**ERT**

**Policy**

**Title:** ERT General Data Protection Regulation (GDPR) Policy

**Number:** POL COR-014-0

**Department:** Corporate

**Effective Date:** 25MAY2018

|  |  |  |
| --- | --- | --- |
|  |  |  |
| **Approvals** | | |
|  |  |  |
|  | **Date Issued for Approval** | **21MAY2018** |
|  |  |  |
|  | **Originator:** | **Chris Watson** |
|  | **Title, Department:** | **Director, Product Strategy** |
|  |  |  |
|  | **Department Approval:** | **Jim Corrigan** |
|  | **Title, Department:** | **President, & CEO** |
|  |  |  |
|  | **Quality Management Approval:** | **Richard Miller** |
|  | **Title, Department:** | **Vice President, Quality Management** |
|  |  |  |
| *Titles indicated are reflective of area of responsibility at time of approval.*  *Electronic signatures for all approvers are maintained on file.* | | |
|  |  |  |

***This document is for circulation within ERT only and must not be passed or copied to other Companies or persons without written permission of Quality Management of ERT.***

1. **General Overview**:

The objective of the Policy is to outline eResearch Technology (ERT’s) responsibilities as they relate to the rights of individuals in respects to their personal data under the European General Data Protection Regulation (GDPR).

The GDPR defines “personal data” as any information relating to an identified or identifiable natural person (a data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

This Policy sets out the procedures that are to be followed when dealing with personal data. The procedures and principles set out herein must be followed at all times by ERT, its employees, agents, contractors, or other parties working on behalf of ERT.

ERT is committed not only to the letter of the law, but also to the spirit of the law and places high importance on the correct, lawful, and fair handling of all personal data, respecting the legal rights, privacy, and trust of all individuals with whom it deals.

1. **The Data Protection Principles**

This Policy aims to ensure compliance with the Regulation. The Regulation sets out the following principles with which any party handling personal data must comply. All personal data must be:

* + processed lawfully, fairly, and in a transparent manner in relation to the data subject;
  + collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
  + adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed;
  + accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
  + kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the Regulation in order to safeguard the rights and freedoms of the data subject;
  + processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

1. **Related Documents**:

DOC COR 014\_01 - GDPR - Personal Information – Accounting of Disclosures

SOP 104 – Confidentiality

SOP 115 – Business Continuity

SOP 761 – IT Service Continuity Management

POL COR-003 – Clinical Misconduct/Fraud Policy

POL COR-004 – Records Retention Policy

POL COR-005 – Security Policy

POL COR-007 – Privacy Policy

POL COR-015 – Staff Records Management Policy

POL COR-016 – Staff Subject Access Request Policy

SOP 122 - Data Protection Procedure for EPG staff on Assessment, Remediation, Reporting and Control of Data Breaches

SOP 123 - Data Protection Procedure for EPG Staff on the Assessment, Generation, Reporting and Control of Data and Data Portability Requests

SOP 124 - Data Protection Procedure for Data Breach Alerting, Personal Data and Data Portability Requests

SOP 125 – Staff Data Retention Schedule

Health Insurance Portability and Accountability Act of 1996 (HIPAA)

General Data Protection Regulations (GDPR)

1. **Definitions/Acronyms**:

Data Controller: Any person (or organisation), public authority, agency or other body which alone or jointly makes decisions with regard to particular personal data including decisions regarding the purposes for which personal data is processed and the way in which it is processed. The Data Controller is FRFL and not an individual.

Data Processor: Any person (or organisation), public authority, agency or other body which alone or jointly (other than an employee of the data controller) who processes the data on behalf of the data controller.

Data Protection Officer(s): This is/are the nominated individual(s) with overall responsibility to address GDPR specific issues. The Data Protection Officer (DPO) shall be designated based upon professional qualities (detailed knowledge of GDPR and data protection practices). The DPO may be a staff member or a contractor who can fulfil the tasks of the role.

Data Subject: An individual who is the subject of personal data including customers and employees

GDPR: General Data Protection Regulation (EU) [2016/679](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016R0679) is an [EU law](https://en.wikipedia.org/wiki/EU_law) on [data protection](https://en.wikipedia.org/wiki/Data_protection) and privacy for all individuals within the [European Union](https://en.wikipedia.org/wiki/European_Union). It also addresses the export of personal data outside the EU. The GDPR aims primarily to give control to citizens and residents over their personal data and to simplify the regulatory environment for [international business](https://en.wikipedia.org/wiki/International_business) by unifying the regulation within the EU.

Individually Identifiable Health Information - Information that is a subset of health information, including demographic information collected from an individual, and:

* 1. Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and
  2. Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and

(i) That identifies the individual; or

(ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Information System: an interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, applications, communications and people.

Personal Data: Data which relates to a living individual who can be identified directly or from those data, or from those data and other information which is in the possession, or is likely to fall into the possession, of the data controller e.g. name, address, telephone number, ID number. Personal data includes an expression of opinion about the individual, and of the intentions of the data controller in respect of that individual.

Personnel: current, past and prospective employees, trainees, temporary workers, contractors, consultants or applicant, or other parties working on behalf of ERT

Processing - Any operation or set of operations which is performed on personal data related to organisation, retrieval, disclosure and deletion of data and includes:

* Collecting and recording data
* Accessing, altering, adding to, merging, deleting data
* Retrieval, consultation or use of data
* Disclosure, dissemination or otherwise making available of data.

Relevant Filing System - Any paper or other manual filing system which is structured so that information about an individual is readily accessible. Although this is the definition of "Relevant Filing System" in the Act, personal data as defined, and covered, by the Act can be held in any format, electronic (including websites and emails), paper-based, photographic etc. from which the individual's information can be readily extracted.

Special Categories of Data - Different from ordinary personal data (such as name, address, telephone) and relates to: Racial or ethnic origin, political opinions, religious or philosophical beliefs, traded-union membership, and the processing of genetic data, biometric data in order to uniquely identify a person or data concerning health or sex life and sexual orientation. Special categories of data are subject to much stricter conditions of processing and explicit consent must be obtained in all cases.

In addition: Processing of data relating to **criminal convictions** **and offences** or related security measures may only be carried out either under the control of official authority or when the processing is authorised by Union law or Member State law providing for adequate safeguards for the rights and freedoms of data subject.  A complete register of criminal convictions may be kept only under the control of official authority.

Workforce: Under HIPAA, this means employees, volunteers, trainees, and other persons under the direct control of a data controller, whether or not they are paid by the data controller. Part II, 45 CFR 160.103.

