1.0 OVERVIEW

The purpose of this Privacy and Integrity Policy ("Policy") is to define, and outline, the company's data privacy and security governance program ("Program") requirements that support Program requirements and this Policy. Such practices enable eResearchTechnology, Inc. (and each of its subsidiaries and affiliates, collectively "ERT") to appropriately manage its privacy and security risks.

ERT is committed to this Policy in protecting the privacy, integrity, and security of those who entrust us with their personal, clinical, protected health information, or individually identifiable health information ("Data," as further defined below) that ERT may access, collect, acquire, use, disclose, store, transfer, retain, or dispose of in all aspects of its business worldwide.

This Policy provides ERT management guidance for maintaining compliance with company data privacy and security standards, including the ERT General Data Protection Regulation (GDPR) Policy, the ERT Health Insurance Portability and Accountability Act Policy, applicable laws and regulations, such as: the General Data Protection Regulation ("GDPR"), the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), ICH E6 GCP, world regulatory authorities, the Helsinki accords, applicable to research with human subjects, and the EU-US and Swiss-US Privacy Shield Frameworks.

The following authorities, without limitation, are applicable to ERT's overall Program compliance and compliance with this Policy:

- The UK Medicines and Healthcare products Regulatory Agency ("MHRA");
- The US Food and Drug Administration ("FDA");
- The European Medicines Agency ("EMA");
- The US Department of Health and Human Services ("DHHS");
- The UK Information Commissioner's Office ("ICO");
- The International Conference on Harmonization - Good Clinical Practice ("ICH-GCP R2");
- The International Organization for Standardization ("ISO");
- The China Food and Drug Administration ("CFDA"); and
- The Pharmaceuticals and Medical Devices Agency ("PMDA")

This Policy applies to all Personnel (as defined below) and any other Agent (as defined below) who may, during their business relationship with ERT, access, collect, acquire, use, disclose, store, transfer, retain, or dispose of Data (collectively "Use," "Used," or "Using").

2.0 RELATED DOCUMENTS

POL COR-005	Security Policy
POL COR-009	ERT HIPAA Policy
POL COR-011	Acceptable Use Policy
POL COR-014	ERT General Data Protection Regulation (GDPR) Policy
SOP 122	Data Privacy and Security Breach Process
SOP 119	Product Life Cycle
SOP 123	Subject Access Request
SOP 1300	Development Life Cycle

External References

FDA web site	21 CFR Part 11: Electronic Records; Electronic Signatures, August 1997

www.ico.org.uk	EU General Data Protection Regulation (GDPR) 2016/679
http://ec.europa.eu/internal_market/e-commerce/directive/index_en.htm	Directive 2000/31/EC on electronic commerce
EurLex web site	EU GCP Directive 2005/28/EC, April 2005
FDA web site	Guidance for Industry - 21 CFR Part 11; Electronic Records; Electronic Signatures -- SCOPE AND APPLICATION (August 2003)
FDA web site	Guidance for Industry: Computerized Systems Used In Clinical Investigations, May 2007
ICH web site	Guidance for Industry: E6 Good Clinical Practice, April 1996
US Department of Commerce website.	ERT Privacy Shield Certification
Electronic Code of Federal Regulations (e-CFR) web site	HIPAA Security and Privacy Rule, 45 CFR Part 164
US Dept. of Commerce web site. http://www.export.gov	EU-US and Swiss-US Privacy Shield Frameworks A Guide to Self-Certification. Including the full text of the official declaration of the Privacy Shield Privacy Principles, as announced on July 12, 2016
http://www.bbb.org/EUprivacy-shield/)	US Better Business Bureau

3.0 DEFINITIONS AND ABBREVIATIONS

Term	Definition
Agent	A third-party, including consultants, that may access, collect, acquire, use, disclose, store, transfer, retain, or dispose of Data (and Sensitive Personal Data, where applicable) on behalf of, and under the instructions of ERT in order to carry out ERT business activities or operations on the company's behalf.
Data	Any personal, clinical, protected health information, individually identifiable health information, relating to an identified, or identifiable natural person, i.e., a Data Subject; a "Data Subject" is one who can be identified, directly or indirectly, in particular by reference to an identifier, such as: a name, telephone number, email address, address information, social security number, date of birth, IP address, an identification number, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of a data subject. Data may also include "Sensitive Personal Data" that reveals a data subject's race, ethnic origin, political opinions, criminal convictions and offences, biometric information, genetics, religious or philosophical beliefs, or trade union membership, or that concerns an individual's health or sex life. Data will be treated as Sensitive Personal Data where it is received from an Agent that treats and identifies it as sensitive.

