
		C.1.4.6	Employee performance evaluations are performed on a semi-annual basis. The performance evaluation is acknowledged by the manager and employee. Corrective actions, including training, development, and performance improvement plans, are applied as necessary.	For a selection of employees, inspected the performance evaluations to ascertain that performance evaluation was acknowledged by the manager and employee and included corrective actions as necessary.	No exception
		C.1.1.5	Management has established separate communication channels in support of the functioning of the internal control components, including anonymous third-party administered whistle-blower hotlines available to internal and external users. Automatic reminders are sent to all employees on a bimonthly basis.	Inspected anonymous communication (whistleblower) policy in place to ascertain that it directed employees to identify and report on concerns and other complaints related to various topics of interest, including satisfaction, ethics, and social responsibility, through a dedicated tool. Inspected automatic reminder configuration to ascertain that it had been configured to send reminders to all employees on a bimonthly basis.	No exception

SOC2 Criteria	SOC 2 Common Criteria Description	Control Number	Control description	Testing procedure	Criteria Conclusion
CC:1.5	COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	C.1.1.3	The SEMT monitors employees' compliance with Dialogue's core values and the HR Policies through the monitoring of Dialogue's Members, Clients, and employees' feedback.	Inspected the reports used by the SEMT to ascertain that they had monitored members, clients, and employees' feedback.	No exception
		C.1.3.3	Formal job descriptions are developed and maintained for each position. Job evaluation framework defines the expectation of each level.	For a sample of positions, inspected the formal job description to ascertain that they had been developed, maintained and that a job evaluation framework defined the expectations for this position.	No exception
		C.1.4.6	Employee performance evaluations are performed on a semi-annual basis. The performance evaluation is acknowledged by the manager and employee. Corrective actions, including training, development, and performance improvement plans, are applied as necessary.	For a selection of employees, inspected the performance evaluations to ascertain that performance evaluation was acknowledged by the manager and employee and included corrective actions as necessary.	No exception
		C.1.5.2	The SEMT establishes performance measures that are aligned with objectives and are reviewed at least annually.	Inspected the minutes of the SEMT meeting when performance measures were reviewed to ascertain that the SEMT establishes performance measures aligned with the company's strategic objectives and reviews them at least annually.	No Exception
CC2.0 – Communication					
CC:2.1	COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	C.2.1.1	Monitoring software is in place to identify and evaluate ongoing system performance, security threats, changing resource utilization needs and unusual system activity. This software sends a message automatically to the operations center.	Inspected the configuration of monitoring software to ascertain that such monitoring software was in place to monitor unusual system performance, security threats, changing resource utilization needs or unusual system activity and to ascertain that automatic messages had been configured.	No exception
		C.2.1.2	SEMT holds weekly meetings (or more as needed) to provide an update on key performance indicators ("KPIs") and functions.	For a sample of SEMT's weekly meeting, inspected the meeting minutes to ascertain that the SEMT had provided an update on KPIs and functions.	No exception

SOC2 Criteria	SOC 2 Common Criteria Description	Control Number	Control description	Testing procedure	Criteria Conclusion
		C.2.1.3	Incidents are logged within a ticketing system and assigned a priority rating using a formal risk assessment formula.	For a sample of incidents, inspected the incident tickets to ascertain those incidents had been logged within a ticketing system and assigned a priority rating using a formal risk assessment formula.	No exception
		C.7.2.1	Incidents are identified and acted upon in a timely manner (same day resolution or mitigation for Priority 0, 2 days for Priorities 1 and 10 days for Priority 2 incidents).	For a sample of incidents, inspected the ticket to ascertain that those incidents had been identified and acted upon in a timely manner (same day resolution or mitigation for Priority 0, 2 days for Priorities 1 and 10 days for Priority 2 incidents).	No exception
		C.2.1.5	Dialogue has implemented processes and procedures relevant to security to produce internal information that is timely, accurate, complete, accessible, and protected.	Inspected the Information Security Policy to ascertain that processes and procedures are in place to ensure that sensitive digital data and critical business systems are identified during the assessment, including internal and external sources of data.	No exception
CC:2.2	COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	C.1.3.2	Dialogue management has established an organizational structure, reporting lines, authority, and responsibilities as part of its ongoing risk assessment and business planning processes. These structures are evaluated at least annually.	Inspected Dialogue's Accountability Chart to ascertain that organizational structure, as well as roles and responsibilities, are clearly defined and documented. Inspected evidence of the annual evaluation of the organizational structure to ascertain the structures are reviewed annually.	No exception
		C.1.3.3	Formal job descriptions are developed and maintained for each position. Job evaluation framework defines the expectation of each level.	For a sample of positions, inspected the formal job description to ascertain that they had been developed, maintained and that a job evaluation framework defined the expectations for this position.	No exception
		C.1.4.5	Employees and contractors are required to complete security awareness training on an annual basis, a record of attendance is maintained and follow-up with the individuals is made in case of non. Attendance.	Inspected evidence of training completion for a sample of active employees and contractors to ascertain that they had completed their security awareness training on an annual basis as required.	No exception

SOC2 Criteria	SOC 2 Common Criteria Description	Control Number	Control description	Testing procedure	Criteria Conclusion
		C.2.2.1	An Information Security policy is in place and is made available to employees and contractors. The policy includes a description of the roles and responsibilities assigned to individuals within the organization regarding security (including access control, incident handling and change requests). The policy is reviewed annually, and changes are approved by the EMT.	Inspected the policy and evidence of it being shared internally to ascertain that an Information Security policy is in place, that it's available to employees and contractors, that the policy is reviewed annually, that changes to the policy are approved by the EMT and that it outlines the roles and responsibilities regarding security, including access control, incident management, and change requests.	No exception
		C.2.2.2	Significant changes to senior management, VP or C-level roles and responsibilities are communicated internally and externally.	For a sample of significant changes to senior management, VP or C-level roles and responsibilities, inspected evidence of the communication to ascertain that the changes had been adequately communicated internally and externally.	No exception
		C.2.2.3	The SEMT establishes quarterly objectives that are reviewed by the Board of Directors. Performance is presented to the Board of Directors every quarter.	For a sample of quarter, inspected the board of directors' minutes to ascertain that the SEMT established quarterly objectives that had been reviewed by the Board of Directors and to ascertain that the performance had been presented to the Board of Directors as well.	No exception
		C.1.1.5	Management has established separate communication channels in support of the functioning of the internal control components, including anonymous third-party administered whistle-blower hotlines available to internal and external users. Automatic reminders are sent to all employees on a bimonthly basis.	Inspected anonymous communication (whistleblower) policy in place to ascertain that it directed employees to identify and report on concerns and other complaints related to various topics of interest, including satisfaction, ethics, and social responsibility, through a dedicated tool. Inspected automatic reminder configuration to ascertain that it had been configured to send reminders to all employees on a bimonthly basis.	No exception
		C.2.2.4	Incident management guidelines and procedures are documented, communicated to internal users.	Inspected the incident management policy and evidence of its communication to ascertain that it defines the steps for identifying and handling incidents and that it is communicated to internal users.	No exception

