CLARIO.
THE BEST OF ERT & BIOCLINICA

Data Privacy and Security Governance Program Overview

Introduction

This paper provides an overview of how Clario, on behalf of itself and each of its affiliates, including eResearchTechnology, Inc. and Bioclinica, Inc. (collectively "Clario"), complies with applicable data privacy laws and regulations to protect the Personal Data that it processes and retains. Clario is a global company with 30 facilities in nine countries across North America, Europe and Asia Pacific, including offices in the United States, the United Kingdom, the European Union, Switzerland, India, China, and Japan. Clario has instituted a global data privacy and security governance program (the "Program") to ensure compliance with applicable requirements globally.

The Program applies to any Personal Data or Personal Information (as defined under applicable data privacy laws and referred to herein as "Data") Clario may access, collect, acquire, use, disclose, store, transfer, retain, or dispose of (collectively, "Processing Activities") in all aspects of its business worldwide. The Program is designed in accordance with Data privacy laws and regulations that may apply directly to our processing of Data, including, without limitation, the European General Data Protection Regulation 2016/679 ("GDPR"), ICH E6 (R2) Good Clinical Practice, the Act on Protection of Personal Information ("APPI"), the California Consumer Privacy Act ("CCPA"), the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), and relevant U.S. Food and Drug Administration guidelines (i.e., 21 CFR Part 11).

Merger with Bioclinica: Clario's efforts to harmonize the Program infrastructure following the 2021 merger of eResearchTechnology, Inc. and Bioclinica, Inc. are ongoing. For the time being, there may be controlled documents, including policies and procedures, distinct to each entity. The Data Privacy Department, working with functional stakeholders across the Company, continues to lead the effort to ensure the Program is consistent for both entities.

Program Requirements

The Program is built around a company culture that respects an individual's right to privacy, which is embedded in the Company's Code of Ethics. The Program applies global standards in the following ways:

General Requirements

- Clario builds a culture of Data privacy compliance by communicating to its employees through mandatory training an awareness of, and appreciation for the importance of meeting, applicable statutory and regulatory Data privacy and security requirements.
- Clario has dedicated Data Privacy and IT Security teams that work to ensure Clario's ongoing compliance with applicable Data privacy laws and regulations.
- Clario has developed and implemented a comprehensive set of written policies and procedures that address applicable privacy and security obligations as outlined in **Appendix 2 and 3**. Clario periodically reviews and updates these policies and procedures in line with applicable data privacy laws and regulations.
- Clario is committed to observing and implementing "best practices" around Data privacy compliance for its business activities, operations, and services ("Services").
- Clario is a Data controller registered with the Information Commissioner's Office ("ICO") in the United Kingdom, the Bavarian Supervisory Authority ("BayLDA") in Germany, Datatilsynet in Denmark, Commission Nationale de l'Informatique et des Libertés ("CNIL") in France, the Federal Commissioner for Data Protection and Freedom of Information ("BfDI") in Germany, the Data Protection Commission ("DPC") in Ireland, the Dutch Data Protection Authority ("Autoriteit Persoonsgegevens") in the Netherlands, The National Supervisory Authority for Personal Data Processing in Romania, and The Federal Data Protection and Information Commissioner ("FDPIC") in Switzerland.

Data Risk Classification

Clario's Program takes a risk-based approach to assessing its Processing Activities. All Data is categorized in accordance with the Data's level or risk and sensitivity, as defined within our Privacy and Integrity Policy (POL-COR-0012) and as specifically outlined in Section 5.14 of it (the Data Risk Classification Chart ("Chart"), also attached hereto as **Appendix 1**).

Clario ensures that all Data it processes receives appropriate organizational and technical protection, but ensures additional scrutiny is applied to the processing of the most sensitive Data or clinical Data (classified on the Chart as "Critical"). When assessing Data risk, Clario looks at the probability that an individual data subject may be reasonably identified, whether traceability aspects exist, and the potential financial, legal, or reputational harm that may be caused to the data subject.

