



Jaeb Center for Health Research

HRPP 607: General Data Protection Regulation Operations

Version: 1.0

Author: Jeannie Perkins

Effective Date: 07 Feb 2020

15310 Amberly Drive, Suite 350

Tampa, FL 33647

(813) 975-8690

VERSION HISTORY

The following table outlines changes for this SOP:

VERSION NUMBER	AUTHOR	APPROVER	EFFECTIVE DATE	REVISION DESCRIPTION
1.0	Jennifer Caetano; Jeannie Perkins; James Pyner; Adam Glassman; Kellee Miller; Karalyn Hadley; Kelly Morillo; Roy Beck	Jeannie Perkins	07 Feb 2020	Integrated the GDPR operational requirements for JCHR implementation.

Contents

Version History	2
1. OVERVIEW	4
2. SCOPE.....	4
3. GDPR DEFINITIONS.....	4
4. GDPR OVERVIEW	6
4.1. When Does GDPR Apply as It Relates To JCHR?	6
4.1.1. What About Special Categories of Data?	7
4.2. When Doesn't GDPR Apply?	8
5. JCHR'S RESPONSIBILITIES UNDER GDPR	8
5.1. GDPR Principles	8
5.2. Rights of the Data Subjects	9
5.3. Managing and Auditing for Compliance.....	9
6. REQUIRED PD/PI ACTIONS	9
6.1. Vendor Qualifications	9
6.2. Requesting a Contract with an Institution Outside of the US	10
6.3. Obtaining a GDPR Determination	10
6.4. Managing an Amendment to GDPR-Related Activities	10
6.5. Creating GDPR Privacy Notice and Consents for the Data Subjects	11
6.6. Reporting a Possible Data Breach or Noncompliance With GDPR.....	11
6.7. Completion of GDPR-Related Primary Activities	11
7. RESEARCH COMPLIANCE COMMITTEE (RCC).....	12
7.1. Structure and Composition of the RCC	12
7.2. RCC Conflict Management.....	12
7.3. GDPR Function of the RCC.....	12
7.3.1. GDPR Monitoring and Oversight.....	13
7.3.2. Breach and Data Noncompliance Management	13
7.3.3. CAPAs	13
7.3.4. Data Subject Inquiry Management	13
7.3.5. GDPR Auditing	13
7.4. Retention of RCC Records.....	14
7.5. Other Applicable Policies and Procedures	14

1. OVERVIEW

This standard operating procedure (SOP) provides the processes and procedures for compliance with applicable provisions of the General Data Protection Regulation (GDPR) as they relate to the rights, confidentiality, privacy and security of data subjects and their personal data. The Jaeb Center for Health Research (JCHR) Protocol Directors/Principal Investigators (PD/Pis) are responsible for ensuring that their teams are following the processes and procedures specified herein to ensure compliance with GDPR privacy, security and data subject autonomy requirements.

2. SCOPE

The JCHR employees that are required to read and sign-off on this SOP no less than every three (3) years and as major changes are made to the contents herein:

- All Staff

3. GDPR DEFINITIONS

Anonymized Data: Information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable (i.e., it is impossible to identify a data subject).

Biometric Data: Personal data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data.

Consent: Any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

Controller: The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

Data Concerning Health: Personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.

Data Protection Officer (DPO): The DPO is involved in all issues relating to the protection of personal data, and shall maintain a level of independence in doing so. The main roles of the DPO are to (1) inform and advise JCHR and its employees who carry out processing of their obligations pursuant to the GDPR, (2) monitor compliance with the GDPR and the organization's applicable policies in relation to the protection of personal data through assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and audits as described herein, (3) provide advice where requested in regards the data

protection impact assessment and monitor its performance pursuant to Article 35, (4) cooperate with the supervisory authorities, as needed, and (5) act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matter.