1. **Individuals Personal Data Rights Overview**:

**5.1 Lawful, Fair, and Transparent Data Processing (lawfulness, Fairness & Transparency)**

The Regulation seeks to ensure that personal data is processed lawfully, fairly, and transparently, without adversely affecting the rights of the data subject. The Regulation states that processing of personal data shall be lawful if at least one of the following applies:

* + the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
  + processing is necessary for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract;
  + processing is necessary for compliance with a legal obligation to which the controller is subject;
  + processing is necessary to protect the vital interests of the data subject or of another natural person;
  + processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
  + processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

**5.2 Processed for Specified, Explicit and Legitimate Purposes (Purpose Limitation)**

ERT collects and processes the personal data set out in Part 5.19 of this Policy. This may include personal data received directly from data subjects (typically this will be data received from ERT employees and processed for employment purposes) and data received from third parties (for example, clients will provide us with information patient information relating to clinical trials ‘scientific research’).

ERT only processes personal data for the specific purposes set out in Part 5.19 of this Policy (or for other purposes expressly permitted by the Regulation). The purposes for which we process personal data will be informed to data subjects at the time that their personal data is collected, where it is collected directly from them, or as soon as possible (not more than one calendar month), should the eventuality occur, collection where it is obtained from a third party.

**5.3 Adequate, Relevant and Limited Data Processing (Data Minimisation)**

ERT will only collect and process personal data for and to the extent necessary for the specific purpose(s) informed to data subjects as under Part 4, above.

**5.4 Accuracy of Data and Keeping Data Up To Date (Accuracy)**

The Company shall ensure that all personal data collected and processed is kept accurate and up-to-date. The accuracy of data shall be checked when it is collected and at regularintervals thereafter. Where any inaccurate or out-of-date data is found, all reasonable steps will be taken without delay to amend or erase that data, as appropriate, to maintain the data accuracy. Typically, the information held by ERT relates to employees and that information will be kept up to date. ERT acts as data processor for its clients and clients provide up to date data.

**5.5 Timely Processing (Storage Limitations)**

ERT shall not keep personal data for any longer than is necessary in light of the purposes for which that data was originally collected and processed. When the data is no longer required, all reasonable steps will be taken to erase it without delay. Personal data may be retained for longer periods providing the personal data is required for scientific or historical research purposes.

**5.6 Secure Processing (integrity & Confidentiality)**

ERT shall ensure that all personal data collected and processed is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction or damage. Further details of the data protection and organisational measures which shall be taken are provided in Parts 5.23 and 5.24 of this Policy.

**5.7 Accountability**

ERT’s Data Protection Officer is Klaus Hoogestraat[datenschutz@ert.com](mailto:datenschutz@ert.com).

ERT shall keep written internal records of all personal data collection, holding, and processing, which shall incorporate the following information:

* + The name and details of ERT, its DPO, and any applicable third-party data controllers;
  + The name and contact details of the Data Controllers and if applicable joint Data Controllers
  + The purposes for which the ERT processes personal data;
  + Details of the categories of personal data collected, held, and processed by the Company; and the categories of data subject to which that personal data relates;
  + Details (and categories) of any third parties (recipients) that will receive personal data from the ERT;
  + Details of any transfers of personal data to non-EEA countries including all mechanisms and security safeguards;
  + Details of how long personal data will be retained by the ERT; and time limits for the erasure of different personal data categories.
  + Detailed descriptions of all technical and organisational measures taken by ERT to ensure the security of personal data.

**5.8 Privacy Impact Assessments**

ERT shall carry out Privacy Impact Assessments when and as required under the Regulation. Privacy Impact Assessments shall be overseen by ERT’s data protection officer and shall address the following areas of importance:

The purpose(s) for which personal data is being processed and the processing operations to be carried out on that data;

Details of the legitimate interests being pursued by the Company;

An assessment of the necessity and proportionality of the data processing operations with respect to the purpose(s) for which it is being processed;

An assessment of the risks posed to individual data subjects; and

Details of the measures in place to minimise and handle risks including safeguards, data security, and other measures and mechanisms to ensure the protection of personal data, sufficient to demonstrate compliance with the Regulation.

**5.9 The Rights of Data Subjects**

The Regulation sets out the following rights applicable to data subjects:

* + The right to be informed including the communication methods;
  + The right of access by the data subject;
  + The right to rectification;
  + The right to erasure (also known as the ‘right to be forgotten’);
  + The right to restrict processing;
  + The right to data portability;
  + The right to object;
  + Rights with respect to automated decision-making and profiling.

**5.10 Keeping Data Subjects Informed**

ERT shall ensure that the following information is provided to every data subject when personal data is collected:

* + Details of ERT including, but not limited to, the identity and contact details of its Data Protection Officer;
  + The purpose(s) for which the personal data is being collected and will be processed (as detailed in Parts 5.19 and 5.20 of this Policy) and the legal basis justifying that collection and processing;
  + Where applicable, the legitimate interests of the Data Controller and/or relevant third parties, upon which ERT is justifying its collection and processing of the personal data;
  + Where the personal data is not obtained directly from the data subject, the categories of personal data collected and processed;
  + Where the personal data is to be transferred to one or more third parties, details of those parties;
  + Where the personal data is to be transferred to a third party that is located outside of the European Economic Area (the “EEA”), details of that transfer, including but not limited to the safeguards in place (see Part 5.23 of this Policy for further details concerning such third country data transfers);
  + Details of the length of time the personal data will be held by ERT (or, where there is no predetermined period, details of how that length of time will be determined);
  + Details of the data subject’s rights under the Regulation to request from the Data Controller to access, rectify, delete or restrict processing of their Personal Data;
  + Details of the data subject’s right to withdraw their consent to ERT’s processing of their personal data at any time;
  + Details of the data subject’s right to complain to the Information Commissioner’s Office (the ‘supervisory authority’ under the Regulation);
  + Where applicable, details of any legal or contractual requirement or obligation necessitating the collection and processing of the personal data and details of any consequences of failing to provide it;
  + Details of any automated decision-making that will take place using the personal data (including but not limited to profiling), including information on how decisions will be made, the significance of those decisions and any consequences.

The information set out above shall be provided to the data subject at the following applicable time:

Where the personal data is obtained from the data subject directly, at the time of collection;

In the event that personal data is not obtained from the data subject directly (i.e. from another party):

* 1. If the personal data is used to communicate with the data subject, at the time of the first communication; or
  2. If the personal data is to be disclosed to another party, before the personal data is disclosed; or
  3. In any event, not more than one month after the time at which ERT obtains the personal data.

**5.11 Data Subject Access**

A data subject may make a subject access request (“SAR”) at any time to find out more about the personal data which ERT holds about them. ERT is normally required to respond to SARs within one month of receipt (this can be extended by up to two months in the case of complex and/or numerous requests, and in such cases the data subject shall be informed of the need for the extension).

