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, USA, 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, world regulatory authorities, the Helsinki accords, applicable to research with human subjects, the EU-US and Swiss-US Privacy Shield Frameworks, the Act on Protection of Personal Information ("APPI"), and the U.S. Food and Drug Administration guidelines (i.e. 21 CFR Part 11).

Program Requirements

The Program is built around a company culture that respects an individual's right to privacy and has been embedded into 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 UK and the Bavarian Supervisory Authority ("BayLDA") in Germany;

- ERT has written policies and procedures that address privacy and security obligations. ERT maintains privacy policies in line with applicable data privacy laws and regulations, supported by the EU Privacy Shield and Swiss Privacy Shield Principles and associated FAQs, and is self-certified with the U.S. Department of Commerce. This voluntary membership demonstrates ERT's commitment to observing "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;

- 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 had a dedicated team comprising of its Data Privacy Officer, Director of Security and Risk Management and other data privacy and security protection specialists 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 and reputation harm) that may be caused to an individual should a privacy incident occur.

Patient clinical trial data or "Subject Data" has been classified as "Restricted Data," as identified in the Chart. Subject Data is collected, in accordance with the applicable study protocol and applicable data protection laws and regulations. Depending on the product line and applicable data collection requirements under the study protocol, data will either be pseudonymized or anonymized. Although ERT classifies Subject Data as Restricted Data, as standard, ERT does not collect personally identifiable information ("PII") in support of its clinical trial services. Rather, clinical trial services use demographic data, such as first initial, last initial, age (in some older studies this may include date of birth), gender, subject ID, and Site ID. Other data types include, business contact information of the Principal Investigator, site supporting staff personnel data, Sponsor personnel data, and vendor personnel data, which include: first name, last name, professional title, business email address, and business telephone number (collectively "Business Contact Information").

Because Restricted Data does not contain PII and no traceability aspects exist due to ERT not holding access to a re-identification key, ERT has classified its risk exposure (for Restricted Data) as lower risk. Separately, while Business Contact Information does identify individuals with certainty and contains traceability aspects, most information is available in the public sector; and therefore, if a privacy incident would occur the impact to affected individuals is likely lower risk given the availability of information in the public domain. As such, ERT has classified Business Contact Information as lower risk.

For further information regarding risk classifications, please review the company's Chart (Appendix 1).

ERT's Security Program

As a leading 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. The security management system 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' Security Management Standard Operating Procedure(s). The system is implemented using information security industry best practices and based on a business risk approach. The ERT Security Program consists of a set of policies and procedures for systematically managing ERT's sensitive 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.

- Security Awareness Training - ERT staff are required to undergo security awareness training, including without limitation: Security Awareness training within 90 days of new-hire on-boarding and annually thereafter.
- Design and development practices that assures security is 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
- 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

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

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

- 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
- Deliver a consistent, documented security management process
- Establish formal procedures to verify and report on security controls
- Provide a security framework to account for all regulatory requirements
- Sustain a continuous improving 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 all the critical systems and associated data that support the principles outlined in ERT's Data Privacy and Security Governance Program.

For more detailed information please contact ERT's Director of Security (ISO) and Risk Management at Security@ert.com

---

Data Transfers:

ERT supports many global clinical trials for its customers; and therefore, ensures that international data transfers that occur outside the European Economic Area and Switzerland adhere to Privacy Shield principles or the EU standard contractual clauses, where required. Such transfers are carried out only to perform the applicable Activities required.

Data Centers and Processing:

GDPR, currently, does not require that clinical trials utilize data centers in multiple geographic locations if or when study sites span multiple continents and countries. ERT supports many studies that were active after GDPR took effect and the company has not had an issue with utilizing data centers in multiple geographic locations to comply with GDPR.

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. KK 1 Chome-19-14 Ginza, Chūō-ku Tōkyō-to 104-0061, Japan 4. 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 UK
- Biomedical Systems B.V.B.A Waversesteenweg 1945 Chaussée de Wavre 1160 Brussels, Belgium

Subcontractors:

ERT's third-party vendors are carefully selected by ERT, 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 suspected or actual unauthorized disclosures (or privacy incidents) it becomes aware of are reported timely, in accordance with applicable contractual requirements, Program requirements, and applicable data privacy and security laws and regulations.

Subject Access Request

ERT has implemented SOP-123 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. 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/.

ERT Employee Informed Consent

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 implemented an employee informed consent process intended to create greater transparency around how the company processes employees' personal data to support its Activities.

ERT Training:

ERT staff are required to undergo compliance training, including without limitation: GXP, GDPR, HIPAA and Security training within 90 days of new-hire on-boarding and annually thereafter. Access to Subject Data is highly-restricted on an "as-needed" basis.

