ERT Data Privacy and Security Governance Program Overview

Introduction

This paper gives an overview about how eResearchTechnologies, Inc., on behalf of itself and each of its affiliates (collectively "ERT"), complies with data privacy laws and regulations to protect personal data processed and retained by it. ERT is a global company with offices located in, without limitation: the EU, the United Kingdom, USA, India, China and Japan, and has instituted a global data privacy and security governance program (the "Program") to ensure compliance with applicable requirements.

The Program applies to personal data ERT may access, collect, acquire, use, disclose, store, transfer, retain, or dispose of in all aspects of its business worldwide. Specifically, the Program is designed in accordance with applicable data privacy laws and regulations, including without limitation: the European General Data Protection Regulation 2016/679 ("GDPR"), the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), ICH E6 (R2) GCP,, the Declaration of Helsinkithe Act on Protection of Personal Information ("APPI"), the California Consumer Privacy Act ("CCPA"), and the U.S. Food and Drug Administration guidelines (i.e. 21 CFR Part 11).

Merger with BioClinca: While ERT and BioClinica have sought to harmonize the Program infrastructure, harmonization shall continue as an ongoing effort, and for the time being, there may be controlled documents, including policies and procedures, distinct to each entity. The data privacy team, and functional stakeholders, in conjunction with quality management shall continue to lead the effort to ensure the quality of the Program will be 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:

- ERT communicates to its employees the cultural importance, and awareness, of meeting statutory and regulatory data privacy and security requirements. ERT is a data controller registered with the Information Commissioner's Office 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 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.
- ERT has written policies and procedures that address privacy and security obligations as outlined in **Appendix 2 and 3**. ERT maintains privacy policies in line with applicable data privacy laws and regulations, in conformance with EU standard contractual clauses (SCCs) or other applicable compliant data transfer mechanisms, e.g. informed consent. ERT is committed to observing and implementing "best practices" around data privacy protection requirements for its Activities

(defined below);

- ERT has established data privacy and security training, and educational programs that promote its privacy and security principles supported by ERT's comprehensive Global Data Privacy Training ("GDPT") that every ERT employee participates in;
- ERT performs on-going monitoring, and review, of the Program. ERT is audited for compliance with data protection laws and regulations, with particular emphasis on administrative, physical,
- and technical security controls; and
- ERT makes available Program resources. ERT has a dedicated data privacy and IT security team(s), who work to ensure ERT is compliant with applicable data privacy laws and regulations across its organization.

Program Risk Assessment

ERT's Program takes a risk-based approach as to how risk is assessed for its business activities, operations, and services (collectively "Activities"). Such Activities account for different data types, the data volume, (that have been classified in accordance with ERT's Data Risk Classification Chart ("Chart") provided below as Appendix 1), assessing (and weighing) the probability of identifying an individual with certainty, whether traceability aspects exist, and potential harm (e.g. financial or reputational harm) that may be caused to an individual should a privacy incident occur. The foregoing criteria aids ERT in determining the overall severity of a privacy incident and associated liability with such incidents.

In connection with ERT's Activities, the following charts outline examples of the data types ERT collects and stores:

Client/Sponsor/CRO Personnel Data

Data obtained during the course of ERT's Activities can be further divided into the following sub-groups:

- Subject/Patient Data - Data collected from clinical trial or project participants;
- 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 ERT, e.g. Investigators/Sites; and
- Client Personnel Data, Data collected from the sponsor/client's personnel.

As standard, Data collected from subjects (or patients) in support of ERT's Activities will generally be pseudonymized. The data collected from each of these sub-groups (above) varies depending on the given ERT product line, as shown in the tables below. The lists in the tables are not exhaustive and the exact data collected is outlined in the applicable sponsor protocol; however, the lists provide a general overview of Data obtained by ERT during its relationships with its sponsors/clients. For further information regarding risk classifications, please review the company's Chart (Appendix 1).