Privacy and Security by Design

As part of Clario's Product Life Cycle Policy (POL-COR-0008), Clario requires the completion of Data Privacy Impact Assessments ("DPIA") and Security Impact Assessments ("SIA") both at the start of any major project involving the processing of Data as well as when there may be a significant change to an existing project or process that involves the processing of Data. The DPIA identifies the types of Data processed; describes the nature, scope, context, and purposes of the processing; and identifies any risks that may be posed by the processing and that must be addressed to comply with applicable privacy laws

and regulations, including the "data minimization" principle that applies under data privacy legal and regulatory regimes including the GDPR and CCPA. The SIA assesses the technical controls that are in place (or that must be in place) to protect Data, including the architectural framework and methodology of encryption.

Data Transfers / Data Localization

Clario's Services are performed globally and, depending on the service line, Processing Activities may occur at any one of the Company's affiliate locations, including within the United States as well as at any one of the Company's international offices located in India, the United Kingdom, Germany, Japan, Switzerland, Belgium, France, and China. Clario's primary data centers are located within the United States and Germany, and Data will be remotely accessed from all company personnel locations.

Provided that transfers of Data are required to perform Activities, Clario ensures it is compliant with all applicable Data transfer requirements, including those required for transfers outside the European Economic Area, Switzerland, the United Kingdom, and other regions. Such transfers are performed in compliance with Program requirements, applicable Data privacy and security laws and regulations, and in conformance with the Court of Justice of the European Union's judgment in Data Protection Commissioner v. Facebook Ireland Limited, Maximillian Schrems (C-311/18) ("Schrems II") as well as the updated Standard Contractual Clauses that went into effect on 4JUNE2021. Such transfers are carried out only to perform the applicable services required of Clario or its agents (where applicable) and where Data subjects have consented to the transfers, where required.

In addition, Clario also ensures any Data transfers comply with relevant Data privacy and security laws and regulations mandating the localization and/or residency of Data, including the Data Security Law ("DSL") in the People's Republic of China and Article 18(6) of the Russian Federal Law on Personal Data (No. 152-FZ).

Data Minimization / Record Retention

In recent years, the enforcement of applicable data privacy laws and regulations (including, among others, the GDPR and CCPA) has made clear the criticality of complying with the principle of "data minimization," which includes implementing practices to ensure (a) that only the Data required to accomplish the particular purpose for which processing is undertaken is collected, and (b) that this Data is retained only for the period of time necessary to accomplish the particular purpose for which the Data was processed. As noted above, Clario approaches the design of new projects and significant updates to existing projects involving Data with a focus on complying with relevant data privacy principles, including data minimization. Clario also works with its customers to ensure study protocols are designed such that the Company collects only the specific Data required to achieve the particular purpose for which the Data is processed. This includes, for example, collecting pseudonymized clinical trial Data and, where possible, avoiding the collection of any patient identifying information such as complete birth dates.

Clario is in the process of implementing a new records retention policy pursuant to which the Company will, subject to overriding statutory, regulatory, or contractual retention requirements and legacy systems limitations, retain customers' clinical trial data in hardcopy and electronic form for seven (7) years after the date on which the database lock for the study occurred, or as required for a specific business line and determined in the individual Work Order. The implementation of this new retention policy is ongoing.

Subcontractors / Sub-processors

Clario carefully selects its third-party vendors in accordance with Program requirements as part of the procurement process. Before vendors are onboarded, a Vendor Data Surveys ("VDS") is conducted to understand and classify in accordance with the Chart the types of Data that will be collected. If the vendor will be processing Data, a Data Privacy Impact Assessment ("DPIA") and Security Impact Assessment ("SIA") also will be conducted to ensure that such vendors are held to standards that are as stringent as those under the master services agreements or Data processing agreements (collectively, "Agreements") in which Clario enters with its Customers (typically, clinical trial sponsors and clinical research organizations ("CROs")). A list of vendors is provided to Customers upon the written request of the sponsor, in accordance with applicable Agreement requirements.