	Data does not include information, so long as it is encoded, anonymized, or de-identified.
Data Breach	Defined as the acquisition, access, use, or disclosure of unsecured Data, in a manner not permitted under applicable data privacy and security laws and regulations, including GDPR and HIPAA, which poses a significant financial, reputational, or other harm to the affected individual.
Data Integrity	Accuracy and consistency pertaining to the systems and processes for Data capture, correction, maintenance, transmission, and retention.
Data Quality	Condition of the Data, i.e. the quality is acceptable for the intended use.
Data Security	Degree to which Data are protected from the risk of accidental or malicious alteration or destruction and from unauthorized access, use, or disclosure, in accordance with the Data Risk Classification Chart, ("Chart"), attached hereto as Exhibit 1, and ERT's POL COR-005 Security Policy
eCommerce	Use of electronic systems and networks by consumers, sellers and other entities to conduct business activities.
ERT Systems and Processes	Devices and applications that capture trial Data, transmission technologies, software applications for storage and review of Data, registrations for users, processes for identification, qualification and training of users, including actions on electronic (and related paper records) that rely on security and authenticity protections provided by ERT for conducting clinical investigations, diagnostic evaluations, and other services delivered to clients.
Patient	Person under a physician's care for a particular disease or condition. NOTE: A subject in a clinical trial is not necessarily a patient, but a patient in a clinical trial is a subject. See also subject, Although, often used interchangeably as a synonym for subject, a healthy volunteer is not a patient.
Personnel	Means ERT current, past and prospective employees, trainees, temporary workers, contractors, or applicants.
Privacy Protection	The appropriate use of Personal Information, or Sensitive Personal Data, under specific circumstances. What is appropriate will depend on context, law, and the individual's expectations.
Security Incident	An attempted or successful unauthorized access, use, disclosure, modification, or destruction of Data or interference with system operations in an information system.
Sponsor	An individual, company, institution or organization which takes responsibility for the initiation, management, or financing of a clinical trial.
Subject	An individual who participates in a clinical trial, either as recipient of the investigational product(s) or as a control.

4.0 PROCEDURE

4.1 ROLES AND RESPONSIBILITIES

The following table lists participant roles and responsibilities required by this process:

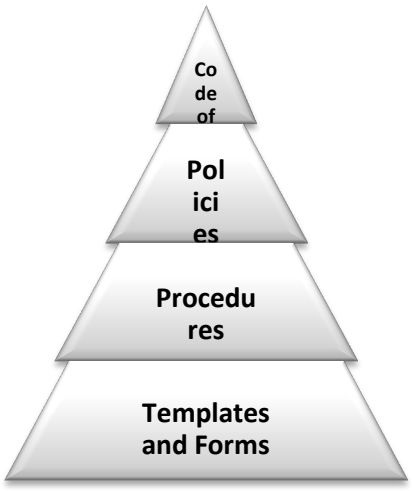
Role	Responsibilities

Data Protection/Privacy Officer(s) ("DPO(s)")/Director of Security and Risk Management ("Security Director")	The DPO(s), and Security Director are responsible for the development, implementation, enforcement, and monitoring of Program requirements to ensure ERT complies with applicable US, EU and regional privacy and security laws and regulations and conforms to industry best practices for clinical trial, healthcare and privacy.

4.2 PROGRAM REQUIREMENTS

ERT shall implement a Program that identifies key compliance elements, and corresponding, compliance documentation.

This Policy, and applicable Program documentation, shall ensure compliance with ERT's Code of Ethics standards and Program hierarchy, as further identified in the chart below.