Cardiac Safety	
Subject/Patient	E.g. Subject ID, Gender, Ethnicity, Age, YOB, or DOB (if applicable), and Health Data. (Note: Could be more depending on

	the applicable protocol)
Investigator/Site/CRO Personnel	E.g. First and Last Name, Business Telephone (landline and mobile number), Email, and Business Address.
Sponsor/Client Personnel	E.g. First and Last Name, Business Telephone (landline and mobile number), Email, and Business Address.

Respiratory	
Subject/Patient	E.g. Subject ID, Gender, Ethnicity, Age, YOB, or DOB (if applicable), and Health Data. (Note: Could be more depending on the applicable protocol)
Investigator/Site/CRO Personnel	E.g. First and Last Name, Business Telephone (landline and mobile number), Email, and Business Address.
Sponsor/Client Personnel	E.g. First and Last Name, Business Telephone (landline and mobile number), Email, and Business Address.

eCOA / Digital Patient	
Subject/Patient	E.g. Subject ID, Gender, Initials (ad hoc), and Age, YOB, or DOB (if applicable). (Note: could be more depending on the protocol). • BYOD - Telephone (mobile) and Email • Virtual Visits - First name, Last name, personal email or telephone number in order to register the user's account. • Multimedia enhancements - includes: Voice recordings of the assessments, which will be stored on ERT's IMS platform for the purpose of quality assurance in regards to the site personnel. Video recordings may also be used for the same purposes. Images may also be captured for additional assessment data.

Investigator/Site/CRO Personnel	E.g. First and Last Name, Business Telephone (landline and mobile number), Email, and Business Address.
Sponsor/Client Personnel	E.g. First and Last Name, Business Telephone (landline and mobile number), Email, and Business Address.

Medical Imaging	
Subject/Patient	E.g. Subject ID, Gender, images (Health Data), etc. (Note: could be more depending on protocol)
Investigator/Site/CRO Personnel	E.g. First and Last Name, Business Telephone (landline and mobile number), Email, and Business Address.
Sponsor/Client Personnel	E.g. First and Last Name, Business Telephone (landline and mobile number), Email, and Business Address.

Trial Oversight	
Subject/Patient	No new data collection. Data, if used, is in support of ODS reporting or Data Insights, are pulled from the applicable source data system.
Investigator/Site/CRO Personnel	No new data collection. Data if used is in support of ODS reporting or Data Insights, are pulled from the applicable source data system.
Sponsor/Client Personnel	No new data collection. Data if used is in support of ODS reporting or Data Insights, are pulled from the applicable source data system.

Wearables and Digital Biomarkers	
Subject/Patient	E.g. Subject ID, Gender, Movement data etc. (Note: could be more depending on the protocol)
Investigator/Site/CRO Personnel	E.g. First and Last Name, Business Telephone (landline and mobile number), Email, and Business Address.
Sponsor/Client Personnel	E.g. First and Last Name, Business Telephone (landline and mobile number), Email, and Business Address.

Drug Safety Solutions – Pharmacovigilance	
Subject/Patient	E.g. Subject ID, Gender, etc. (Note: could be more depending on the protocol) Protected health information in support of centralized analysis
Investigator/Site/CRO Personnel	E.g. First and Last Name, Business Telephone (landline and mobile number), Email, and Business Address.
Sponsor/Client Personnel	E.g. First and Last Name, Business Telephone (landline and mobile number), Email, and Business Address.