SOC2 Criteria	SOC 2 Common Criteria Description	Control Number	Control description	Testing procedure	Criteria Conclusion
		C.2.2.5	Dialogue posts a description of its IT services, system boundaries, and system processes that include infrastructure, software, people, processes and procedures and data on its intranet for internal users.	Inspected Dialogue's intranet to ascertain that a description of IT services, system boundaries, and system processes that include infrastructure, software, people, processes and procedures and data was available to internal users.	No exception
CC:2.3	COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	C.2.3.1	Dialogue posts notifications about customer impacting changes to the public website.	Inspected Dialogue's public website to ascertain that documentation about customer impacting changes had been made available to Dialogues Members and Clients.	No exception
		C.2.2.2	Significant changes to senior management, VP or C-level roles and responsibilities are communicated internally and externally.	For a sample of significant changes to senior management, VP or C-level roles and responsibilities, inspected evidence of the communication to ascertain that the changes had been adequately communicated internally and externally.	No exception
		C.2.3.2	Dialogue security commitments regarding the system are included in the master services agreement with their clients. In addition, a summary of these commitments is available on Dialogue's public website.	For a selection of clients, inspected the contracts to ascertain that Dialogue's security commitments regarding the system are included in the master services agreement with Clients. Inspected Dialogue's public website to ascertain that a summary of these commitments is available.	No exception
		C.2.3.3	Documentation of system operations is available to Dialogues Members and Clients on Dialogue's public website.	Inspected Dialogue's public website to ascertain that documentation of system operations had been made available to Dialogues Members and Clients.	No exception
		C.2.3.4	Clients' responsibilities, which include reporting operational failures, incidents, problems, concerns and complaints, and the process of doing so, are described in Dialogue's public website.	Inspected Dialogue's public website to ascertain that clients' responsibilities, which include reporting operational failures, incidents, problems, concerns and complaints, and the process of doing so, are described.	No exception

SOC2 Criteria	SOC 2 Common Criteria Description	Control Number	Control description	Testing procedure	Criteria Conclusion
CC3.0 – Risk assessment					
CC:3.1	COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	C.1.3.2	Dialogue management has established an organizational structure, reporting lines, authority, and responsibilities as part of its ongoing risk assessment and business planning processes. These structures are evaluated at least annually.	Inspected Dialogue's Accountability Chart to ascertain that organizational structure, as well as roles and responsibilities, are clearly defined and documented. Inspected evidence of the annual evaluation of the organizational structure to ascertain the structures are reviewed annually.	No exception
		C.3.1.1	The SEMT evaluates the need for additional tools and resources in order to achieve business and security objectives, while assessing risks involved.	Inspected the SEMT meetings' minutes to ascertain that the SEMT had evaluated the need for additional tools and resources in order to achieve business objectives, while assessing risks involved.	No exception
		C.3.1.2	Dialogue has defined a formal risk management process that includes risk and fraud identification, assessment, and mitigation plans. Risk and fraud assessments are documented, updated quarterly by the SEMT, and includes risk and fraud identification, assessment, and mitigation plans. Resources are allocated per the risk assessment results.	Inspected the risk management process and the risk register to ascertain whether a formal risk management process that includes risk and fraud identification, assessment and mitigation plans had been implemented. For a sample of quarters, inspected the documentation of the quarterly risk and fraud assessments performed by the SEMT to ascertain it included risk and fraud identification, assessment and mitigation plans which included resource allocation where applicable.	No exception
		C.3.1.3	The Privacy Officer, General Counsel and Compliance Manager are responsible for ensuring that dialogue complies with applicable laws, regulations, and standards.	Inspected the Privacy Officer, General Counsel and Compliance Manager job descriptions to ascertain that it included responsibilities to ensure that dialogue complied with applicable laws, regulations, and standards.	No exception
CC:3.2	COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for	C.2.1.1	Monitoring software is in place to identify and evaluate ongoing system performance, security threats, changing resource utilization needs and unusual system activity. This software sends a message automatically to the operations center.	Inspected the configuration of monitoring software to ascertain that such monitoring software was in place to monitor unusual system performance, security threats, changing resource utilization needs or unusual system activity and to ascertain that automatic messages had been configured.	No exception

SOC2 Criteria	SOC 2 Common Criteria Description	Control Number	Control description	Testing procedure	Criteria Conclusion
	determining how the risks should be managed.	C.3.1.2	Dialogue has defined a formal risk management process that includes risk and fraud identification, assessment, and mitigation plans. Risk and fraud assessments are documented, updated quarterly by the SEMT, and includes risk and fraud identification, assessment, and mitigation plans. Resources are allocated per the risk assessment results.	Inspected the risk management process and the risk register to ascertain whether a formal risk management process that includes risk and fraud identification, assessment and mitigation plans had been implemented. For a sample of quarters, inspected the documentation of the quarterly risk and fraud assessments performed by the SEMT to ascertain it included risk and fraud identification, assessment and mitigation plans which included resource allocation where applicable.	No exception
		C.3.2.2	Dialogue engages third-party security specialists to conduct internal and external vulnerability assessments at least annually. Findings are assessed, communicated, and acted upon as needed.	Inspected the results of the third-party security specialists' internal and external vulnerability assessments to ascertain vulnerability assessments were performed at least annually and whether the findings had been assessed, communicated, and acted upon as needed.	No exception
		C.3.2.3	Annually, management obtains, and reviews reports on controls provided by subservience organizations and evaluates the impact on Dialogue's internal controls.	Inspected the annual review of subservice organizations SOC reports to ascertain that management obtains, and reviews reports on controls provided by subservience organizations and evaluates the impact on Dialogue's internal controls.	No exception
CC:3.3	COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.	C.1.1.5	Management has established separate communication channels in support of the functioning of the internal control components, including anonymous third-party administered whistle-blower hotlines available to internal and external users. Automatic reminders are sent to all employees on a bimonthly basis.	Inspected anonymous communication (whistleblower) policy in place to ascertain that it directed employees to identify and report on concerns and other complaints related to various topics of interest, including satisfaction, ethics, and social responsibility, through a dedicated tool. Inspected automatic reminder configuration to ascertain that it had been configured to send reminders to all employees on a bimonthly basis.	No exception