Privacy Events: Unauthorized Disclosures, Data Breaches, and Security Incidents

Clario has a comprehensive policy and process to identify, remediate, and timely notify Customers of actual, or potential, privacy and security events that may implicate Data or data privacy rights. Pursuant to our Data Privacy and Security Incident Management SOP-COR-0004, any Clario personnel or agent (where applicable) who becomes aware of any potential or identified Unauthorized Disclosure, Data Breach, or Security Incident is required to report the event to the Data Privacy and/or IT Security Department(s) within the same calendar day of becoming aware so the event can be investigated and remediated as appropriate. Customers impacted by a privacy event shall be informed without undue delay and in accordance with contractual requirements. In addition, Clario has a defined disciplinary policy that applies to personnel who cause violations of Data privacy law or regulation to occur.

For events that are classified as a Data Breach, Security Incident, or that otherwise require remediation actions, an Incident Report shall be generated within 45 days of the completion of an investigation into the event. The Incident Report shall include a complete issue analysis (i.e., root cause) and outline resolution and remediation actions (i.e., corrective and preventative actions).

Subject Access Requests ("SARs")

Clario has implemented policies and procedures supporting Subject Access Requests ("SAR") that outline the processes that are required to comply with the exercise of individuals' data privacy rights and to ensure compliance with the applicable data protection laws and regulations.

An individual may submit a SAR at any time to find out more about the Data Clario holds about them. Such requests can be made via the DSAR link on Clario's external website

(https://ertprivacy.exterro.net/portal/dsar.htm?target=ertprivacy) or by calling at our toll free telephone number +1-800-515-2279 in compliance with the CCPA.

Clario will respond to SARs within 30 days of receipt, and in compliance with applicable Data privacy laws and regulations, unless additional time is warranted due to the complexity of the request, at which point the requestor will be informed of the need for an extension.

In addition to "standard" SARs submitted by an individual data subject, Clario has developed a process for the removal of Unauthorized Personally Identifiable Information ("Unauthorized PII") is Data that is outside the data parameters outlined in the governing study protocol or project documentation that was transmitted to Clario in error by clinical trial sites and received within Clario systems. Clario leverages its SAR process to ensure Customers are informed of occurrences involving Unauthorized PII, and provided the information necessary to determine the best course of action, including potential redaction or deletion of the data from Clario's systems, as well as to appropriately document the chosen course of action.

Clario Employee Informed Consent and Privacy Notice

As part of Clario's ongoing initiative to increase its Data privacy and security posture and ensure compliance with Program requirements and applicable Data protection laws and regulations, the Company has implemented an employee informed consent process or Data privacy notice to provide increased transparency around how the Company processes employees' Data.

Data Privacy and Security Training

Clario has established and implemented Data privacy and security training and educational programming for employees that promotes the core privacy and security principles underpinning the Program. This includes Clario's comprehensive Global Data Privacy Training ("GDPT").

The GDPT is an annual mandatory interactive training designed to introduce employees as well as any Company agents, consultants, contractors, and other associates whose work involves the processing of Data to Program requirements and applicable Data privacy laws and regulations. The GDPT includes a required review of Clario's corporate privacy policies and procedures as well as the completion of activities and assessments to demonstrate knowledge attained through the training. The GDPT must be completed within 45 days of onboarding and annually thereafter for all applicable personnel.

Data Processing Activities

Clario collects and "processes" Data only as required to perform its Services, as defined within the applicable Agreements. For clinical trial Services, this shall include the collection, organization, structuring, and storage of Data as specified within the project protocol and in accordance with the Sponsor's informed consent process for clinical trial participants.

Clario collects the following categories and types of Data for its Services:

- Subject/Patient Data: This category includes Data collected from clinical trial or project participants. As standard, Data collected for these participants is "Pseudonymized Data." Pseudonymized Data means Data that has been obscured so as to no longer directly identify an individual.