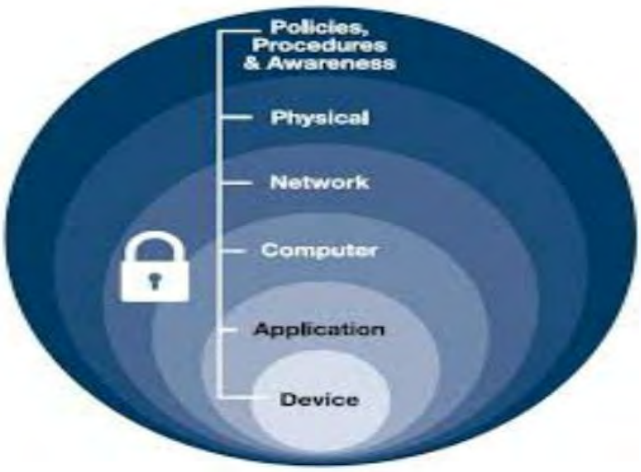
Vendor/Supplier	
Vendor Personnel	First and Last Name, Business Telephone (landline and mobile number), Email, and Business Address.

ERT's Security Program

As a provider of clinical trial SaaS solutions and services, ERT understands that customers rely on us to provide solutions that assure security, to protect clinical data and Personally Identifiable Information (PII), and to monitor security controls and manage security processes. Security management is integrated into all essential business activities and serves as ERT's mechanism to appropriately establish, implement, operate, monitor, review, maintain security controls that are required today, and add or update security controls as regulatory and compliance entities mandate.

The Security Program also provides assurances as documented and audited in ERT's Security Management Standard Operating Procedure(s). Systems are implemented using information security industry best practices and based on a risk-based approach. The ERT Security Program consists of a set of policies and procedures for systematically managing personal data and related risks, including:

- ERT designed the security of its infrastructure in 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 ERT uses to support operational security. This layered protection creates a strong security foundation for ERT. See diagram below:



- Security Awareness Training - ERT staff are required to undergo security awareness training, within 30 days of new-hire on-boarding and at least annually thereafter.
- Data Privacy and Security-by-Design assure privacy and security are built into ERT products and services.
- Implementation, maintenance and monitoring of security procedures and associated security controls.
- Building, operating and monitoring systems to protect against data theft or unauthorized access.
- Building, operating and monitoring infrastructure to secure computer systems, networks and database environments.
- Ensuring necessary level of encryption for data in transit and data at rest as required by applicable

domestic and international law.

- Applying critical software patches to servers, networks, applications and databases.
- Conducting both internal and 3rd party vulnerability scans and penetration tests.
- Identifying and remediating security vulnerabilities without unreasonable delay.
- Implement access management controls for Personal Information collected for product lines such as Virtual Visits by ensuring that additional data collection will be stored in the cloud with AWS encryption, store information in a separate database with limited and controlled access and separate- out PII collected (for user account access) from the clinical trial data that are collected.

For further information regarding ERT Security Operating Procedures (SOPs) please review the Diagram under Appendix 2 and 3.

ERT' Security and Risk Management organization manages the Security Program to:

- Where feasible, align with customer data security requirements and contractual data security and privacy obligations;
- Align with ERT's Data Privacy legal and privacy obligations to ensure applicable administrative, physical and technical controls are satisfied;
- Work to deliver a consistent, documented security management process;
- Work to establish formal procedures to verify and report on security controls;
- Provide a security framework to account for applicable regulatory requirements; and
- Sustain a security program aligned to evolving regulatory and compliance mandates and ERT strategic priorities.

ERT's security framework is tailored to align with certain principles prescribed in ISO/IEC 27001:2013. These requirements enable ERT to consistently and effectively manage the confidentiality, integrity and availability of its critical systems and associated data that support the principles outlined in ERT's Program. For more detailed information please contact Security@ert.com.

Data Transfers

ERT shall ensure Data Transfers (including making Data available remotely) outside the European Economic Area, Switzerland, the United Kingdom, and other applicable global regions are performed in compliance with Program requirements, applicable data privacy and security laws and regulations, and in conformance with the EU standard contractual clauses or other applicable compliant data transfer mechanisms, e.g. informed consent. Such transfers are carried out only to perform the applicable services required of ERT or its agents (where applicable) and where data subjects have consented to the transfers, where required.