All subject access requests received must be forwarded to ERT’s Data Protection Officer and/or nominated representatives as detailed in the Data Protection Procedure for EPG Staff on the Assessment, Generation, Reporting and Control of Data and Data Portability Requests SOP.

ERT does not charge a fee for the handling of normal SARs. ERT reserves the right to charge reasonable fees based upon administrative costs, for additional copies of information that has already been supplied to a data subject, and for requests that are manifestly unfounded or excessive, particularly where such requests are repetitive.

**5.12 Rectification of Personal Data**

If a data subject informs ERT that personal data held is inaccurate or incomplete, requesting that it be rectified, the personal data in question shall be rectified, and the data subject informed of that rectification, within one month of receipt the data subject’s notice (this can be extended by up to two months in the case of complex requests, and in such cases the data subject shall be informed of the need for the extension).

In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of any rectification of that personal data.

**5.13 Erasure of Personal Data**

Data subjects may request that ERT erases the personal data it holds about them in the following circumstances:

* + It is no longer necessary for the Company to hold that personal data with respect to the purpose for which it was originally collected or processed;
  + The data subject wishes to withdraw their consent to the Company holding and processing their personal data;
  + The data subject contests and can confirm that the Personal Data held is inaccurate;
  + The data subject objects to the Company holding and processing their personal data (and there is no overriding legitimate interest to allow the Company to continue doing so) (see Part 18 of this Policy for further details concerning data subjects’ rights to object);
  + The personal data has been processed unlawfully;
  + The personal data needs to be erased in order for the Company to comply with a particular legal obligation;
  + The personal data is being held and processed for the purpose of providing information society services to a child.
  + Supported by a request for the data to be erased by the Data Controller or Joint Data Controller when this is nor ERT.

Unless ERT has reasonable grounds to refuse to erase personal data, all requests for erasure shall be complied with, and the data subject informed of the erasure, within one month of receipt of the data subject’s request (this can be extended by up to two months in the case of complex requests, and in such cases the data subject shall be informed of the need for the extension).

In the event that any personal data that is to be erased in response to a data subject request has been disclosed to third parties, those parties shall be informed of the erasure (unless it is impossible or would require disproportionate effort to do so).

**5.14 Restriction of Personal Data Processing**

Data subjects may request that ERT ceases processing the personal data it holds about them. If a data subject makes such a request, ERT shall retain only the amount of personal data pertaining to that data subject that is necessary to ensure that no further processing of their personal data takes place.

In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of the applicable restrictions on processing it (unless it is impossible or would require disproportionate effort to do so).

**5.15 Data Portability**

Where data subjects have given their consent to ERT to process their personal data in such a manner or the processing is otherwise required for the performance of a contract between ERT and the data subject, data subjects have the legal right under the Regulation to receive a copy of their personal data and to use it for other purposes (namely transmitting it to other data controllers, e.g. other organisations).

To facilitate the right of data portability, ERT shall make available all applicable personal data to data subjects in the following human readable format**[**s**]**:

* + .DOC/.DOCX
  + .XLS
  + .TXT

Where technically feasible, if requested by a data subject, personal data shall be sent directly to another data controller.

All requests for copies of personal data shall be complied with within one month of the data subject’s request (this can be extended by up to two months in the case of complex requests in the case of complex or numerous requests, and in such cases the data subject shall be informed of the need for the extension).

**5.16 Objections to Personal Data Processing**

Data subjects have the right to object to ERT processing their personal data based on legitimate interests (including profiling), direct marketing (including profiling), and processing for scientific and/or historical research and statistics purposes.

Where a data subject objects to ERT processing their personal data based on its legitimate interests, ERT shall cease such processing forthwith, unless it can be demonstrated that ERT’s legitimate grounds for such processing override the data subject’s interests, rights and freedoms; or the processing is necessary for the conduct of legal claims.

Where a data subject objects to ERT processing their personal data for direct marketing purposes, the Company shall stop such processing immediately.

Where a data subject objects to ERT processing their personal data for scientific and/or historical research and statistics purposes, the data subject must, under the Regulation, ‘demonstrate grounds relating to his or her particular situation’. ERT is not required to comply if the research is necessary for the performance of a task carried out for reasons of public interest.

**5.17 Automated Decision-Making**

In the event that ERT uses personal data for the purposes of automated decision-making and those decisions have a legal (or similarly significant effect) on data subjects, data subjects have the right to challenge to such decisions under the Regulation, requesting human intervention, expressing their own point of view, and obtaining an explanation of the decision from ERT.

The right described above does not apply in the following circumstances:

* + The decision is necessary for the entry into, or performance of, a contract between ERT and the data subject;
  + The decision is authorised by EU or Swiss law, providing adequate data protection is applied; or
  + The data subject has given their explicit consent.

**5.18 Profiling**

Should ERT use personal data for profiling purposes, the following shall apply:

* + Clear information explaining the profiling will be provided, including its significance and the likely consequences;
  + Appropriate mathematical or statistical procedures will be used;
  + Technical and organisational measures necessary to minimise the risk of errors and to enable such errors to be easily corrected shall be implemented; and
  + All personal data processed for profiling purposes shall be secured in order to prevent discriminatory effects arising out of profiling (see Parts 22 and 23 of this Policy for more details on data security).

**5.19 Personal Data**

The following personal data may be collected, held, and processed by ERT:

* + Data relating to Personnel to enable ERT to fulfil its obligations related to their employment as described in Part 5.20 of this Policy.
  + Data relating to patients where ERT acts as data processor for its clients when undertaking clinical trials.
  + Information provided to ERT directly by patients in relation to the provision of social information services.

**5.20 Personnel Data**

The categories of personal data that ERT collect, uses, transfers and stores about Personnel may include:

* + Identification data and personal characteristics (e.g name, address, date of birth, gender, email address, phone number(s), picture, signature and other contact details);
  + National identifier information (Passport number, Social security number, BRP, full birth certificate, NINO card / Letter);
  + Family and social details (marital status, dependents, emergency contact names and addresses, medical GP contact details);
  + Education, results/grade, qualification, career history and any references obtained during recruitment;
  + Employment details (job description, title and duties, hire date, qualifications, health and safety data, work time/utilization records, retirement details, departure details, employment history, training, and career achievements and performance, line manager and feedback from employee about their time with ERT and reasons for leaving);
  + Financial data (payroll details including salary, pension schemes calculation and other benefits; tax information, bank account details and credit card details);
  + Connection data (Password, employee ID, IP address);
  + Absences records relating to health, sickness, holiday and other leave (e.g seminar, maternity or paternal leave);
  + Details of any investigations and proceedings, including, disciplinary, accident, or other reports; identification data and personal characteristics (e.g name, date of birth, age, gender, email address, phone number(s));
  + Correspondence or any other information that you have given to ERT.