SOC2 Criteria	SOC 2 Common Criteria Description	Control Number	Control description	Testing procedure	Criteria Conclusion
		C.2.3.2	Dialogue security commitments regarding the system are included in the master services agreement with their clients. In addition, a summary of these commitments is available on Dialogue's public website.	For a selection of clients, inspected the contracts to ascertain that Dialogue's security commitments regarding the system are included in the master services agreement with Clients. Inspected Dialogue's public website to ascertain that a summary of these commitments is available.	No exception
		C.2.3.4	Clients' responsibilities, which include reporting operational failures, incidents, problems, concerns and complaints, and the process of doing so, are described in Dialogue's public website.	Inspected Dialogue's public website to ascertain that clients' responsibilities, which include reporting operational failures, incidents, problems, concerns and complaints, and the process of doing so, are described.	No exception
		C.3.1.2	Dialogue has defined a formal risk management process that includes risk and fraud identification, assessment, and mitigation plans. Risk and fraud assessments are documented, updated quarterly by the SEMT, and includes risk and fraud identification, assessment, and mitigation plans. Resources are allocated per the risk assessment results.	Inspected the risk management process and the risk register to ascertain whether a formal risk management process that includes risk and fraud identification, assessment and mitigation plans had been implemented. For a sample of quarters, inspected the documentation of the quarterly risk and fraud assessments performed by the SEMT to ascertain it included risk and fraud identification, assessment and mitigation plans which included resource allocation where applicable.	No exception
		C.3.3.1	Guidelines for employees to identify fraudulent activities and to report suspected fraudulent acts are established.	Inspected evidence that the guidelines to identify fraudulent activities and report suspected fraudulent acts are established and available via intranet to all employees	No exception
CC:3.4	COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.	C.1.3.2	Dialogue management has established an organizational structure, reporting lines, authority, and responsibilities as part of its ongoing risk assessment and business planning processes. These structures are evaluated at least annually.	Inspected Dialogue's Accountability Chart to ascertain that organizational structure, as well as roles and responsibilities, are clearly defined and documented. Inspected evidence of the annual evaluation of the organizational structure to ascertain the structures are reviewed annually.	No exception

SOC2 Criteria	SOC 2 Common Criteria Description	Control Number	Control description	Testing procedure	Criteria Conclusion
		C.3.1.2	Dialogue has defined a formal risk management process that includes risk and fraud identification, assessment, and mitigation plans. Risk and fraud assessments are documented, updated quarterly by the SEMT, and includes risk and fraud identification, assessment, and mitigation plans. Resources are allocated per the risk assessment results.	Inspected the risk management process and the risk register to ascertain whether a formal risk management process that includes risk and fraud identification, assessment and mitigation plans had been implemented. For a sample of quarters, inspected the documentation of the quarterly risk and fraud assessments performed by the SEMT to ascertain it included risk and fraud identification, assessment and mitigation plans which included resource allocation where applicable.	No exception
		C.3.2.3	Annually, management obtains, and reviews reports on controls provided by subservience organizations and evaluates the impact on Dialogue's internal controls.	Inspected the annual review of subservice organizations SOC reports to ascertain that management obtains, and reviews reports on controls provided by subservience organizations and evaluates the impact on Dialogue's internal controls.	No exception
		C.3.4.1	An up-to-date high-level system architecture of Dialogue's system components are maintained, accounting for additions and removal and is posted on Dialogue's intranet and is available to its internal users.	Inspected Dialogue's high-level system architecture of system components to ascertain that it had been maintained, considered additions and removal and that it had been posted on Dialogue's intranet and that it had been available to its internal user.	No exception
		C.3.4.2	Management identifies and assesses changes to controls by performing an annual review of the control matrix.	Inspected the control matrix and a summary of control changes presented to the board of directors to ascertain that management identifies and assesses changes to the controls annually.	No exception
CC4.0 – Monitoring Activities					
CC:4.1	COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the	C.2.1.1	Monitoring software is in place to identify and evaluate ongoing system performance, security threats, changing resource utilization needs and unusual system activity. This software sends a message automatically to the operations center.	Inspected the configuration of monitoring software to ascertain that such monitoring software was in place to monitor unusual system performance, security threats, changing resource utilization needs or unusual system activity and to ascertain that automatic messages had been configured.	No exception

SOC2 Criteria	SOC 2 Common Criteria Description	Control Number	Control description	Testing procedure	Criteria Conclusion
	components of internal control are present and functioning.	C.3.2.2	Dialogue engages third-party security specialists to conduct internal and external vulnerability assessments at least annually. Findings are assessed, communicated, and acted upon as needed.	Inspected the results of the third-party security specialists' internal and external vulnerability assessments and the following internal communications to ascertain that the findings had been assessed, communicated, and acted upon as needed.	No exception
CC:4.2	COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.	C.4.2.1	Identified internal control deficiencies are followed up until resolution by the Compliance Manager. Report of deficiencies arising from security processes such as certification and accreditation, compliance, monitoring, audits, and vulnerability scans are provided to the board of directors and senior management.	For a sample of quarters, inspected the Ethics and Compliance reports to ascertain that internal control deficiencies are followed up until resolution by the Compliance Manager and to ascertain that the deficiencies are presented to the board of directors and senior management quarterly.	No exception
CC5.0 – Control activities					
CC:5.1	COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	C.2.1.1	Monitoring software is in place to identify and evaluate ongoing system performance, security threats, changing resource utilization needs and unusual system activity. This software sends a message automatically to the operations center.	Inspected the configuration of monitoring software to ascertain that such monitoring software was in place to monitor unusual system performance, security threats, changing resource utilization needs or unusual system activity and to ascertain that automatic messages had been configured.	No exception
		C.4.2.1	Identified internal control deficiencies are followed up until resolution by the Compliance Manager. Report of deficiencies arising from security processes such as certification and accreditation, compliance, monitoring, audits, and vulnerability scans are provided to the board of directors and senior management.	For a sample of quarters, inspected the Ethics and Compliance reports to ascertain that internal control deficiencies are followed up until resolution by the Compliance Manager and to ascertain that the deficiencies are presented to the board of directors and senior management quarterly.	No exception

SOC2 Criteria	SOC 2 Common Criteria Description	Control Number	Control description	Testing procedure	Criteria Conclusion
		C.3.1.1	The SEMT evaluates the need for additional tools and resources in order to achieve business and security objectives, while assessing risks involved.	Inspected the SEMT meetings' minutes to ascertain that the SEMT had evaluated the need for additional tools and resources in order to achieve business objectives, while assessing risks involved.	No exception
		C.3.1.2	Dialogue has defined a formal risk management process that includes risk and fraud identification, assessment, and mitigation plans. Risk and fraud assessments are documented, updated quarterly by the SEMT, and includes risk and fraud identification, assessment, and mitigation plans. Resources are allocated per the risk assessment results.	Inspected the risk management process and the risk register to ascertain whether a formal risk management process that includes risk and fraud identification, assessment and mitigation plans had been implemented. For a sample of quarters, inspected the documentation of the quarterly risk and fraud assessments performed by the SEMT to ascertain it included risk and fraud identification, assessment and mitigation plans which included resource allocation where applicable.	No exception
		C.3.2.2	Dialogue engages third-party security specialists to conduct internal and external vulnerability assessments at least annually. Findings are assessed, communicated, and acted upon as needed.	Inspected the results of the third-party security specialists' internal and external vulnerability assessments and the following internal communications to ascertain that the findings had been assessed, communicated, and acted upon as needed.	No exception
		C.5.1.1	As part of the Risk Management Program, risks and related mitigations are documented in the Risk Register.	Inspected Dialogue's risk register to ascertain that risks and mitigation plans are documented in the risk register.	No exception
CC:5.2	COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	C.1.3.2	Dialogue management has established an organizational structure, reporting lines, authority, and responsibilities as part of its ongoing risk assessment and business planning processes. These structures are evaluated at least annually.	Inspected Dialogue's Accountability Chart to ascertain that organizational structure, as well as roles and responsibilities, are clearly defined and documented. Inspected evidence of the annual evaluation of the organizational structure to ascertain the structures are reviewed annually.	No exception