  For Clario Services (and as a general practice for clinical studies), Pseudonymized Data means Clario receives a Subject ID, or a unique coded number, that does not directly identify the person participating in the study. Furthermore, Clario does not have access to the re-identification key, which is held exclusively by the clinical site. See specifics in Table 1[1] below.

Table 1:

Clario Service	Subject/Patient Data Processed
 Cardiac	○ personal identification number assigned to data subjects participating in the clinical research or other forms of medical research (e.g. Subject ID, Site ID); ○ age or year of birth; ○ (possibly) date of birth; ○ (possibly) initials; ○ (possibly) ethnicity
 Respiratory	○ personal identification number assigned to data subjects participating in the clinical research or other forms of medical research (e.g., Subject ID, Site ID); ○ age or year of birth; ○ (possibly) date of birth; ○ (possibly) initials; ○ (possibly) ethnicity
 eCOA	○ Personal identification number assigned to data subjects participating in the clinical research or other forms of medical research (e.g., Subject ID, Site ID); ○ information related to Caregivers (for pediatric studies) ○ age or year of birth; ○ (possibly) date of birth; ○ (possibly) initials; ○ (possibly) ethnicity; ○ (possibly) email address or telephone numbers for assessment reminders

1 The purpose of these Tables is to provide a general overview of Data obtained by Clario during its relationships with its sponsors/clients. The information in the Tables is not exhaustive and the exact Data collected is outlined in the applicable sponsor protocol.

 Imaging	○ personal identification number assigned to data subjects participating in the clinical research or other forms of medical research (e.g., Subject ID, Site ID); ○ protected health information in the form of medical imaging and clinical data in support of centralized analysis; ○ age or year of birth; ○ (possibly) date of birth; ○ (possibly) initials; ○ (possibly) description of characteristics of physical features of the body; ○ (possibly) health data including clinical test results, samples and tissues, sample number and clinical visit number; ○ (relevant elements of) medical history
 Precision Motion	○ personal identification number assigned to data subjects participating in the clinical research or other forms of medical research (e.g., Subject ID, Site ID); ○ information related to Caregivers (for pediatric studies); ○ age or year of birth; ○ (possibly) date of birth

- Investigator/Site/CRO Data: Data collected from the individuals who conduct the clinical trial, but who are not employees of the sponsor/client and who are not necessarily contracting directly with Clario (e.g., Investigators/Sites). See specifics outlined in Table 2 below; and

- Client Personnel Data: Data collected from the sponsor/client's personnel. See specifics outlined in Table 2 below.

Table 2:

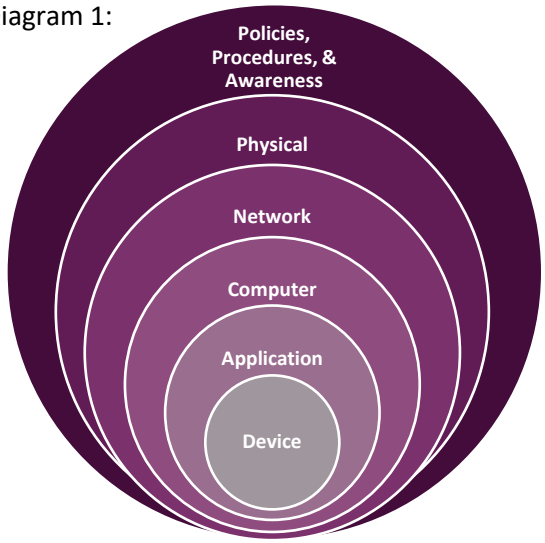
Clario Service	Investigator, Site, and Client Data Processed
All	○ Name (first and last); ○ Log-in data (e.g., username, email address, password, password reset questions); ○ Business communication data (e.g., telephone, fax, mobile phone, e-mail); ○ (possibly) connection data (e.g., logs, IP address, cookies); ○ (possibly) website data (e.g., Cookies, information request

Clario's Security Program

As a provider of clinical trial Software-as-a-Service solutions, Clario understands that customers rely on us to provide solutions that assure system-wide technical and organizational measures to protect their Data, as well as monitor security controls and manage security processes. Privacy and security by design is integrated into all essential business activities and serves to appropriately establish, implement, operate, monitor, review, and maintain security controls for today and the future.