Prior to employment, throughout employment, and for as long as is necessary after termination of employment, ERT will need to process personal data for purposes connected with employment, including to comply with its legal obligations under applicable local laws and as necessary in connection with the performance of contract of employment. Personal data is also processed by ERT for its legitimate business interests, including for the operation of standard business functions such as human resource management, legal and/or regulatory compliance and/or administrative, accounting and managerial purposes.

In particular, the abovementioned categories of data are processed for the following purposes:

* To determine suitability to role,
  + obtain proof of previous career history
  + preserve the documents of rejected applicants for managing applicant selection process and employee hiring process;
* To support an employee’s life cycle,
  + personnel records
  + timekeeping
  + congratulations on company anniversaries,
  + target agreement and
  + target measurement

gets managed

* To set up salary payments / deductions, etc. via payroll;
* To assist in HR process enabling the employee be set up and receive current benefits, used for childcare, management of pension scheme, and to know whom any monies are payable to in the event of death;
* Where applicable - for internal use to monitor absence, and to obtain signed consent to write employees’ GP for a medical report on the current illness that keep them away from work;
* To review the evidence and case allegations and action any formal outcome in the framework of keeping disciplinary records;
* To manage employee survey with external support;
* To enable transfer of CVs to third parties as proof of suitability;
* For internal use to record, monitor and review training needs and training received.

ERT will retain personal data relating to Personnel for at least the period of the employment relationship. Once period of employment is ended ERT will retain personal data for up to two years or where applicable as long as is necessary to comply with any and all applicable laws. Personal Data will thereafter be deleted.

Personal data concerning Personnel may need to be transferred to relevant third party such as

* customers,
* government or regulatory bodies,
* insurers,
* legal, medical and other professional advisers,
* administrators of employer pension schemes or employee’s pension provider where required,
* or to ERT’s entities located in other countries for employment related services, business operations and for the purposes set out in Part 5.20 above.

For any transfer of personal data to a third country, ERT have guaranteed an adequate level of data protection in accordance with Part 5.23 of this Policy.

**5.21 Data Protection Measures**

ERT shall ensure that all its employees, agents, contractors, or other parties working on its behalf comply with the following when working with personal data:

* + All emails containing personal data must be encrypted and password protected using (S-MIME) Secure Multipurpose Mail Extension;
  + Where any personal data is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it should be securely deleted and disposed of. Hardcopies should be shredded, and electronic copies should be deleted securely as detailed in the Records Retention Policy.
  + Personal data may be transmitted over secure networks only; transmission over unsecured networks is not permitted in any circumstances;
  + Personal data may not be transmitted over a wireless network if there is a wired alternative that is reasonably practicable;
  + Personal data contained in the body of an email, whether sent or received, should be copied from the body of that email and stored securely. The email itself should be deleted. All temporary files associated therewith should also be deleted;
  + Where Personal data is to be sent by facsimile transmission the recipient should be informed in advance of the transmission and should be waiting by the fax machine to receive the data;
  + Where Personal data is to be transferred in hardcopy form it should be passed directly to the recipient or sent using a registered carrier as detailed in the Data Protection Procedure for EPG Staff on the Assessment, Generation, Reporting and Control of Data and Data Portability Requests.
  + No personal data may be shared informally and if an employee, agent, sub-contractor, or other party working on behalf of ERT requires access to any personal data that they do not already have access to, such access should be formally requested from the DPO with an appropriate Data Privacy Agreement being implemented;
  + All hardcopies of personal data, along with any electronic copies stored on physical, removable media should be stored securely in a locked box, drawer, cabinet or similar;
  + No personal data may be transferred to any employees, agents, contractors, or other parties, whether such parties are working on behalf of ERT or not, without the authorisation the DPO with an appropriate Data Privacy Agreement being implemented;
  + Personal data must be handled with care at all times and should not be left unattended or on view to unauthorised employees, agents, sub-contractors or other parties at any time;
  + If personal data is being viewed on a computer screen and the computer in question is to be left unattended for any period of time, the user must lock the computer and screen before leaving it;
  + No personal data should be stored on any mobile device (including, but not limited to, laptops, tablets and smartphones), whether such device belongs to the Company or otherwise, without the formal written approval the DPO with an appropriate Data Privacy Agreement being implemented. In the event of such approval, strictly in accordance with all instructions and limitations described at the time the approval is given, and for no longer than is absolutely necessary;
  + No personal data should be transferred to any device personally belonging to an employee and personal data may only be transferred to devices belonging to agents, contractors, or other parties working on behalf of ERT where the party in question has agreed to comply fully with the letter and spirit of this Policy and of the Regulation (which may include demonstrating to ERT that all suitable technical and organisational measures have been taken);
  + All personal data stored electronically should be backed up in accordance with the Data Retention Policy with backups stored onsite **AND/OR [**offsite**]**. All backups should be encrypted i.e. all electronic copies of personal data, should be stored securely using passwords and data encryption;
  + All passwords used to protect personal data should be changed regularly and should not use words or phrases that can be easily guessed or otherwise compromised. All passwords must contain a combination of uppercase and lowercase letters, numbers, and symbols.All software used by ERT is designed to require such passwords;
  + Under no circumstances should any passwords be written down or shared between any employees, agents, contractors, or other parties working on behalf of ERT, irrespective of seniority or department. If a password is forgotten, it must be reset using the applicable method. IT staff do not have access to passwords;
  + In the event that personal data held by ERT is used for marketing purposes, it shall be the responsibility of the DPO to ensure that no data subjects have added their details to any marketing preference databases including, but not limited to, the Telephone Preference Service, the Mail Preference Service, the Email Preference Service, and the Fax Preference Service. Such details should be checked at least annually.

**5.22 Organisational Measures**

ERT shall ensure that the following measures are taken with respect to the collection, holding, and processing of personal data:

* + All employees, agents, contractors, or other parties working on behalf of ERT shall be made fully aware of both their individual responsibilities and ERT’s responsibilities under the Regulation and under this Policy, and shall be provided with a copy of this Policy;
  + Only employees, agents, sub-contractors, or other parties working on behalf of ERT that need access to, and use of, personal data in order to carry out their assigned duties correctly shall have access to personal data held by ERT;
  + All employees, agents, contractors, or other parties working on behalf ERT handling personal data will be appropriately trained to do so;
  + All employees, agents, contractors, or other parties working on behalf of ERT handling personal data will be appropriately supervised;
  + Methods of collecting, holding and processing personal data shall be regularly evaluated and reviewed;
  + The performance of those employees, agents, contractors, or other parties working on behalf of ERT handling personal data shall be regularly evaluated and reviewed;
  + All employees, agents, contractors, or other parties working on behalf of ERT handling personal data will be bound to do so in accordance with the principles of the Regulation and this Policy by contract;
  + All agents, contractors, or other parties working on behalf of ERT handling personal data must ensure that any and all of their employees who are involved in the processing of personal data are held to the same conditions as those relevant employees of ERT arising out of this Policy and the Regulation;
  + Where any agent, contractor or other party working on behalf of ERT handling personal data fails in their obligations under this Policy that party shall indemnify and hold harmless ERT against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

**5.23 Transferring Personal Data to a Country Outside the EEA**

ERT may from transfer (‘transfer’ includes making available remotely) personal data to countries outside of the EEA.