SOC2 Criteria	SOC 2 Common Criteria Description	Control Number	Control description	Testing procedure	Criteria Conclusion
		C.2.1.1	Monitoring software is in place to identify and evaluate ongoing system performance, security threats, changing resource utilization needs and unusual system activity. This software sends a message automatically to the operations center.	Inspected the configuration of monitoring software to ascertain that such monitoring software was in place to monitor unusual system performance, security threats, changing resource utilization needs or unusual system activity and to ascertain that automatic messages had been configured.	No exception
		C.4.2.1	Identified internal control deficiencies are followed up until resolution by the Compliance Manager. Report of deficiencies arising from security processes such as certification and accreditation, compliance, monitoring, audits, and vulnerability scans are provided to the board of directors and senior management.	For a sample of quarters, inspected the Ethics and Compliance reports to ascertain that internal control deficiencies are followed up until resolution by the Compliance Manager and to ascertain that the deficiencies are presented to the board of directors and senior management quarterly.	No exception
		C.3.1.1	The SEMT evaluates the need for additional tools and resources in order to achieve business and security objectives, while assessing risks involved.	Inspected the SEMT meetings' minutes to ascertain that the SEMT had evaluated the need for additional tools and resources in order to achieve business objectives, while assessing risks involved.	No exception
		C.3.2.2	Dialogue engages third-party security specialists to conduct internal and external vulnerability assessments at least annually. Findings are assessed, communicated, and acted upon as needed.	Inspected the results of the third-party security specialists' internal and external vulnerability assessments and the following internal communications to ascertain that the findings had been assessed, communicated, and acted upon as needed.	No exception
		C.5.2.1	Management develops a list of control activities to manage the technology infrastructure and security access management risks identified during the risk assessment process.	Inspected the Cybersecurity Risk Assessment and Risk Registry to ascertain that Dialogue developed a list of control activities to manage the technology infrastructure and security access management risks.	No exception
		C.5.2.2	Dialogue uses documented methodologies for software development and acquisition, which includes a project management framework and change control procedures, including security and processing integrity.	Inspected Dialogue's policies documenting methodologies for software development and acquisition to ascertain that it was documented and included a project management framework and change control procedures, including security and processing integrity.	No exception

SOC2 Criteria	SOC 2 Common Criteria Description	Control Number	Control description	Testing procedure	Criteria Conclusion
CC:5.3	COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	C.1.1.3	The SEMT monitors employee's compliance with Dialogue's core values and the HR Policies through the monitoring of Dialogue's Members, Clients and employees' feedback.	Inspected the reports used by the SEMT to ascertain that they had monitored members, clients, and employees' feedback.	No exception
		C.2.2.1	An Information Security policy is in place and is made available to employees and contractors. The policy includes a description of the roles and responsibilities assigned to individuals within the organization regarding security (including access control, incident handling and change requests). The policy is reviewed annually, and changes are approved by the EMT.	Inspected the policy and evidence of it being shared internally to ascertain that an Information Security policy is in place, that it's available to employees and contractors, that the policy is reviewed annually, that changes to the policy are approved by the EMT and that it outlines the roles and responsibilities regarding security, including access control, incident management, and change requests.	No exception
CC6.0 – Logical and physical access					
CC:6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	C.2.3.3	Documentation of system operations is available to Dialogues Members and Clients on Dialogue's public website.	Inspected Dialogue's public website to ascertain that documentation of system operations had been made available to Dialogues Members and Clients.	No exception
		C.6.1.1	Access rights are assigned to security roles based on the requirements for the job function. User IDs are assigned security roles based on the individual's job responsibilities and are documented and approved by the employee's manager.	For a selection of users, inspected their access rights and the documentation of their roles and responsibility to ascertain that access rights are assigned to security roles based on the requirements for the job function and that user IDs are assigned security roles based on the individual's job responsibilities and is documented and approved by the employee's manager.	No exception
		C.6.1.2	Systems are configured to authenticate internal and external users with a unique user account and to enforce user account and password requirements to make the user individually accountable for access to the system.	Inspected system configurations to ascertain that they had been configured to authenticate internal and external users with a unique user account and to enforce user account and password requirements.	No exception
		C.6.1.3	Internal and external users meet password complexity and entropy standards.	Inspected system configurations to ascertain that Internal and external users meet password complexity and entropy standards.	No exception

SOC2 Criteria	SOC 2 Common Criteria Description	Control Number	Control description	Testing procedure	Criteria Conclusion
		C.6.1.4	Access to the production environment is restricted to authorized personnel and is only permitted through an encrypted connection (SSH) to the database private network managed and secured by a virtual private cloud (VPC).	Inspected system configurations to ascertain that access to the production environment is restricted to authorized personnel and is only permitted through an encrypted connection (SSH) to the database private network managed and secured by a virtual private cloud (VPC).	No exception
		C.6.1.5	The information security policy prohibits the transmission of sensitive information over the Internet or other public communications paths (e.g., e-mail) unless it is encrypted.	Inspected the information security policy to ascertain that it prohibits the transmission of sensitive information over the Internet or other public communications paths (e.g., e-mail) unless it is encrypted.	No exception
		C.6.1.6	At least annually, user access rights reviews are performed by compliance on employees, care professionals and contractors, including system administrators, and corrections are applied, when necessary, in a timely manner.	Inspected a sample of quarterly user access review documentation to ascertain that the user access rights reviews were performed by compliance on employees, care professionals and contractors, including system administrators, and corrections were applied in a timely manner.	Exception noted – Although the user access review was performed as per the defined frequency, for two sampled user access reviews, the reviews were not completed timely following the extraction of the user list to be reviewed. In addition, the user access review is not designed to assess whether access permissions are still required for active personnel.
		C.6.1.7	Communications use secure transport such as SSL and HTTPS.	Inspected system configurations to ascertain that communications use secure transport such as SSL and HTTPS.	No exception

SOC2 Criteria	SOC 2 Common Criteria Description	Control Number	Control description	Testing procedure	Criteria Conclusion
		C.6.1.8	Care professionals and Software Engineering team members use two-factor authentication which is enforced by the system.	Inspected system configuration to ascertain that the two-factor authentication had been enforced for care professionals and Software Engineering.	No exception
		C.6.1.9	Firewall configurations restrict connections between entrusted networks and any system components in Dialogue's environment.	Inspected system configuration to ascertain that firewall configurations restrict connections between entrusted networks and any system components in Dialogue's environment.	No exception
CC:6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	C.6.2.1	Employee, care professional and contractor user IDs are created only after being approved by management.	For a sample of new users ID, inspected the documented approval to ascertain that to ensure that employee, care professional and contractor user IDs are created only after being approved by management.	No exception
		C.6.2.2	Presto Organization Accounts are created and Presto Administrators (i.e., Clients HR administrators when requested) are assigned by Dialogue's Presto Super Administrator.	For a sample of new clients, observe the platform to ascertain that the Presto Organization account was created and the communication to the client to ascertain that Presto Administrators have been assigned by Dialogue's Presto Super Administrator.	No exception.
		C.6.2.3	Upon request from an authorized client representative, Member accounts are created by Dialogue's Presto Super Administrator.	For a selection of client requests, inspected the request to ascertain that Member accounts were created by Dialogue's Presto Super Administrator upon request from an authorized client representative.	No exception
		C.6.2.4	Upon request from the client, Member accounts are deactivated by Dialogue's Presto Super Administrator in a timely manner.	For a selection of Member accounts deactivation requests, inspected the requests to ascertain that Member accounts were deactivated by Dialogue's Presto Super Administrator in a timely manner .	No exception
		C.6.2.5	Upon Member signup, the account is activated if the Member is on the eligibility list.	Using a test account, observe the member sign-up process to ascertain that the account had been activated only if the member was on the eligibility list.	No exception