The Clario Security Program has been designed in cumulative layers that build upon one another: from the physical security of Data centers, to the security protections of our hardware and software, to the processes Clario uses to support operational security. This layered protection creates a strong security foundation for Clario.

Diagram 1:



Additionally, Clario's security framework is tailored to align with certain principles prescribed in ISO/IEC 27001:2013. These requirements enable Clario to consistently and effectively manage the confidentiality, integrity and availability of its critical systems and associated Data that support the principles outlined in Clario's Program. This includes the following measures:

- Clario clinical systems are hosted with some of the largest data center providers, including Amazon Web Services (AWS), Azure, and Equinix. Access to these data centers is strictly controlled and monitored by 24/7 onsite security staff, biometric scanning, and video surveillance. AWS, Azure and Equinix maintain multiple certifications for their data centers, including ISO 27001, PCI DSS, Cloud Security Alliance Controls, and SOC report. Formal audits on each of our infrastructure providers are undertaken on an annual basis;
- Clario's defense-in-depth posture includes the use of multiple solutions that, in concert, ensure that our ecosystem meets the appropriate regulatory and security standards. Clario clinical applications are protected by intrusion detection systems / intrusion protection systems (IDS / IPS) network sensors, firewalls, load balancers, web application firewalls, and endpoint security

systems. In combination, these solutions work to protect us from malware, denial-of-service (DOS) events, and unauthorized access;

- Clario's ecosystem of products and services is extensively monitored for security events, potential malware, and anomalous traffic patterns. In tandem, our application performance monitoring and user session activity monitoring platform is distinguished from the monitoring of our infrastructure, facilitating the speedy triage of observed events between operational, infrastructure, and security teams.;
- Clario maintains a patch management standard operating procedure (SOP), and runs all production servers with the latest security patches provided by their operating system vendors. Security patches are applied at regular intervals, and "critical" patches are applied as soon as they have passed regression testing and are available to release;
- Vulnerability scans run continuously across the Clario network, checking for any incidence where systems require patch management. In addition to these vulnerability scans, Clario is contracted with an external company that performs a network-wide penetration test annually;
- User access management is tightly governed across our corporate, clinical, and management systems in accordance with Clario Access Management SOP, and based on the principle of least privilege. Privileged accounts are tightly governed by our Access Management SOP that defines Privileged Access Management and our associated audit procedures;
- Data shall be protected with the necessary levels of encryption for Data in transit and Data at rest, or compensating controls, as required by applicable domestic and international law.
- Quarterly CyberVadis security assessments are performed to provide validated external assurance of Clario's cyber maturity; and
- Annual SOC 2 Type 2 and ISO 9001 certifications are conducted.

For additional information about Clario's Program and how it ensures compliance with GDPR and other data privacy laws and regulations, please review Clario's Privacy and Integrity Policy, located at: https://clario.com/about/legal-and-privacy/privacy-and-integrity-policy/

For general inquiries regarding the Clario Privacy and Security Program Infrastructure, direct your inquiries to Privacy@clario.com, or contact:

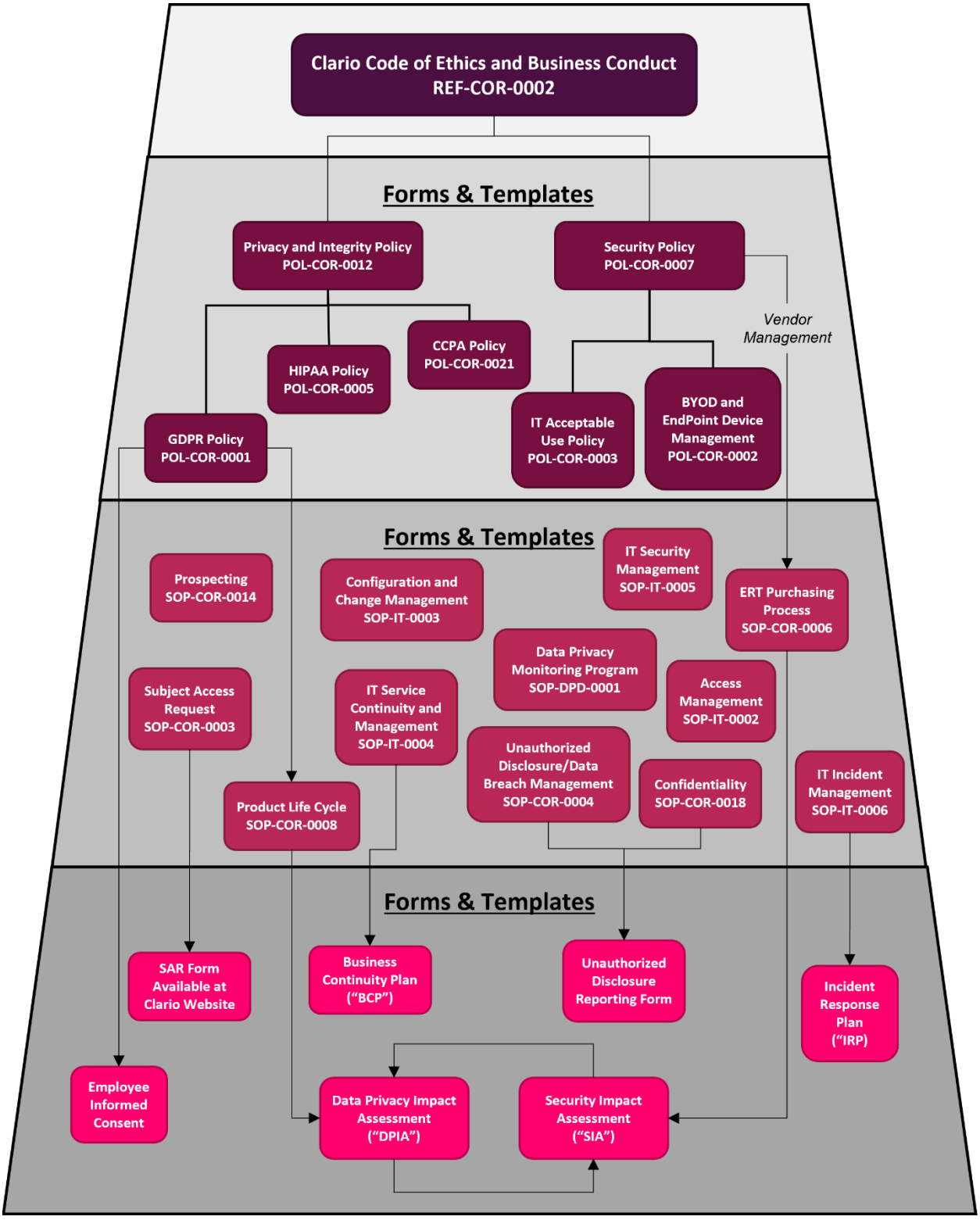
Lauren Misztal, Vice President, Global Privacy & Deputy Compliance Officer, Assistant General Counsel (lauren.misztal@clario.com).

For more detailed information about Clario's technical or organizational security controls, please contact SecOps@clario.com.