Privacy	Program Infrastructure	Security
Code of Ethics		**Code of Ethics**
Privacy and Integrity Policy		**Security Policy**
GDPR Policy		**Acceptable Use Policy**
HIPAA Policy		**BYOD and Device Management**
Data Privacy and Security Breach Process		**Incident Management**
Subject Access Request		**Change Management**
Prospecting		**Development Life Cycle**
Product Life Cycle		**Access Management**
Data Privacy Impact Assessment		**Security Management**
Data Processing Templates		**Security Impact Assessment**
Data Privacy Matrix		**Incident Response Plan**

Program supporting policies and procedures shall comprise of this Policy, ERT's General Data Protection Regulation Policy ("GDPR"), the ERT Health Insurance Portability and Accountability Act ("HIPAA") Policy, ERT's Security Policy, ERT's Acceptable Use Policy, and related ERT Standard Operating Procedures, such as: the Data Privacy and Security Breach Process, Subject Access Requests, Product Life Cycle, and Development Life Cycle.

Additional supporting Program documentation shall include, without limitation: a data privacy compliance matrix; master service agreement templates, data processing agreement templates and corresponding security exhibit, employment informed consents, a breach notification form and corresponding tracker, training materials, a data protection statement, and any other applicable supporting documentation necessary for overall Program compliance.

All applicable Program documentation shall align with the Policy principles herein and shall meet ERT's risk-based data privacy categorizations, as further documented in the Chart.

4.3 DATA PRIVACY RISK CATEGORIZATION

ERT shall establish a data privacy risk categorization that establishes Data types and associated risk rankings, as further outlined in the Chart.

Data security controls shall be assigned, in accordance with the Chart risk-ranking and applicable data privacy and security laws and regulations' requirements.

4.4 GENERAL DATA PRIVACY PRINCIPLES

ERT complies with the EU-US and Swiss-US Privacy Shield Frameworks, as set forth by the US Department of Commerce regarding Data collection, use, and retention from European Union member countries and Switzerland. ERT shall ensure compliance with the standards, as documented under Section 15 herein.

ERT shall ensure, to the best of its ability, Data is correct, accessible, and conforms to 21 CFR Part 11/Annex 11 controls.

ERT shall ensure site investigators can fulfill their regulatory obligations to maintain, and retain, records obtained using ERT Systems and Processes about Subjects in a clinical investigation.

ERT shall ensure sites have the applicable tools available, and documentation, in order to provide Subjects access to Data during, and after, a clinical investigation.

ERT shall disclose to Sponsors, and site investigators, (who must comply with regulations pertaining to clinical research and eCommerce) applicable Data required to fulfill regulatory responsibilities under FDA 21CFR 312 subpart D for Data Integrity, in clinical trials, for medical products, using ERT Systems and Processes. Data Integrity shall be clear-cut, validated, and auditable.

ERT shall ensure any Data Use by its Personnel, or Agents (where applicable), are done only to perform the applicable service, only the minimum amount of Data is Used, and such Use is done in accordance with Program requirements, this Policy, and applicable data privacy and security laws and regulations.

ERT shall comply with Data disclosure requests, it may be required to fulfill, under the investigatory and enforcement powers of the Federal Trade Commission and any other regulatory agencies identified under this Policy.

Adherence, by ERT, to these General Data Privacy Principles and Access may be limited, to the extent required, to meet any other legal, governmental, national security, or public interest obligations.

4.5 PERSONNEL DATA - COLLECTION AND ACCESS

Data, and Sensitive Personal Data, related to Personnel are subject to Privacy Protection and Data Security, in accordance with this Policy, the Chart, and all applicable US, EU, Swiss, and regional privacy laws and regulations.

ERT Uses Personnel Data, or Sensitive Personal Data, in a transparent way and only shares or discloses such Data for the following reasons, including without limitation: (i) employee management and administration (including both during and after employment); (ii) employment verification; (iii) administering employee benefits; (iv) administering personal short or long-term compensation programs or benefits; (v) evaluating performances; (vi) managing corporate programs;(vii) conducting disciplinary

proceedings; (viii) addressing labor relations issues; (ix) processing health insurance claims; and (x) Data share with Agents for related employment services, including payroll processors and support services. Any request to share Data, or Sensitive Personal Data, with non-Agents, shall only occur if authorized by the individual in writing, subject to other legal and regulatory requirements.