SOC2 Criteria	SOC 2 Common Criteria Description	Control Number	Control description	Testing procedure	Criteria Conclusion
		C.6.2.6	In accordance with the off-boarding procedure, employee, care professional and contractor user IDs are removed according to the date of termination and physical assets including, if any, computers, accessories, and office keys, are returned.	For a sample of the terminated employees, care professionals and contractors, inspected the off-boarding tickets to ascertain that user IDs were removed according to the date of termination and physical assets including, if any, computers, accessories, and office keys, were returned.	No exception
		C.6.2.7	Upon contract termination, or within 7 days, all Presto Administrators are deactivated.	For a sample of terminated Presto administrators, inspected the logs to ascertain that Presto Administrators had been deactivated upon contract termination or within 7 days.	No exception
		C.6.1.6	At least annually, user access rights reviews are performed by compliance on employees, care professionals and contractors, including system administrators, and corrections are applied, when necessary, in a timely manner.	Inspected a sample of quarterly user access review documentation to ascertain that the user access rights reviews were performed by compliance on employees, care professionals and contractors, including system administrators, and corrections were applied in a timely manner.	Exception noted – Although the user access review was performed as per the defined quarterly frequency, for two sampled user access reviews, the reviews were not completed timely following the extraction of the user list to be reviewed. In addition, the user access review is not designed to assess whether access permissions are still required for active personnel.

SOC2 Criteria	SOC 2 Common Criteria Description	Control Number	Control description	Testing procedure	Criteria Conclusion
CC:6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	C.6.1.1	Access rights are assigned to security roles based on the requirements for the job function. User IDs are assigned security roles based on the individual's job responsibilities and are documented and approved by the employee's manager.	For a selection of users, inspected their access rights and the documentation of their roles and responsibility to ascertain that access rights are assigned to security roles based on the requirements for the job function and that user IDs are assigned security roles based on the individual's job responsibilities and is documented and approved by the employee's manager.	No exception
		C.6.2.4	Upon request from the client, Member accounts are deactivated by Dialogue's Presto Super Administrator in a timely manner.	For a selection of Member accounts deactivation requests, inspected the requests to ascertain that Member accounts were deactivated by Dialogue's Presto Super Administrator in a timely manner .	No exception
		C.6.2.7	Upon contract termination, or within 7 days, all Presto Administrators are deactivated.	For a sample of terminated Presto administrators, inspected the logs to ascertain that Presto Administrators had been deactivated upon contract termination or within 7 days.	No exception
		C.6.1.6	At least annually, user access rights reviews are performed by compliance on employees, care professionals and contractors, including system administrators, and corrections are applied, when necessary, in a timely manner.	Inspected a sample of quarterly user access review documentation to ascertain that the user access rights reviews were performed by compliance on employees, care professionals and contractors, including system administrators, and corrections were applied in a timely manner.	Exception noted – Although the user access review was performed as per the defined quarterly frequency, for two sampled user access reviews, the reviews were not completed timely following the extraction of the user list to be reviewed. In addition, the user access review is not designed to assess whether access permissions are still required for active personnel.

SOC2 Criteria	SOC 2 Common Criteria Description	Control Number	Control description	Testing procedure	Criteria Conclusion
CC:6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorize personnel to meet the entity's objectives.	C.3.2.3	Annually, management obtains, and reviews reports on controls provided by subservience organizations and evaluates the impact on Dialogue's internal controls.	Inspected the annual review of subservice organizations SOC reports to ascertain that management obtains, and reviews reports on controls provided by subservience organizations and evaluates the impact on Dialogue's internal controls.	No exception
		C.6.4.1	Dialogue office is protected by locking mechanisms, 24-hour video surveillance and an alarm system.	Observed Dialogue's office to ascertain that they had been protected by locking mechanisms, 24-hour video surveillance and an alarm system.	No exception
		C.6.4.2	Alarm codes for Dialogue's office are changed quarterly.	For a sample of quarters, inspected the communication on alarm codes changes to ascertain the alarm codes are changed quarterly.	No exception
CC:6.5	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	C.2.2.1	An Information Security policy is in place and is made available to employees and contractors. The policy includes a description of the roles and responsibilities assigned to individuals within the organization regarding security (including access control, incident handling and change requests). The policy is reviewed annually, and changes are approved by the EMT.	Inspected the policy and evidence of it being shared internally to ascertain that an Information Security policy is in place, that it's available to employees and contractors, that the policy is reviewed annually, that changes to the policy are approved by the EMT and that it outlines the roles and responsibilities regarding security, including access control, incident management, and change requests.	No exception
		C.6.2.6	In accordance with the off-boarding procedure, employee, care professional and contractor user IDs are removed according to the date of termination and physical assets including, if any, computers, accessories, and office keys, are returned.	For a sample of the terminated employees, care professionals and contractors, inspected the off-boarding tickets to ascertain that user IDs were removed according to the date of termination and physical assets including, if any, computers, accessories, and office keys, were returned.	No exception
		C.6.5.1	Dialogue employees' laptops are encrypted to ensure the protection and confidentiality of all information stored on local disks.	Inspected system configurations of the mobile device management system to ascertain that Dialogue employees' laptops are encrypted.	No exception

SOC2 Criteria	SOC 2 Common Criteria Description	Control Number	Control description	Testing procedure	Criteria Conclusion
		C.6.5.2	Dialogue Information Security Sensitive Asset Policy defines measures that include sending, storing, or disposing of information in a manner commensurate with the sensitivity of the information.	Inspected Dialogue's privacy policy to ascertain that it defined measures that include sending, storing, or disposing of information in a manner commensurate with the sensitivity of the information. Inspected system retention configuration to ascertain that financial and medical data are automatically purged after the retention period prescribed in the system.	No exception
CC:6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	C.3.2.2	Dialogue engages third-party security specialists to conduct internal and external vulnerability assessments at least annually. Findings are assessed, communicated, and acted upon as needed.	Inspected the results of the third-party security specialists' internal and external vulnerability assessments and the following internal communications to ascertain that the findings had been assessed, communicated, and acted upon as needed.	No exception
		C.6.1.2	Systems are configured to authenticate internal and external users with a unique user account and to enforce user account and password requirements to make the user individually accountable for access to the system.	Inspected system configurations to ascertain that they had been configured to authenticate internal and external users with a unique user account and to enforce user account and password requirements.	No exception
		C.6.1.4	Access to the production environment is restricted to authorized personnel and is only permitted through an encrypted connection (SSH) to the database private network managed and secured by a virtual private cloud (VPC).	Inspected system configurations to ascertain that access to the production environment is restricted to authorized personnel and is only permitted through an encrypted connection (SSH) to the database private network managed and secured by a virtual private cloud (VPC).	No exception
		C.6.1.5	The information security policy prohibits the transmission of sensitive information over the Internet or other public communications paths (e.g., e-mail) unless it is encrypted.	Inspected the information security policy to ascertain that it prohibits the transmission of sensitive information over the Internet or other public communications paths (e.g., e-mail) unless it is encrypted.	No exception