Appendix 1 Data Risk Classification Chart

	Data Type	Risk Classification	Data Examples
Critical	Subject/Patient Clinical Trial Data	**Restricted Data** Data that would cause severe harm to individuals and/or Clario if disclosed. Controls strictly limit the ability to use this information, including no ability to extract for operational purposes, unless authorized in writing by Clario Management.	• Subject ID, Gender, Year of Birth, Date of Birth, Weight, Height, Ethnicity, etc. • Protected health information • Clinical trial results Data
High	Clario Personnel Data; Sponsor personnel Data; Site personnel Data; Agent personnel Data; Sales Prospect Data; and Website Visitor Data.	**Private Data** Data that would likely cause harm to individuals and/or Clario if disclosed. Controls limit access but allow information to be extracted and accessed for business operational purposes.	• Personally Identifiable Information, first and last name, email address, address, social security number, information, private telephone number, etc. • Financial Records including banking information for direct deposit • Employee credentials • Business email address and telephone number • CVs • Passwords that can be used to access confidential information
Medium	Clario Confidential Information	**Proprietary Data** Information that Clario, a Client, or a Vendor treats as confidential and integral to its business operations.	• Policies and Procedures • Clario's financial and accounting records • Training materials • Press Statements • Audit reports
Low	Clario Corporate Website	**Public Data** Information that is widely known or readily accessible to the public and provided by Clario.	• Social media profiles (e.g., LinkedIn, Facebook, Twitter, etc.) • Online address directories (e.g., White Pages)

Appendix 2


Clario Code of Ethics and Business Conduct
REF-COR-0002
Forms & Templates
Privacy and Integrity Policy
POL-COR-0012
Security Policy
POL-COR-0007
Vendor Management
CCPA Policy
POL-COR-0021
HIPAA Policy
POL-COR-0005
GDPR Policy
POL-COR-0001
IT Acceptable Use Policy
POL-COR-0003
BYOD and EndPoint Device Management
POL-COR-0002
Forms & Templates
Prospecting
SOP-COR-0014
Configuration and Change Management
SOP-IT-0003
IT Security Management
SOP-IT-0005
ERT Purchasing Process
SOP-COR-0006
Data Privacy Monitoring Program
SOP-DPD-0001
Subject Access Request
SOP-COR-0003
IT Service Continuity and Management
SOP-IT-0004
Access Management
SOP-IT-0002
Unauthorized Disclosure/Data Breach Management
SOP-COR-0004
Confidentiality
SOP-COR-0018
IT Incident Management
SOP-IT-0006
Product Life Cycle
SOP-COR-0008
Forms & Templates
SAR Form Available at Clario Website
Business Continuity Plan ("BCP")
Unauthorized Disclosure Reporting Form
Incident Response Plan ("IRP")
Employee Informed Consent
Data Privacy Impact Assessment ("DPIA")
Security Impact Assessment ("SIA")

Appendix 3

Bioclinica maintains additional policies and procedures relevant to privacy and security

Policies

- POL-GL-QA-005 - Data Integrity Policy
- POL-GL-IT-006 - Encryption Standard
- POL-GL-IT-007 - Endpoint Security Policy
- POL-GL-IT-008 - Password Policy
- FLS-IS-013 – Patient Privacy
- POL-GL-IT-003 - Online Storage & Removable Media Policy
- POL-GL-GO-001 - Business Continuance Plan
- POL-GL-IT-009 - Disaster Recovery Planning
- POL-GL-IT-010 - Network Device Security Policy
- POL-GL-QA-002 - Data Retention (Project and Non-Project)

SOPs

- GL-IT-010 - Network Security Intrusion Defense
- GL-IT-007 - Incident and Request Management
- POL-GL-IT-002 - IT Event Log Privacy Policy
- GL-IT-W012 - Security Auditing Procedure
- GL-QA-027 - Quality Events Management
- GL-QA-030 - CAPA Management
- GL-QA-009 - Critical Issue Communication, Escalation, and Resolution
- GL-QA-012 - Long-Term Storage, Retrieval and Destruction of Study Related Data