The transfer of personal data to a third country outside of the EEA shall take place only if one or more of the following applies:

* + The transfer is to a country, territory, or one or more specific sectors in that country (or an international organisation), that the European Commission has determined ensures an adequate level of protection for personal data;
  + The transfer is to a country (or international organisation) which provides appropriate safeguards in the form of a legally binding agreement between public authorities or bodies; binding corporate rules; standard data protection clauses adopted by the European Commission; compliance with an approved code of conduct approved by a supervisory authority (e.g. the Information Commissioner’s Office); certification under an approved certification mechanism (as provided for in the Regulation); contractual clauses agreed and authorised by the competent supervisory authority; or provisions inserted into administrative arrangements between public authorities or bodies authorised by the competent supervisory authority;
  + The transfer is made with the informed consent of the relevant data subject(s);
  + The transfer is necessary for the performance of a contract between the data subject and the Company (or for pre-contractual steps taken at the request of the data subject);
  + The transfer is necessary for important public interest reasons;
  + The transfer is necessary for the conduct of legal claims;
  + The transfer is necessary to protect the vital interests of the data subject or other individuals where the data subject is physically or legally unable to give their consent; or
  + The transfer is made from a register that, under UK or EU law, is intended to provide information to the public and which is open for access by the public in general or otherwise to those who are able to show a legitimate interest in accessing the register.

**5.24 Data Breach Notification**

If any staff become aware of any potential or identified personal data breach they must be reported immediately to ERT’s DPO in accordance with the Data Breach and Personal Data Requests - ERT Staff SOP. It will be the responsibility of the DPO to notify the Data Controller (if that is not ERT) in accordance with the Data Breach – ERT Privacy Group SOP. If ERT is the Data Controller the DPO will report the breach to senior management and affected staff in accordance with the Data Breach – ERT Privacy Group SOP

If a personal data breach occurs and that breach is likely to result in a risk to the rights and freedoms of data subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the DPO must ensure that the relevant supervisory agency e.g. Information Commissioner’s Office is informed of the breach without delay, and in any event, within 72 hours after having become aware of it. If this is delayed for any reason this must also be shared with the supervisory agency.

In the event that a personal data breach is likely to result in a high risk (that is, a higher risk than that described under Part 25.2) to the rights and freedoms of data subjects, the DPO must ensure that all affected data subjects are informed of the breach directly and without undue delay.

Data breach notifications shall include the following information:

* + The nature of the personal data breach identified;
  + The categories and approximate number of data subjects concerned;
  + The categories and approximate number of personal data records concerned;
  + The name and contact details of ERT’s data protection officer (or other contact point where more information can be obtained);
  + The likely consequences of the breach;
  + Details of the measures taken, or proposed to be taken, by ERT to address the breach including, where appropriate, measures to mitigate its possible adverse effects.

1. **Personal Data Uses and Disclosures Overview**:

This procedure addresses the handling, safeguarding, using, and disclosing personal data. In accordance with eResearch Technology (“ERT”) Data Privacy Agreement with its Clients (“Data Controllers”) and its vendors (“Data Processors”), we must ensure the privacy of an individual’s personal data.

## Personal Data Uses and Disclosures Procedure:

7.1 MINIMUM NECESSARY

When using, disclosing or requesting personal data, ERT will make reasonable efforts to limit personal data to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request. Any staff contacted will respond and inform the DPO and nominated staff in accordance with the Data Breach and Personal Data Requests - ERT Staff SOP. The DPO and/or nominated staff will address the request in accordance with the Personal Data Request – ERT Privacy Group SOP.

The following are situations in which the Minimum Necessary provisions would **not** apply:

* Uses or Disclosures that are required by law
* Uses or Disclosures made to the individual
* Uses or Disclosures made pursuant to an authorization
* Disclosures to a health care provider for treatment purposes
* Disclosures to the Information Commissioners Office (ICO) for enforcement purposes
* Uses or Disclosures that are required for compliance with GDPR requirements

Before using or disclosing personal data consider two basic questions:

* 1. How much information is needed to fulfil the purpose of this request?
  2. Are we about to provide information that is not necessary to fulfil the purpose of this request?

7.2 USES AND DISCLOSURES OF PERSONAL DATA

1. ERT will not use personal data for purposes other than as permitted by the GDPR, this Policy, and by the applicable Data Privacy Agreement with a Data Controller.
2. In terms of ERT’s use of personal data, workforce members may use or access personal data only in connection to the services ERT is performing on behalf of a data controller (client) or in furtherance of engaging a subcontractor to perform such services on behalf of ERT.
3. Generally, if a workforce member’s immediate supervisor (or the Data Protection Officer (DPO)) has not expressly instructed the workforce member that a certain type of use or disclosure of personal data is permissible, the workforce member must immediately notify the DPO about the possible use or disclosure and only use or disclose the personal data with the DPO’s express permission.
4. The following types of disclosures are regularly entertained by Data Controllers and Data Processors, and the workforce is aware that they may arise. In accordance with the above stated general policy, a workforce member may use or disclose personal data for the following purposes, but **must** **consult with the DPO before doing so** (even if a prior instance of this sort of disclosure has been discussed with the workforce member’s immediate supervisor or the DPO:
5. Lawsuits and Disputes: personal data may be disclosed in response to a subpoena/court order, discovery request, or other lawful order from a court.
6. As Required by Law: ERT will disclose personal data about individuals when required to do so by EU, European state or local law.
7. As Permitted by Law: To the extent that the law permits ERT to release information, we may disclose personal data if asked to do so by a law enforcement official as part of law enforcement activities; in investigations of criminal conduct or of victims of crime; in response to court orders; in emergency circumstances.
8. Troubleshooting for investigator sites confirming data sources as part of a regulatory inspection.
9. **Individuals Personal Data Rights Overview**:

Under GDPR, in addition to being able to request an accounting of personal data disclosures, individuals also have the right to request access to or obtain a copy of, request an amendment to or a restriction of their personal data maintained in a designated record set. To the extent ERTis obligated to respond to such requests on behalf of a Data Controller client (as set forth in the associated Data Privacy Agreement), ERT will comply with the GDPR requirements that are applicable to the Data Controller client in the performance of such obligation. Prior to responding to any request by a Data Controller client or an individual for an accounting, access to personal data, an amendment of personal data, or a restriction to personal data, the ERT workforce member in receipt of the request shall promptly contact the DPO and handle the request as directed by the DPO.