SOC2 Criteria	SOC 2 Common Criteria Description	Control Number	Control description	Testing procedure	Criteria Conclusion
		C.6.1.6	At least annually, user access rights reviews are performed by compliance on employees, care professionals and contractors, including system administrators, and corrections are applied, when necessary, in a timely manner.	Inspected a sample of quarterly user access review documentation to ascertain that the user access rights reviews were performed by compliance on employees, care professionals and contractors, including system administrators, and corrections were applied in a timely manner.	Exception noted – Although the user access review was performed as per the defined quarterly frequency, for two sampled user access reviews, the reviews were not completed timely following the extraction of the user list to be reviewed. In addition, the user access review is not designed to assess whether access permissions are still required for active personnel.
		C.6.1.7	Communications use secure transport such as SSL and HTTPS.	Inspected system configurations to ascertain that communications use secure transport such as SSL and HTTPS.	No exception
		C.6.1.8	Care professionals and Software Engineering team members use two-factor authentication which is enforced by the system.	Inspected system configuration to ascertain that the two-factor authentication had been enforced for care professionals and Software Engineering.	No exception
		C.6.6.1	Dialogue uses intrusion-prevention techniques to detect and/or prevent intrusions into the network.	Inspected system configuration to ascertain that intrusion prevention techniques were implemented to detect and/or prevent intrusions into the network.	No exception
		C.6.6.2	Access to the cloud and firewalls is strictly controlled; and users are required to meet password complexity and entropy standards.	Inspected lists of users to ascertain that access to the cloud and firewalls is strictly controlled. Inspected system configuration to ascertain users meet password complexity and entropy standards.	No exception

SOC2 Criteria	SOC 2 Common Criteria Description	Control Number	Control description	Testing procedure	Criteria Conclusion
CC:6.7	The entity restricts the transmission, movement, and removal of information to be authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	C.6.1.1	Access rights are assigned to security roles based on the requirements for the job function. User IDs are assigned security roles based on the individual's job responsibilities and are documented and approved by the employee's manager.	For a selection of users, inspected their access rights and the documentation of their roles and responsibility to ascertain that access rights are assigned to security roles based on the requirements for the job function and that user IDs are assigned security roles based on the individual's job responsibilities and is documented and approved by the employee's manager.	No exception
		C.6.1.5	The information security policy prohibits the transmission of sensitive information over the Internet or other public communications paths (e.g., e-mail) unless it is encrypted.	Inspected the information security policy to ascertain that it prohibits the transmission of sensitive information over the Internet or other public communications paths (e.g., e-mail) unless it is encrypted.	No exception
		C.6.1.7	Communications use secure transport such as SSL and HTTPS.	Inspected system configurations to ascertain that communications use secure transport such as SSL and HTTPS.	No exception
		C.6.7.1	Employees and contractors operating systems are configured to accept updates automatically. System hardening and configuration standards are defined for all system types.	Inspected system configurations to ascertain that system hardening and configuration standards are defined for all system types and that automated updates are applied for all operating systems.	No exception
		C.6.7.2	USB media must be encrypted before they can be used on laptop devices.	Inspected system configurations to ascertain that USB media must be encrypted before they can be used on laptop devices.	No exception
		C.6.7.3	Data backups are encrypted during creation.	Inspected system configurations to ascertain that data backups are encrypted during creation.	No exception
		C.6.7.4	Dialogue has implemented mobile device management policy and maintained the mobile device list.	Inspected the mobile device management policy to ascertain that it was implemented. Inspected the list of mobile devices to ascertain that a list was maintained.	No exception

SOC2 Criteria	SOC 2 Common Criteria Description	Control Number	Control description	Testing procedure	Criteria Conclusion
CC:6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	C.2.1.1	Monitoring software is in place to identify and evaluate ongoing system performance, security threats, changing resource utilization needs and unusual system activity. This software sends a message automatically to the operations center.	Inspected the configuration of monitoring software to ascertain that such monitoring software was in place to monitor unusual system performance, security threats, changing resource utilization needs or unusual system activity and to ascertain that automatic messages had been configured.	No exception
		C.6.1.5	The information security policy prohibits the transmission of sensitive information over the Internet or other public communications paths (e.g., e-mail) unless it is encrypted.	Inspected the information security policy to ascertain that it prohibits the transmission of sensitive information over the Internet or other public communications paths (e.g., e-mail) unless it is encrypted.	No exception
		C.6.1.6	At least annually, user access rights reviews are performed by compliance on employees, care professionals and contractors, including system administrators, and corrections are applied, when necessary, in a timely manner.	Inspected a sample of quarterly user access review documentation to ascertain that the user access rights reviews were performed by compliance on employees, care professionals and contractors, including system administrators, and corrections were applied in a timely manner.	Exception noted – Although the user access review was performed as per the defined quarterly frequency, for two sampled user access reviews, the reviews were not completed timely following the extraction of the user list to be reviewed. In addition, the user access review is not designed to assess whether access permissions are still required for active personnel.
		C.6.1.7	Communications use secure transport such as SSL and HTTPS.	Inspected system configurations to ascertain that communications use secure transport such as SSL and HTTPS.	No exception

SOC2 Criteria	SOC 2 Common Criteria Description	Control Number	Control description	Testing procedure	Criteria Conclusion
		C.6.7.1	Employees and contractors operating systems are configured to accept updates automatically. System hardening and configuration standards are defined for all system types.	Inspected system configurations to ascertain that system hardening and configuration standards are defined for all system types and that automated updates are applied for all operating systems.	No exception
		C.6.8.1	End users are only allowed to install applications from identified developers or the App Store.	Inspected system configurations to ascertain that end-users can only install applications from identified developers or the App Store.	No exception
CC7.0 – System operation					
CC:7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	C.2.1.1	Monitoring software is in place to identify and evaluate ongoing system performance, security threats, changing resource utilization needs and unusual system activity. This software sends a message automatically to the operations center.	Inspected the configuration of monitoring software to ascertain that such monitoring software was in place to monitor unusual system performance, security threats, changing resource utilization needs or unusual system activity and to ascertain that automatic messages had been configured.	No exception
		C.3.2.2	Dialogue engages third-party security specialists to conduct internal and external vulnerability assessments at least annually. Findings are assessed, communicated, and acted upon as needed.	Inspected the results of the third-party security specialists' internal and external vulnerability assessments and the following internal communications to ascertain that the findings had been assessed, communicated, and acted upon as needed.	No exception
		C.3.2.3	Annually, management obtains, and reviews reports on controls provided by subservience organizations and evaluates the impact on Dialogue's internal controls.	Inspected the annual review of subservice organizations SOC reports to ascertain that management obtains, and reviews reports on controls provided by subservience organizations and evaluates the impact on Dialogue's internal controls.	No exception
		C.6.7.1	Employees and contractors operating systems are configured to accept updates automatically. System hardening and configuration standards are defined for all system types.	Inspected system configurations to ascertain that system hardening and configuration standards are defined for all system types and that automated updates are applied for all operating systems.	No exception