Data Centers and Processing

ERT's Activities takes place globally and depending on the service line, such Activities may occur at one of the company's affiliate locations located at:

- eResearch Technology, Inc. Headquarters 1818 Market St, Suite 1000 Philadelphia, PA 19103
- US Biomedical Systems India Pvt. Ltd. 452A Bharathy Street 605001 Pondicherry, India

- ERT Inc. 2F, 2-13-13 Nihonbashi Kayabacho, Chuo-ku, Tokyo 103-0025, Japan
- PHT Corporation SARL Chemin Louis-Hubert 2
- eResearchTechnology GmbH Sieboldstrasse 3, 97230 Estenfeld, Germany
- eResearch Technology Limited Peterborough Business Park Lynch Wood Peterborough PE2 6FZ United Kingdom
- Biomedical Systems B.V.B.A Waversesteenweg 1945 Chaussée de Wavre 1160 Brussels, Belgium
- APDM, Inc., 2828 S. Corbett Avenue, Suite 135, Portland, OR 97201
- iCardiac Technologies LLC, 3750 Monroe Ave., Suite 600, Pittsford, NY 15436
- Exco InTouch Limited, Unit 6 Wheatcroft Business Park Landmere Lane, Edwalton, United Kingdom
- 211 Carnegie Center Drive Princeton, NJ 08540
- 7707 Gateway Boulevard, 3rd floor Newark, CA 94560
- Bioclinica GmbH Landsberger Strasse 290 80687 Munich, Germany
- 16 Rue de Montbrilliant "Buroparc Rive Gauche" Bâtiment T3 et T4 69003 FR 35 439 429 440 Lyon, France
- London, England 72 Hammersmith Road, 6th Floor W14 8UD, London, UK
- 11F No.3, Lane 227, Dong Yu Road, Pudong New Area Shanghai, China 200126
- MAO Building 7F, 3-12-4 Kyobashi, Chuo-ku, Tokyo 104-0031, Japan
- Bangalore, India
- #120P-122P, Belagola Industrial Area K.R.S. Road, Metagalli, Mysore – 570016, India

Subcontractors

ERT carefully selects its third-party vendors in accordance with Program requirements and its procurement process. Where necessary, data privacy impact assessments will be performed ensuring that such vendors are held to standards that are as restrictive as those under ERT's sponsor/client service agreements or data processing agreements (collectively "Agreement"). A list of vendors are provided to ERT sponsors in the applicable Agreement or upon the written request of the sponsor, in accordance with applicable Agreement requirements.

Unauthorized Disclosures/Privacy Incidents

ERT shall ensure that if any ERT personnel and agents (where applicable) become aware of any potential or identified Unauthorized Disclosure, Data Breach, or Security Incident, then such incidents are reported timely, in accordance with Unauthorized Disclosure/Data Breach Management and Corrective and Preventive Actions (CAPA), or other controlled procedural documents and forms governing IT Security Incident Management.

Subject Access Request

ERT has implemented policies and procedures supporting Subject Access Requests, which covers the processes required to comply with individuals' data privacy rights and to ensure compliance with the applicable data protection laws and regulations.

An individual may make a subject access request ("SAR"), in writing, at any time, to find out more about the personal data ERT holds about them. Such requests should be submitted to privacy@ert.com or

dataprivacy@bioclinica.com. ERT will respond to SARs within 30 days of receipt, unless additional time is warranted due to the complexity of the request, at which point, the individual will be informed of the need for an extension.

The SAR form is available at:

- https://www.ert.com/privacy-policy/
- https://www.bioclinica.com/privacy-policy

ERT Employee Informed Consent and Privacy Notice

As part of ERT's on-going initiative to increase its data privacy and security posture and ensure compliance with its Program requirements and applicable data protection laws and regulations, the company has implemented an employee informed consent process or data privacy notice, intended to create greater transparency around how the company processes employees' personal data to support its Activities.