1. **Safeguarding Personal Data Overview**:

These policies and procedures address the safeguarding of personal data. ERT must have in place administrative, technical, and physical safeguards to protect the privacy of personal data.

## Safeguarding Personal Data Procedure:

10.1 SAFEGUARDS

1. ERT will take reasonable efforts to safeguard personal data from any intentional or unintentional use or disclosure that is a violation of the GDPR. Such safeguards include, but are not limited to the following:
   1. Workforce members must ensure that all documents containing personal data are placed in the designated cabinet/filing space and that these are locked when unattended, including at the end of each working day.
   2. Workforce members must dispose of documents containing personal data that is no longer required in the appropriate manner. This may involve returning the personal data to the Data Controller client or shredding / confidential waste bins to permanently destroy the personal data.
2. ERT will take reasonable efforts to limit incidental uses or disclosures of personal data made pursuant to an otherwise permitted or required use or disclosure.
3. **Workforce Training Overview**:

This procedure addresses the training of the workforce of ERT in the GDPR. The workforce consists of but is not limited to the following: employees, volunteers, and affiliates.

## Workforce Training Procedure:

1. All current members of the workforce who are likely to come into contact with personal data will be given annual GDPR awareness training and trained in the GDPR ERT’s policies and procedures with respect to personal data.
2. New members of the workforce will receive GDPR awareness training and training in the GDPR and ERT’s policies and procedures with respect to personal data upon employment.
3. If there is a material change in the GDPR or ERT’s privacy policies and procedures, all members of the workforce whose duties are directly affected by the change will be retrained within 30 days of document approval.
4. Training records will be maintained in the TMS training database.

1. If it is determined that any subcontractor of ERT requires HIPAA training, ERT will either provide the training or require the subcontractor to provide documentation of such training.
2. **Employee Sanctions Overview**:

The purpose of this section is to address non-compliance with the GDPR or the privacy and security policies and procedures of ERT, which govern the confidentiality of personal data.

It is the policy of ERT to take appropriate steps to promote compliance with the requirements for maintaining the confidentiality of personal data. ERT takes seriously its requirements under GDPR and applicable Data Privacy Agreements with Data Controllers to protect the confidentiality of personal data and will respond appropriately to violations of these policies.

The appropriate response to such violations will depend on the severity of the violation, and the record of the employee.

The response will be decided after investigating the specific facts of the situation and may include, but is not limited to, such actions as: system changes, additional education, a written reprimand, a suspension, and termination of employment.

Employees and others who are working on behalf of ERT, who report, in good faith, violations of the GDPR or ERT’s policies and procedures shall not be retaliated against. They may report any retaliation to their direct supervisor, or the DPO. All reports shall be referred to the DPO. The DPO shall determine who will investigate the matter.

## Employee Sanctions Procedure:

1. It is the responsibility of the DPO to determine the appropriate process to follow when aware of allegations of a violation of the GDPR or ERT’s privacy and security policies and procedures by an employee. If it is determined that a violation that could result in disciplinary action has occurred, the DPO in conjunction with Senior Management and HR has the responsibility to determine the appropriate response. This is detailed in Clinical Misconduct/Fraud Policy for employee sanctions and Privacy Policy and may result in dismissal.
2. One of the factors to consider when determining the appropriate response for a violation of the GDPR or ERT’s privacy and security policies and procedures is the severity of the violation. ERT has determined that there are four categories of violations.

* Type I – these violations are inadvertent or accidental breaches of confidentiality that may or may not result in the actual disclosure of personal data (for example, sending an email to an incorrect address).
* Type II – these violations result from failure to follow existing policies/procedures governing privacy or security (for example, failure to fulfill training requirements).
* Type III – these violations include inappropriately accessing a patient’s record without a job-related need to know (for example, accessing the record of a friend or co-worker out of curiosity without a legitimate need to know the information).
* Type IV – these violations include accessing and using personal data for personal gain or to harm another person.

1. In addition to the severity of the violation, factors such as the past record of the employee must be considered. As a result, the appropriate response must be determined on a case-by-case basis. For example, while an inadvertent violation might normally result in additional education, it could result in more serious action if it was part of a pattern of violations or other performance problems.
2. All violations must immediately be reported to ERT’s DPO.
3. Each instance of workforce disciplinary action regarding the privacy or security of personal data is to be documented in a written or electronic record by the DPO. The Sanctions log will contain the following information:

* Name of employee
* Description of violation
* Level of breach or violation
* Location of breach or violation
* Date and time of breach or violation
* Disciplinary action taken

1. This documentation must be retained for 25 years from the date of its creation or the date when it was last in effect whichever is later.
   1. **Workforce Terminations Overview**:

This procedure addresses the handling of privacy and security issues when an employee (or other member of the workforce) of ERT leaves or is terminated.

## 14.2 Workforce Terminations Procedure:

1. When an individual will no longer be a member of ERT, both physical and electronic access to information will be denied.
2. New combinations to combination locks will be issued; if a new combination cannot be issued then the combination lock will be changed.
3. Security system access codes will be changed immediately, and to the extent possible prior to informing the employee of the termination decision.
4. Security will be notified that the individual leaving ERT is no longer granted access under any conditions.
5. All office staff will be notified that the individual leaving ERT is no longer granted access (keys, combinations, passwords, and etc.) under any conditions.
6. The individual leaving ERT will be removed from all access lists.
7. The individual leaving ERT will turn in their keys, tokens, or cards that allow access to their supervisor or the security officer as part of terms of receiving their final paycheck.
8. All user accounts of the individual leaving ERT will be terminated, and if termination is initiated by ERT, all access to user accounts and personal data shall be discontinued prior to the workforce member being informed about the termination.
9. Any partners or entities that have access to protected health information will be notified to deny the terminated individual access.
10. **Data Controllers Overview**:

This procedure addresses the interactions between ERT and GDPR Data Controllers. GDPR Data Controllers include:

* **Clients**: Pharmaceutical companies,
* **Investigators**: physicians, clinics, hospitals, etc..
* **ERT**: where specified in the contract ERT may become the Data Controller.