SOC2 Criteria	SOC 2 Common Criteria Description	Control Number	Control description	Testing procedure	Criteria Conclusion
CC:7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	C.2.1.1	Monitoring software is in place to identify and evaluate ongoing system performance, security threats, changing resource utilization needs and unusual system activity. This software sends a message automatically to the operations center.	Inspected the configuration of monitoring software to ascertain that such monitoring software was in place to monitor unusual system performance, security threats, changing resource utilization needs or unusual system activity and to ascertain that automatic messages had been configured.	No exception
		C.3.2.2	Dialogue engages third-party security specialists to conduct internal and external vulnerability assessments at least annually. Findings are assessed, communicated, and acted upon as needed.	Inspected the results of the third-party security specialists' internal and external vulnerability assessments and the following internal communications to ascertain that the findings had been assessed, communicated, and acted upon as needed.	No exception
		C.3.2.3	Annually, management obtains, and reviews reports on controls provided by subservience organizations and evaluates the impact on Dialogue's internal controls.	Inspected the annual review of subservice organizations SOC reports to ascertain that management obtains, and reviews reports on controls provided by subservience organizations and evaluates the impact on Dialogue's internal controls.	No exception
		C.7.2.1	Incidents are identified and acted upon in a timely manner (same day resolution or mitigation for Priority 0, 2 days for Priorities 1 and 10 days for Priority 2 incidents).	For a sample of incidents, inspected the ticket to ascertain that the incident had been identified and acted upon in a timely manner (same day resolution or mitigation for Priority 0, 2 days for Priorities 1 and 10 days for Priority 2 incidents).	No exception
		C.7.2.2	High severity incidents are analyzed in postmortem reviews and a root cause analysis is prepared and reviewed.	For a sample of high severity incidents, inspected the postmortem reviews to ascertain that a root cause analysis was prepared and reviewed.	No exception
CC:7.3	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives	C.2.1.1	Monitoring software is in place to identify and evaluate ongoing system performance, security threats, changing resource utilization needs and unusual system activity. This software sends a message automatically to the operations center.	Inspected the configuration of monitoring software to ascertain that such monitoring software was in place to monitor unusual system performance, security threats, changing resource utilization needs or unusual system activity and to ascertain that automatic messages had been configured.	No exception

SOC2 Criteria	SOC 2 Common Criteria Description	Control Number	Control description	Testing procedure	Criteria Conclusion
	(security incidents) and, if so, takes actions to prevent or address such failures.	C.2.3.4	Clients' responsibilities, which include reporting operational failures, incidents, problems, concerns and complaints, and the process of doing so, are described in Dialogue's public website.	Inspected Dialogue's public website to ascertain that clients' responsibilities, which include reporting operational failures, incidents, problems, concerns and complaints, and the process of doing so, are described.	No exception
		C.7.2.1	Incidents are identified and acted upon in a timely manner with a security incident response plan (same day resolution or mitigation for Priority 0, 2 days for Priorities 1 and 10 days for Priority 2 incidents).	For a sample of incidents, inspected the ticket to ascertain that the incident had been identified and acted upon in a timely manner (same day resolution or mitigation for Priority 0, 2 days for Priorities 1 and 10 days for Priority 2 incidents).	No exception
		C.7.2.2	High severity incidents are analyzed in postmortem reviews and a root cause analysis is prepared and reviewed.	For a sample of high severity incidents, inspected the postmortem reviews to ascertain that a root cause analysis was prepared and reviewed.	No exception
		C.7.3.1	Security incidents are logged, tracked, and communicated to affected parties by management until resolved.	For a sample of security incidents, inspected the ticket to ascertain that incidents are logged, tracked, and communicated to affected parties by management until resolved.	No exception
CC:7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	C.2.1.1	Monitoring software is in place to identify and evaluate ongoing system performance, security threats, changing resource utilization needs and unusual system activity. This software sends a message automatically to the operations center.	Inspected the configuration of monitoring software to ascertain that such monitoring software was in place to monitor unusual system performance, security threats, changing resource utilization needs or unusual system activity and to ascertain that automatic messages had been configured.	No exception
		C.2.3.1	Dialogue posts notifications about customer impacting changes to the public website.	Inspected Dialogue's public website to ascertain that documentation about customer impacting changes had been made available to Dialogues Members and Clients.	No exception
		C.2.1.3	Incidents are logged within a ticketing system and assigned a priority rating using a formal risk assessment formula.	For a sample of incidents, inspected the incident tickets to ascertain those incidents had been logged within a ticketing system and assigned a priority rating using a formal risk assessment formula.	No exception

SOC2 Criteria	SOC 2 Common Criteria Description	Control Number	Control description	Testing procedure	Criteria Conclusion
		C.3.2.2	Dialogue engages third-party security specialists to conduct internal and external vulnerability assessments at least annually. Findings are assessed, communicated, and acted upon as needed.	Inspected the results of the third-party security specialists' internal and external vulnerability assessments and the following internal communications to ascertain that the findings had been assessed, communicated, and acted upon as needed.	No exception
		C.7.2.1	Incidents are identified and acted upon in a timely manner with a security incident response plan (same day resolution or mitigation for Priority 0, 2 days for Priorities 1 and 10 days for Priority 2 incidents).	For a sample of incidents, inspected the ticket to ascertain that the incident had been identified and acted upon in a timely manner (same day resolution or mitigation for Priority 0, 2 days for Priorities 1 and 10 days for Priority 2 incidents).	No exception
		C.7.2.2	High severity incidents are analyzed in postmortem reviews and a root cause analysis is prepared and reviewed.	For a sample of high severity incidents, inspected the postmortem reviews to ascertain that a root cause analysis was prepared and reviewed.	No exception
		C.7.4.1	A Data Security Incident Response Plan is documented, updated, and approved by management annually.	Inspected the Incident Response Plan to determine whether it had been documented, updated, and approved by management annually.	No exception
		C.7.4.2	Roles and responsibilities of teams involved in the incident response and the communications distribution list are identified.	Inspected the Incident Response Plan to ascertain that the roles and responsibilities of teams involved in the incident response and the communications distribution list are identified.	No exception
CC:7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	C.2.1.1	Monitoring software is in place to identify and evaluate ongoing system performance, security threats, changing resource utilization needs and unusual system activity. This software sends a message automatically to the operations center.	Inspected the configuration of monitoring software to ascertain that such monitoring software was in place to monitor unusual system performance, security threats, changing resource utilization needs or unusual system activity and to ascertain that automatic messages had been configured.	No exception
		C.2.3.1	Dialogue posts notifications about customer impacting changes to the public website.	Inspected Dialogue's public website to ascertain that documentation about customer impacting changes had been made available to Dialogues Members and Clients.	No exception