ERT Training

ERT shall ensure that its personnel complete ERT's Global Data Privacy Training (GDPT) within 45 days of new-hire on-boarding and annually thereafter. The GDPT is designed to introduce personnel to Program requirements and applicable data privacy laws and regulations. ERT shall ensure that its agents, who are required to use personal data to fulfill Activities on ERT's behalf, complete comparable data privacy and security training (to the GDPT) before any services begin.

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

For additional information about Bioclinica's, an ERT company, Program and how it ensures compliance with GDPR and other data privacy laws and regulations, please review ERT's Privacy and Integrity Policy, located at: https://www.bioclinica.com/privacy-policyInquiries

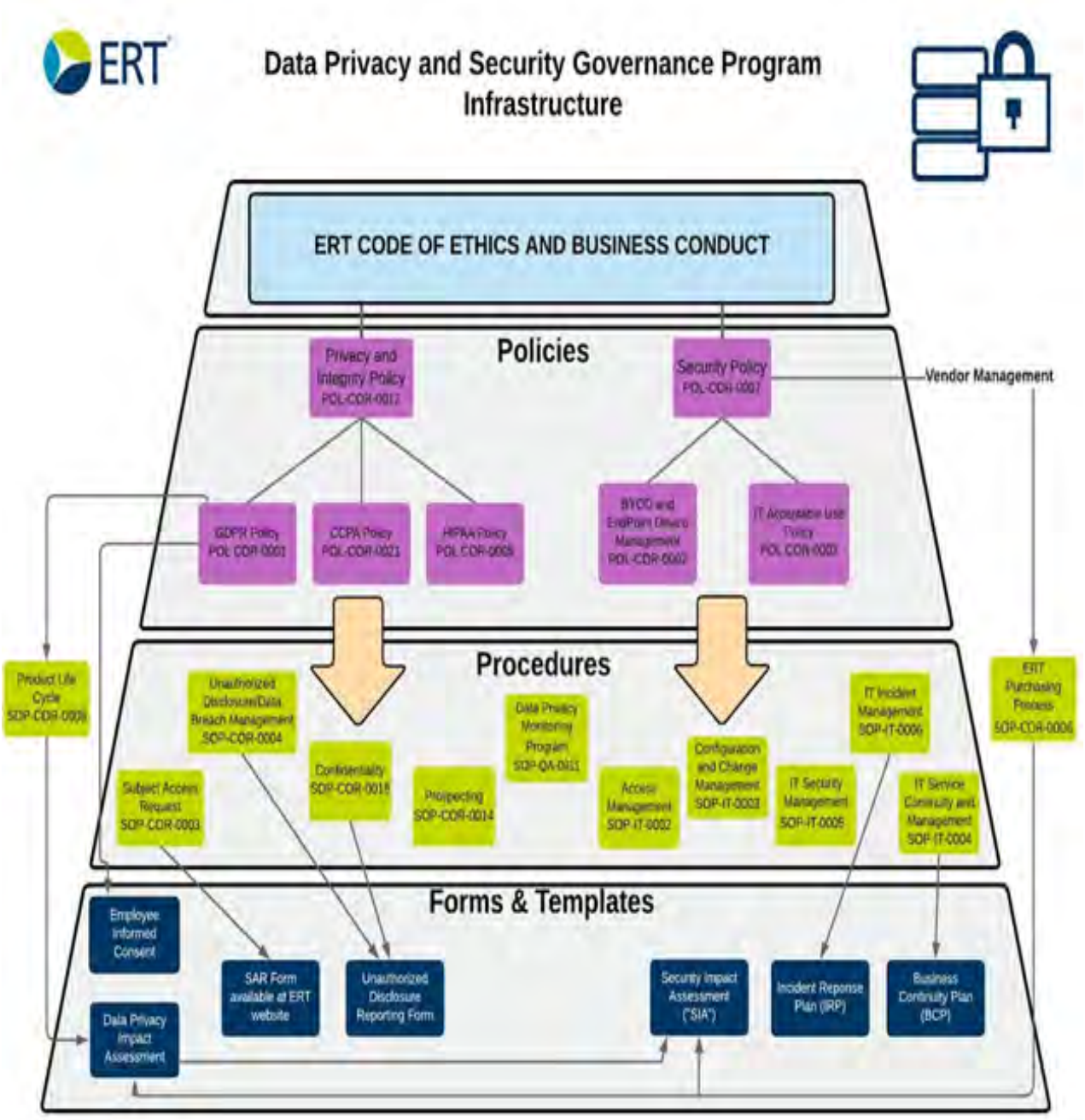
For general inquiries regarding the ERT Privacy and Security Program Infrastructure, direct your inquiries to privacy@ert.com, or contact these people for addition questions: Veronica Contreras, Data Privacy Officer, Counsel: privacy@ert.com