ERT will manage Data, and Sensitive Personal Data, of its Personnel, (from both foreign and domestic office locations, to ERT corporate headquarters located in the United States of America, in accordance with the Chart classifications and company Program requirements.

4.6 SITES, SUBJECTS, SPONSORS AND AGENTS - COLLECTION AND ACCESS

Data, and Sensitive Personal Data, captured from Patients or Subjects, sites, Sponsors, and Agents (during clinical research activities) are subject to Privacy Protection and Data Protection, in accordance with this Policy, the Chart, protections contractually agreed to, and applicable US, EU, Swiss, and applicable regional data privacy and security laws and regulations.

Patient information required to be disclosed to Sponsors shall be pseudonymized, or anonymized, (i.e. individual identifying factors are given unique identifiers or are removed, so that; only certain demographic information, such as an ID code is visible, or no Personal Data, or Sensitive Personal Data are disclosed at all and are not publicly available). Sponsors shall not have access to Data, or Sensitive Personal Data, from Subjects beyond what is defined, and allowed, within the study protocol and informed consent disclosures.

Data requiring disclosure to site investigators, who have clinical responsibility for Patients in the trial, for purposes of reviewing clinically relevant Data, or Sensitive Personal Data, are subject to Privacy Protection and Data Security, in accordance with this Policy, the Chart, and other applicable data privacy and security protections.

ERT will not share Data, or Sensitive Personal Data, about patients, site-staff, or Sponsor personnel with Agents, unless those parties are contractually bound to adhere to substantially the same Program and quality procedures, instructions, and written agreements. Any request to share Data, or Sensitive Personal Data, with non-Agents shall only occur if authorized by the individual in writing.

Services performed by ERT, in the context of a trial, are subject to ERT's Program requirements, Quality Management program requirements, and applicable sponsor instructions and written agreements.

4.7 DATA PROTECTION MEASURES

ERT shall ensure Personnel, and Agents (where applicable), comply with the company's Privacy Protection, and Data Security measures, in accordance with Program requirements, this Policy, and other applicable data privacy and security laws and regulations.

4.8 ORGANIZATIONAL MEASURES

ERT shall ensure that the following measures are taken when Using Data, in accordance with Program Requirements, this Policy, and applicable data privacy and security laws and regulations:

1. Personnel, and Agents (where applicable), shall be made aware of Program requirements and shall be provided with a copy of this Policy, where necessary;

2. Only those Personnel, and Agents (where applicable), shall be authorized to Uses Data in order to carry out the assigned duties;

3. Personnel, and Agents, Using Data will be appropriately trained, and supervised, to ensure compliance with Program requirements and applicable data privacy and security laws and regulations;

4. Data Use shall be periodically reviewed to ensure compliance with Program requirements, this Policy, and applicable data privacy and security laws and regulations;

5. ERT shall periodically evaluate (and review) Personnel, and Agent, performance to ensure compliance with Program requirements, and this Policy, in accordance with applicable data privacy and security laws and regulations;

4.9 DATA TRANSFERS

ERT shall ensure Data transfers (including making Data available remotely) outside the European Economic Area are performed in compliance with applicable data privacy and security laws and regulations, in conformance with Privacy Shield principles, or the EU standard contractual clauses, where required, such transfers are carried out only to perform the applicable services required of ERT, or its Agents (where applicable) and Subjects, Patients, and Personnel have consented to the transfers, where required.

4.10 DATA BREACHES

ERT shall ensure if any Personnel, and Agents (where applicable), become aware of any potential or identified Data Breach, or Security Incident, such incidents shall be reported timely, in accordance with Program requirements and applicable data privacy and security laws and regulations.

4.11 TRAINING

ERT shall ensure its Personnel, who are required to Use Data to fulfil business services and operations, complete data privacy and security training, within 90 days of new-hire on-boarding, and annually thereafter.

ERT shall ensure its Agents, who are required to Use Data to fulfil business services and operations, on ERT's behalf complete data privacy and security training before any services begin.