ERT is considered a Data Processor, which is a person or organization that performs a function or activity involving the processing i.e. use or disclosure of personal data on behalf of a Data Controller, but is not part of the Data Controller’s workforce. Data Processors can be but are not limited to the following:

|  |  |
| --- | --- |
| * Claims processors or administrators | * Lawyers |
| * Billing Agencies | * Accountants |
| * Benefit managers | * Collection Agencies |
| * Consultants | * Medical Answering Services |
| * Clearing houses | * Temporary Staffing Agencies |
| * Storage Facilities | * Pharmacies |

When Data Processors are involved in the use or disclosure of personal data while performing a function on behalf of a Data Controller, they are expected to adhere to the same standards for safeguarding personal data as the Data Controller. Data Controllers are expected to assure that personal data is used and disclosed appropriately by entering into Data Privacy Agreements with all Data Processors, before the Data Processor is used..

## 15.1 Data Controllers Procedure:

1. ERT will sign a Data Privacy Agreement with all Data Controllers from which it receives or will receive personal data.
2. ERT will appropriately safeguard any personal data entrusted to our organization.
3. ERT will sign an agreement stating that we will not use or disclose personal data in any manner which would not be permissible for the Data Controller under GDPR.
4. ERT will:  
   1. Not use or further disclose personal data other than as permitted under the Data Privacy Agreement or as required by law.
   2. Use appropriate safeguards to prevent use or disclosure of personal data other than provided by the Data Privacy Agreement.
   3. Report to ERT’s and Data Controller’s DPO (or other designated official) any violation of use or disclosure as stated in the contract.
   4. Notify Data Controller of any unauthorized acquisition, access, use, or disclosure of Unsecured personal data held on Data Controller’s behalf, including the identity of each individual who is the subject of the Unsecured personal data breach (for more information, see Breach Notification Policy).
   5. Ensure that any subcontractors (sub Data Processors) to whom it provides personal data agree to the same restrictions.
   6. Upon request, provide a list of subcontractors (sub Data Processors) with their contact information that have been granted access to personal data to Data Controller’s DPO upon request (for more information, see GDPR Policy - Subcontractors).
   7. Maintain evidence that ERT’s workforce members and subcontractors have been trained in protecting personal data upon request to Data Controller’s DPO.
   8. Maintain a list of uses and disclosures of individual's personal data outside of treatment, payment, and healthcare operations and provide them upon request to help satisfy GDPRs right for individuals to request an accounting of personal data uses and disclosures (for more information, see GDPR Policy - Accounting of Personal Data Disclosures section).
5. All reported and/or discovered violations of a Data Privacy Agreement will be reported to the DPO.
6. **Subcontractors Overview**:

This procedure addresses ERT interactions with subcontractors (sub Data Processors). A subcontractor is a person or organization that performs a function or activity involving the use or disclosure of personal data, including electronic personal data, on behalf of ERT, but is not part of ERT’s workforce. Subcontractors can be but are not limited to the following:

|  |  |
| --- | --- |
| * Claims processors | * Lawyers |
| * Temp/Staffing Agencies | * Accountants |
| * Billing Companies | * Collection Agencies |
| * Consultants | * Record Storage Facilities |
| * Data Centers | * Aggregators |

ERT has adopted this policy to ensure that its subcontractors protect the personal data that they create, receive, transmit or maintain for or on behalf of ERT. Subcontractors of ERT are expected to adhere to the same standards for safeguarding personal data as ERT staff are. ERT will assure that personal data is used and disclosed appropriately by:

* Entering into Data Privacy Agreement to protect the security, integrity and confidentiality of personal data.
* Investigating when complaints or other credible evidence of violations by a subcontractor are received.
* Taking reasonable steps to correct a breach, notify the applicable Data Controller of the breach, and if necessary terminate the contract with a subcontractor after becoming aware of a material breach by the subcontractor.

**16.1 Related Section**:

Please reference the *Accounting and Disclosures* Section of this Policy.

## 16.2 Subcontractors Procedure:

ERT will obtain satisfactory assurances that the subcontractor will appropriately safeguard any personal data entrusted to it.

The subcontractor will sign a Data Privacy Agreement stating that it will not use or disclose personal data in any manner that would not be permissible under the GDPR or the agreement.

Subcontractor will:

* 1. Not use or further disclose personal data other than as permitted under the agreement or as required by law.
  2. Use appropriate safeguards to prevent use or disclosure of personal data other than provided by the agreement.
  3. Report to ERT’s DPO any violation of use or disclosure as stated in the agreement.
  4. Notify ERT of any unauthorized acquisition, access, use, or disclosure of Unsecured personal data they hold on ERTs behalf, including the identity of each individual who is the subject of the Unsecured personal data breach. For further information on reporting breaches of Unsecured personal data, please refer to ERT’s Breach Notification Policy.
  5. Ensure that any subcontractors to whom the subcontractor provides personal data agree to the same restrictions and execute a Data Privacy Agreement.
  6. Provide a list of subcontractors (along with their contact information) that have been granted access to personal data to ERT’s DPO.
  7. Provide proof that its employees and subcontractors have been trained in personal data.

All reported and/or discovered violations of Data Privacy Agreement will be recorded and maintained in a file with the signed agreement.

If ERT becomes aware of a pattern or practice of the subcontractor that constitutes a material breach or violation of the subcontractor’s obligations under its agreement, ERT will take actions (discussions with the subcontractor, sanctions, etc.) to cure the breach or to end the violation. If such steps are not successful ERT will terminate the agreement if feasible. If it is not feasible to terminate the agreement, ERT will report the problem to the applicable data controller for which the PERSONAL DATA belongs.

1. **Accounting of Disclosures Overview**:

Under GDPR, individuals have the right to request an accounting of personal data disclosures made by ERT on behalf of Data Controllers. As a Data Processor, in order to provide Data Controllers with the necessary information to respond to individuals’ requests for an accounting of personal data disclosures, ERT will have to track disclosures of individual’s personal data every time it is used outside of the project or staff requirements.

**17.1 Related Section**:

Please reference the Accounting and Disclosures Section of this Policy.

## 17.2 Accounting of Disclosures Procedure:

17.2.1 RIGHT TO AN ACCOUNTING OF DISCLOSURES

Individuals have the right to request an accounting of disclosures of personal data made by ERT for or on behalf of Data Controllers, except for disclosures:

* 1. To individuals of personal data about them;
  2. Pursuant to an authorization by the individual;
  3. Incident to an otherwise permissible or required use or disclosure;
  4. As part of a limited data set (data that does not include directly identifiable information), used for research, used for public health purposes;
  5. For a facility’s directory or to persons involved in the individual’s care;
  6. For national security or intelligence purposes;
  7. To correctional institutions or law enforcement;
  8. For a health care provider or plan’s treatment, payment or health care operations.