For general inquiries regarding Bioclinica, an ERT company, Privacy and Security Program Infrastructure, direct inquiries to: dataprivacy@bioclinica.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 ERT if disclosed. Controls strictly limit the ability to use this information, including no ability to extract for operational purposes, unless authorized in writing by ERT Management. Includes Subject/Patient Clinical Trial Data.	• Subject ID, Gender, Year of Birth, Date of Birth, Weight, Height, Ethnicity, etc. • Protected health information • Clinical trial results data
High	ERT Personnel Data; Sponsor personnel Data; Site personnel Data, CRO personnel Data, Agent personnel Data, Sales Prospect Data, and Website Visitor Data.	**Private Data** Data that would likely cause harm to individuals and/or ERT 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	ERT Confidential Information	**Proprietary Data** Information that ERT, a Client, or a Vendor treats as confidential and integral to its business operations.	• Policies and Procedures • ERT's financial and accounting records • Training materials • Press Statements • Audit reports
Low	ERT Corporate Website	**Public Data** Information that is widely known or readily accessible to the public and provided by ERT.	• Social media profiles (e.g., LinkedIn, Facebook, Twitter, etc.) • Online address directories (e.g., White Pages)

Appendix 2


Data Privacy and Security Governance Program Infrastructure
ERT CODE OF ETHICS AND BUSINESS CONDUCT
Policies
Privacy and Integrity Policy POL-CDR-0012
Security Policy POL-CDR-0007
Vendor Management
GDPR Policy POL CDR-0001
CCPA Policy POL-CDR-0021
HIPAA Policy POL CDR-0005
BYOD and EndPoint Device Management POL-CDR-0002
IT Acceptable Use Policy POL CDR-0003
Procedures
Product Life Cycle SDP-CDR-0009
Unauthorized Disclosure/Data Breach Management SOP-CDR-0004
Data Privacy Monitoring Program SOP-QA-0011
IT Incident Management SOP-IT-0006
ERT Purchasing Process SOP-CDR-0006
Subject Access Request SOP-CDR-0003
Confidentiality SOP-CDR-0015
Prolpecting SOP-CDR-0014
Access Management SOP-IT-0002
Configuration and Change Management SOP-IT-0003
IT Security Management SOP-IT-0005
IT Service Continuity and Management SOP-IT-0004
Forms & Templates
Employee Informed Consent
SAR Form available at ERT website
Unauthorized Disclosure Reporting Form
Security Impact Assessment ("SIA")
Incident Reponse Plan (IRP)
Business Continuity Plan (BCP)
Data Privacy Impact Assessment

Appendix 3

Bioclinica, an ERT Company, Data Privacy and Security Governance Program Infrastructure

Code of Business Ethics

Policies

- POL-GL-QA-001 - Data Privacy Policy
- 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 Dat

Forms / Templates

- Data Breach Form
- QER/CAPA Form