4.12 PRIVACY SHIELD FRAMEWORKS

ERT complies with the EU-US and Swiss-US Privacy Shield Frameworks, as set forth by the US Department of Commerce, regarding Data collection, use, and retention from European Union member countries and Switzerland. ERT adheres to the Privacy Shield Principles of Notice, Choice, and Accountability for Onward Transfer, Security, Data Integrity and Purpose Limitation, Access, Recourse, Enforcement, and Liability. To learn more about the Privacy Shield program, and to view our certification page, please visit https://www.privacyshield.gov/.

Data transferred under the Privacy Shield Frameworks, ERT is subject to the investigatory and enforcement authority of the Federal Trade Commission.

Under the Privacy Shield Frameworks, ERT shall comply with the requirements to notify EU and Swiss individuals whose Data is transferred into the United States, ensuring the following requirements are satisfied:

- Individuals have the right to access their Data. EU and Swiss individuals wishing to do so may submit a subject access request, to privacy@ert.com, and such request will be managed, in accordance with ERT's SOP-123 Subject Access Request.
- EU and Swiss individuals' Data may be shared in response to lawful requests by public authorities, including to meet national security and law enforcement requirements.
- ERT is liable for the onward transfer of EU and Swiss individual Data to Agents (where applicable), in accordance with applicable service agreements, unless ERT can prove it was not a party to the actions giving rise to the damages.

In compliance with the Privacy Shield Principles, ERT commits to resolve complaints about individuals' privacy and ERT's Use of your Data transferred to the United States under the Privacy Shield. European Union and Swiss individuals with Privacy Shield inquiries or complaints should first contact ERT at: privacy@ert.com.

ERT has further committed to refer unresolved privacy complaints (under the Privacy Shield Principles) to an independent dispute resolution mechanism, the BBB EU PRIVACY SHIELD, operated by the Council of Better Business Bureaus. If you do not receive timely acknowledgment of your complaint, or if your complaint is not satisfactorily addressed, please visit www.bbb.org/EU-privacy-shield/for-eu-consumers for more information and to file a complaint. This service is provided free of charge to you.

If your complaint involves Personnel Data transferred to the United States from the EU, or Switzerland, in the context of the employment relationship, and ERT does not address it satisfactorily, ERT commits to cooperate with the panel established by the EU data protection authorities ("DPA Panel") (or the Swiss Federal Data Protection and Information Commissioner, as applicable) and to comply with the advice given by the DPA Panel (or Commissioner, as applicable) with regard to such Personnel Data. To pursue an unresolved Personnel complaint, individuals should contact the state or national data protection or labor authority in the appropriate jurisdiction. Complaints related to Personnel Data should not be addressed to the BBB EU PRIVACY SHIELD.

Contact details for the EU data protection authorities can be found at http://ec.europa.eu/justice/data-protection/bodies/authorities/index_en.htm

Contact details for the Swiss Federal Data Protection and Information Commissioner can be found at https://www.edoeb.admin.ch/edoeb/en/home/the-fdpic/links/data-protection---switzerland.html

If your Privacy Shield complaint cannot be resolved through the above channels, under certain conditions, individuals may invoke binding arbitration for some residual claims not resolved by other redress mechanisms. See Privacy Shield Annex 1 at https://www.privacyshield.gov/article?id=ANNEX-I-introduction.

4.13 SANCTIONS

ERT shall ensure appropriate steps are taken to comply with Program requirements, this Policy, and applicable data privacy and security regulations for maintaining Data confidentiality. Any violation of Program requirements, this Policy, or other applicable data privacy and security regulations, by Personnel (or Agents, where applicable) shall be grounds for corrective action, up to, and including: termination, or revocation, of the applicable service agreement.

4.14 AUDIT

ERT shall ensure Program requirements, identified herein, are routinely audited, by its Quality Management Department (or outside auditor, where required) no less than once annually, to ensure compliance with applicable data privacy and security laws and regulations.

4.15 RECORD RETENTION

All documents (electronic or hard copy) produced in accordance with this Policy, shall be retained in accordance with the ERT Record Retention Policy.

EXHIBIT 1

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 limit access, 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	**Proprietary Data** – Data which would	• Policies and Procedures

	Information	not cause harm if disclosed, but ERT has chosen to keep confidential. Controls allow access with little technical barriers.	• 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