Each ERT workforce member has the responsibility to log disclosures of personal data that must be included in an accounting of disclosures. If a workforce member encounters any type of disclosure that must be included in an accounting of disclosures, the workforce member must log the disclosure in the appropriate Personal Information - Accounting of Disclosures form (DOC COR 014\_01). The form will be maintained in the individual’s file. This form will enable ERT to provide the individual or data controller with the following information regarding the disclosure:

* 1. Date of the disclosure;
  2. The name of the recipient;
  3. The address of the recipient, if known;
  4. A brief description of the information that was disclosed; and
  5. A brief statement of the purpose of the disclosure or a copy of the original request for information.

To request an accounting of disclosures, the individual, or a data controller on behalf of the individual, must submit a request to the DPO via an appropriate method.

The request should indicate in what form they want the list (for example, on paper or electronically). Any list they request will be free.

If the request is by an individual, ERT will notify the Data Controller in accordance with the applicable Data Privacy Agreement.

ERT will notify the individual or Data Controller of the cost involved prior to preparing the accounting so that they may choose to withdraw or modify their request at that time before any costs are incurred. If pursuant to the associated Business Associate Agreement ERT is responsible for providing an individual with an accounting, the individual must pay the applicable fee in full before they can obtain the requested accounting.

If pursuant to the associated Business Associate Agreement ERT is responsible for responding to an individual’s request for an accounting, we will respond within 30 calendar days. If additional time is needed, we will inform the individual or data controller within the 30 days in writing of the delay, the reason for the delay, and the date the accounting will be provided that will be no later than 60 days from the original request.

1. **Breach Notification Overview**:

This procedures section addresses the discovery and notification of breaches of Unsecured personal data.

## 18.1 Breach Notification Procedure:

IMPROPER USES/DISCLOSURES OF PERSONAL DATA

When any type of improper use/disclosure of personal data is discovered:

1. ERTwill notify the affected Data Controller in accordance with the applicable Data Privacy Agreement.
2. ERT will, if required by the applicable Data Privacy Agreement and to the extent possible, provide written documentation to the data controller including:
   1. The details of the improper use/disclosure of personal data.
   2. The likely impact and consequences of the breach;
   3. The date the improper use/disclosure of personal data occurred.
   4. The date the improper use/disclosure was discovered.
   5. A list of names and associated contact information for those individuals whose personal data was affected.
   6. What actions those individuals whose personal data was affected should take.
   7. What actions ERT are taking to mitigate the improper use/disclosure of personal data.
   8. Contact information for further information.

18.1.1 DETERMINING IF A BREACH HAS OCCURRED

1. Breach Defined.
   1. “Personal Data Breach” is defined to mean the acquisition, access, use, or disclosure of a patient’s *Unsecured personal data* in a manner not permitted pursuant to the GDPR that compromises the security or privacy of the personal data at issue.
   2. Impermissible uses or disclosures will be presumed to be a Breach unless ERT demonstrates that there is a low probability that the personal data has been compromised. ERT will consider the following factors (along with any other relevant considerations) to determine if personal data has been compromised:
2. The nature and extent of the personal data involved, including types of identifiers and the likelihood of re-identification;
3. The unauthorized person who used the personal data or to whom it was disclosed;
4. Whether the personal data was actually acquired or viewed; and
5. The extent to which the risk to the personal data has been mitigated.
   1. Personal data can only be breached if it is “Unsecured.” The Information Commissioners Office (“ICO”) has defined Unsecured personal data to mean personal data that has not been:
      1. Encrypted consistent with standards set by the National Institute for Standards and Technology (“NIST”); or
      2. Destroyed in a manner that renders the information irrecoverable, such as shredding for paper records. Thus, while GDPR does not require the use of encryption, encrypting personal data can significantly reduce the risk, such that a Data Controller will be required to provide notice of a Breach.
6. Exception to the Breach Definition. The following three situations are excluded from the definition of Breach:
   1. The unintentional acquisition, access, or use of personal data by any ERT workforce member or person acting under the authority of ERT, if such acquisition, access or use was made in good faith, within their scope of authority, and does not result in further use or disclosure in a manner not permitted by the Privacy Rule.
   2. The inadvertent disclosure of personal data by an individual otherwise authorized by ERT to access personal data to another workforce member of ERT, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under GDPR.
   3. An unauthorized disclosure of personal data where a workforce member ofERT has a good faith belief that an unauthorized person to whom personal data is disclosed would not reasonably have been able to retain the information.
7. De-identified Personal Data. If information is de-identified in accordance with GDPR,
8. It is not personal data and any inadvertent or unauthorized use or disclosure of such information will not be considered a Breach.
9. Breach Discovered. A Breach shall be treated as discovered by ERT on the first day on which the Breach is known, or by exercising reasonable diligence would have been known, to any member of ERT’s workforce (other than the individual(s) committing the Breach).

18.1.2 INTERNAL REPORTING OF SUSPECTED BREACHES

1. Any employee, officer, or subcontractor of ERT who has reason to believe that a Breach has occurred shall immediately report the suspected or actual Breach to ERT’s DPO. Unless otherwise set forth in an applicable Data Privacy Agreement, the report from a subcontractor shall be made orally within 24 hours of becoming aware of a suspected or actual Breach.
2. ERT’s DPO will initiate an assessment to:
   1. Evaluate the incident, and instruct employees, officers, or subcontractors on necessary actions to investigate the Breach,
   2. Consider the factors described above (along with any other relevant considerations) to determine if personal data has been compromised
   3. Determine how to advise individuals to protect themselves and prevent similar Breaches from occurring in the future.
   4. Prepare the required notifications of the Breach. The DPO shall coordinate with appropriate ERT management personnel and legal counsel to determine whether the Breach gives rise to any reporting obligations under state security breach reporting laws.

18.1.3 BREACH NOTIFICATION REQUIREMENTS

If it is determined that a Breach has occurred, ERT must undertake the following steps:

1. Except as otherwise required by the applicable Data Privacy Agreement, ERT will notify the affected Data Controller without unreasonable delay and in no case later than 30 calendar days after discovery of the Breach.
2. Our notification will include, to the extent possible, the following information:
   1. The details of the Breach.
   2. Whether the Breach involved secured or unsecured personal data.
   3. The likely impact and consequences of the breach;
   4. The date the Breach occurred.
   5. The date the Breach was discovered.
   6. A list of names and associated contact information for those individuals whose personal data was breached.
   7. What steps those individuals whose personal data was breached should take?
   8. What steps we are taking to mitigate the breach.
   9. Contact information for further information.
3. Support of the Data controller in addressing any breaches, will be executed as described in section IMPROPER USES/DISCLOSURES OF PERSONAL DATA Item 2.

**REVISION HISTORY**

|  |  |  |  |
| --- | --- | --- | --- |
| Version/  Revision | Date  Effective | Originator | Comments |
| 0 | 25MAY2018 | Chris Watson | Original Version |