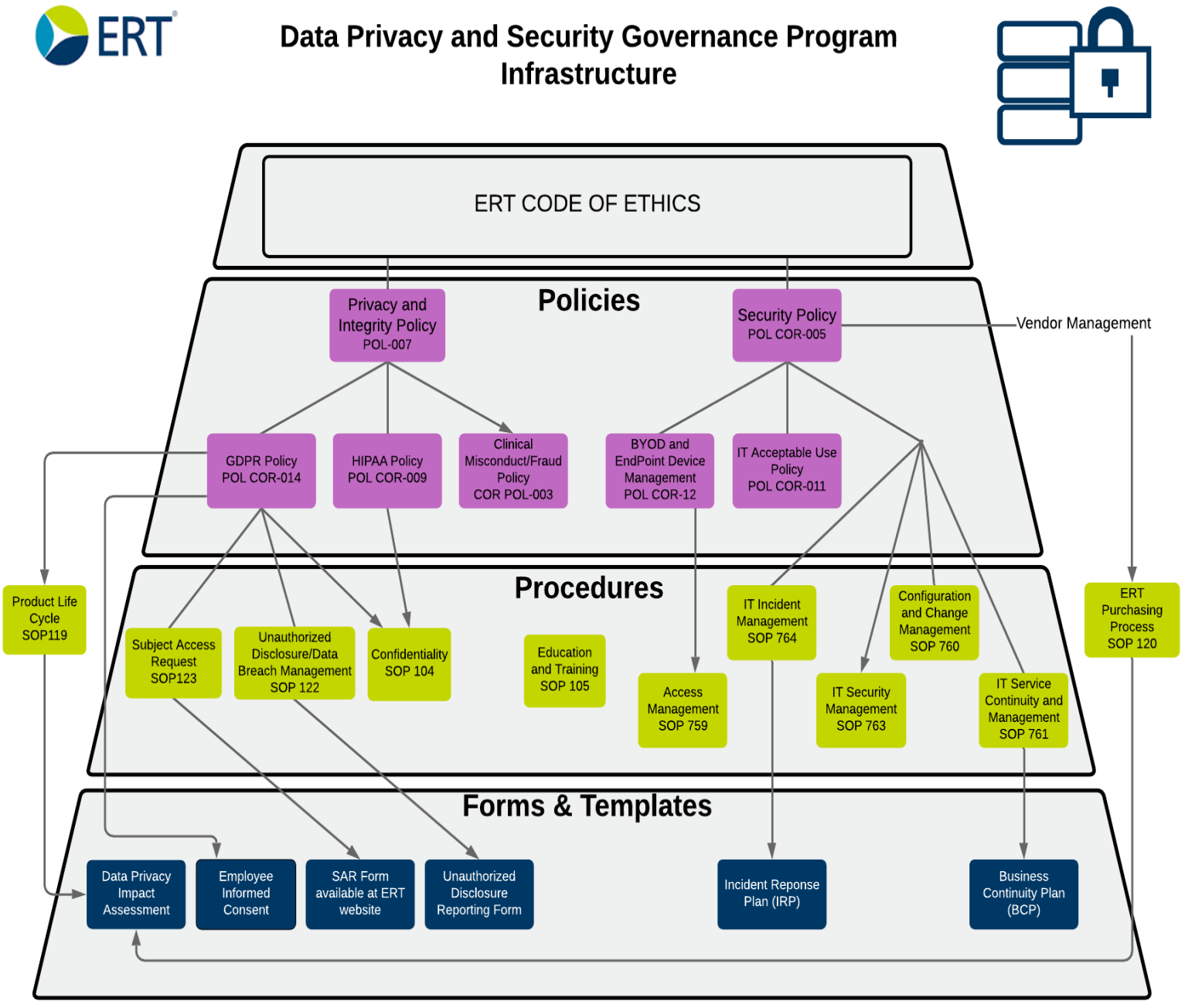
For additional information about ERT's Program and how it ensures compliance with GDPR and other data privacy laws and regulations, please review ERT's Privacy and Integrity Policy, located at: https://www.ert.com/privacy-policy/

Appendix 1

ERT's Data Risk Classification Chart:

LEVEL	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	• Social Security Numbers in association with protected health information or personally identifiable information. • Certain individually identifiable medical records and genetic information • Specific contractual or customer obligations • Research information classified as highly restricted use
High	ERT Employee Data; Client personnel Data; and Vendor personnel Data	**Private Data** - Data that would likely cause harm to individuals and/or ERT if disclosed. Controls limitaccess, but allow information to be extracted and accessed for business operational purposes.	• Protected Health Information • Personally Identifiable Information, including Social Security Number and National ID • Financial Records, including banking information for direct deposit • Employee credentials; • Business email address and telephone number • CV's • Passwords that can be used to access confidential information.
Medium	ERT Confidential Information	**Proprietary Data** – Data which would not cause harm if disclosed, but ERT has chosen to keep confidential. Controls allow access with little technical barriers.	• Policies and Procedures • ERT's financial and accounting records • Training materials • Press Statements • Audit reports
Low	ERT Corporate Website	**Public Data** – Data that readily accessible to the general public and not received, or disclosed, 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
Policies
Privacy and Integrity Policy POL-007
Security Policy POL COR-005
Vendor Management
GDPR Policy POL COR-014
HIPAA Policy POL COR-009
Clinical Misconduct/Fraud Policy COR POL-003
BYOD and EndPoint Device Management POL COR-12
IT Acceptable Use Policy POL COR-011
Procedures
Product Life Cycle SOP119
Subject Access Request SOP123
Unauthorized Disclosure/Data Breach Management SOP 122
Confidentiality SOP 104
Education and Training SOP 105
Access Management SOP 759
IT Incident Management SOP 764
Configuration and Change Management SOP 760
IT Security Management SOP 763
IT Service Continuity and Management SOP 761
ERT Purchasing Process SOP 120
Forms & Templates
Data Privacy Impact Assessment
Employee Informed Consent
SAR Form available at ERT website
Unauthorized Disclosure Reporting Form
Incident Reponse Plan (IRP)
Business Continuity Plan (BCP)