SOC2 Criteria	SOC 2 Common Criteria Description	Control Number	Control description	Testing procedure	Criteria Conclusion
		C.3.2.2	Dialogue engages third-party security specialists to conduct internal and external vulnerability assessments at least annually. Findings are assessed, communicated, and acted upon as needed.	Inspected the results of the third-party security specialists' internal and external vulnerability assessments to ascertain vulnerability assessments was performed at least annually and whether the findings had been assessed, communicated, and acted upon as needed.	No exception
		C.3.2.3	Annually, management obtains, and reviews reports on controls provided by subservience organizations and evaluates the impact on Dialogue's internal controls.	Inspected the annual review of subservice organizations SOC reports to ascertain that management obtains, and reviews reports on controls provided by subservience organizations and evaluates the impact on Dialogue's internal controls.	No exception
		C.7.2.2	High severity incidents are analyzed in postmortem reviews and a root cause analysis is prepared and reviewed.	For a sample of high severity incidents, inspected the postmortem reviews to ascertain that a root cause analysis was prepared and reviewed.	No exception
CC8.0 – Change management					
CC:8.1	The entity authorizes, designs, develops, or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	C.3.4.1	An up-to-date high-level system architecture of Dialogue's system components are maintained, accounting for additions and removal and is posted on Dialogue's intranet and is available to its internal users.	Inspected Dialogue's high-level system architecture of system components to ascertain that it had been maintained, considered additions and removal and that it had been posted on Dialogue's intranet and that it had been available to its internal user.	No exception
		C.8.1.1	Test environments are logically separated from production environments.	Observed the test and production environments to ascertain that they had been logically separated.	No exception
		C.8.1.2	An independent reviewer evaluates and approves system change requests via a pull request process, after which changes are deployed automatically to production.	For a sample of system changes, inspected the pull requests to ascertain that an independent reviewer had evaluated and approved the changes before they had been deployed automatically to production.	No exception
		C.8.1.3	The ability to push for changes to the production environment is restricted to Technology personnel.	Inspected the system configuration to ascertain that the ability to push changes to the production environment had been restricted to Software Engineering personnel.	No exception

SOC2 Criteria	SOC 2 Common Criteria Description	Control Number	Control description	Testing procedure	Criteria Conclusion
		C.8.1.4	Automated continuous integration testing of system changes is performed prior to deployment to the production environment.	For a sample of system changes, inspected log of testing to ascertain that the changes had been subjected to automated continuous integration testing prior to deployment to the production environment.	No exception
		C.8.1.5	Emergency changes follow the incident procedure, are analyzed in postmortem reviews and a root cause analysis is prepared and reviewed.	For a sample of emergency changes, inspected the tickets and postmortem analysis to ascertain that the incident procedure was followed and that a root cause analysis was prepared and reviewed.	No exception
CC9.0 – Risk mitigation					
CC:9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	C.3.1.1	The SEMT evaluates the need for additional tools and resources in order to achieve business and security objectives, while assessing risks involved.	Inspected the SEMT meetings' minutes to ascertain that the SEMT had evaluated the need for additional tools and resources in order to achieve business objectives, while assessing risks involved.	No exception
		C.3.1.2	Dialogue has defined a formal risk management process that includes risk and fraud identification, assessment, and mitigation plans. Risk and fraud assessments are documented, updated quarterly by the SEMT, and includes risk and fraud identification, assessment, and mitigation plans. Resources are allocated per the risk assessment results.	Inspected the risk management process and the risk register to ascertain that a formal risk management process that includes risk and fraud identification, assessment and mitigation plans had been implemented. For a sample of quarters, inspected the documentation of the quarterly risk and fraud assessments performed by the SEMT to ascertain it included risk and fraud identification, assessment and mitigation plans which included resource allocation where applicable.	No exception
		C.3.2.2	Dialogue engages third-party security specialists to conduct internal and external vulnerability assessments at least annually. Findings are assessed, communicated, and acted upon as needed.	Inspected the results of the third-party security specialists' internal and external vulnerability assessments to ascertain vulnerability assessments were performed at least annually and whether the findings had been assessed, communicated, and acted upon as needed.	No exception

SOC2 Criteria	SOC 2 Common Criteria Description	Control Number	Control description	Testing procedure	Criteria Conclusion
		C.3.2.3	Annually, management obtains, and reviews reports on controls provided by subservience organizations and evaluates the impact on Dialogue's internal controls.	Inspected the annual review of subservice organizations SOC reports to ascertain that management obtains, and reviews reports on controls provided by subservience organizations and evaluates the impact on Dialogue's internal controls.	No exception
		C.9.1.1	Dialogue subscribes to cyber and error and omission insurance policies to offset the financial impact in the event of a breach.	Inspected the cyber and error and omission insurance policies to ascertain that Dialogue had been subscribing to cyber and error and omission insurance policies.	No exception
		C.9.1.2	Dialogue Business Continuity and Disaster Recovery Plan is documented and tested annually.	Inspected Business Continuity and Disaster recovery Plan and the minutes of the annual tabletop exercise to ascertain the Business Continuity and Disaster Recovery Plan has been documented and tested annually.	No exception
CC:9.2	The entity assesses and manages risks associated with vendors and business partners.	C.3.2.3	Annually, management obtains, and reviews reports on controls provided by subservience organizations and evaluates the impact on Dialogue's internal controls.	Inspected the annual review of subservice organizations SOC reports to ascertain that management obtains, and reviews reports on controls provided by subservience organizations and evaluates the impact on Dialogue's internal controls.	No exception
		C.1.1.4	Upon hire, Dialogue's employees (including care professionals and contractors) are required to acknowledge and sign confidentiality / nondisclosure agreement.	For a sample of new employees, care professionals and contractors, inspected evidence of the signed formal nondisclosure/confidentiality agreement to ascertain that it had been acknowledged.	No exception
		C.9.2.1	To manage risks associated with vendors and business partners who are involved in the provisioning of virtual health care services or have access to Dialogue's systems, Dialogue obtains signed contracts or agreements which include a confidentiality clause.	For a sample of vendors and business partners who are involved in the provisioning of virtual health care services or have access to Dialogue's systems, inspected the contracts to ascertain that the agreements included a confidentiality clause.	No exception

Section 5 – Other Information Provided by Dialogue Health Technologies Inc. That is Not Covered by the Service Auditor's Report

Management's Response to Exceptions Identified by the Auditor

Dialogue has considered the exception noted during the audit and has developed a strategy for remediation. The table below provides an overview of changes to the control environment, which Dialogue has already implemented.

Ref.	Control Description	Deloitte Exception	Management's Response
C.6.1.6	At least annually, user access rights reviews are performed by compliance on employees, care. professionals and contractors, including system administrators, and corrections are applied, when necessary, in a timely manner.	Although the user access review was performed as per the defined frequency, for two sampled user access reviews, the reviews were not completed timely following the extraction of the user list to be reviewed. In addition, the user access review is not designed to assess whether access permissions are still required for active personnel.	We acknowledge the finding in the SOC2 report. Dialogue has processes in place to automatically grant and revoke user access based on role. To address the issue and enhance our access review process, we have deployed Okta Identity Governance and instituted a new bi-annual review process where each manager is responsible for reviewing the manually assigned accesses of their direct reports to ensure that access permissions are only maintained for users with a current legitimate business need. All unneeded accesses are removed as part of the review.