European Economic Area (EEA): An international agreement which enables the extension of the European Union's single market to non-EU member parties (includes EU, Norway, Iceland, and Lichtenstein). All members of the EEA comply with GDPR, although GDPR only specifically references the EU.

European Union (EU): A political and economic union of 28 member states that are located primarily in Europe.

Genetic Data: Personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question.

General Data Protection Regulation (GDPR): Regulation 2016/679 is a regulation in EU law on data protection and privacy for all individual citizens of the European Union and the European Economic Area. It also addresses the transfer of personal data outside the EU and EEA areas. It was implemented 25 May 2018.

Personal Data: Any information relating to an identified or identifiable natural person ('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.

Personal Data Breach: means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Processing: Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Processor: A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

Profiling: Any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements.

Pseudonymization: The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

Representative: A natural or legal person established in the Union who, designated by the controller or processor in writing pursuant to Article 27, represents the controller or processor with regard to their respective obligations under this Regulation.

Special Categories: Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation.

NOTE: While most definitions have been taken directly from GDPR, the use of “z” has replaced the use of “s” in some instances to reflect the spelling used in the United States, however, these changes do not affect the use of the words herein (e.g., ‘organizational’ replaces ‘organisational’). Further, not all of the GDPR definitions are contained herein.

4. GDPR OVERVIEW

4.1. When Does GDPR Apply as It Relates To JCHR?

GDPR applies when JCHR will be involved in:

1. offering goods or services to **living** people in the EEA (this would be when JCHR is the Coordinating Center or Data Management for an EEA company’s research even if there are no EEA study participants or data - because the employees are themselves data subjects), or
2. monitoring the behavior of **living** people residing in the EEA (i.e., research with EEA study participants or their data).

Research falls under the scope of ‘monitoring behavior’ as it involves the processing of “personal data”. Remember that “personal data” is any piece of information that does, or **can be** used to, identify a live person living in the EEA (i.e., data subject), even if de-identified data is coming through another company in the EEA and they hold a code (e.g., JCHR is the statistical center).

It is important to note that a key stipulation of GDPR is that EEA data subjects are **profiled** participants of the research (or their data is profiled). However, if we are contracting with a company or organization that resides in the EEA, then we must still comply with applicable parts of GDPR, **even if** EEA data subjects and/or their data are not profiled.

The “processing” of personal data includes essentially anything that can be done with or to personal data (such as collecting, accessing, storing, organizing, combining, altering, retrieving,

disclosing, deleting, etc.). These provisions cover much more than what the Health Insurance Portability and Accountability Act (HIPAA) covers. Some examples of “personal data” include:

- Names
- Addresses (physical and virtual, such as IP Address)
- Identification Card Number
- Phone Numbers (and other contact information)
- Location Data (e.g., GPS)
- Demographic Information (unique enough to possibly identify a person)
- Health-Related Information (including biological samples)
- CVs/Biosketches, Financial Disclosure Forms, Employer, and/or Licenses

Notice that that last bullet would be information that we would get from investigators and their staff, independent contractors, vendors, etc. Under GDPR, even these individuals are considered data subjects and receive the same rights as study participants. However, as noted below in GDPR Principles, if JCHR would have a contract directly with one of these individuals, and if we are processing their data as necessary for the performance of that contract or to fulfill a legal obligation (e.g., to confirm qualifications), then JCHR would not need to obtain explicit consent. Otherwise, as in the case where the individual is not a party to the contract, but rather his/her employer is the party, then the PD/PI is responsible for obtaining a signed Research Personnel GDPR Privacy Notice and Consent to allow JCHR to obtain this information prior to each person’s assessment of qualifications. Since the processing of research personnel personal data does not change by protocol, JCHR may obtain one consent for general JCHR processing and should not need to obtain a new consent per protocol.

Even JCHR’s processing of coded data can fall under the requirements of GDPR. So, even when the data cannot be attributed to a specific person without additional information like a code key (i.e., pseudonymized data), the regulation still applies because there is a *possibility* or method available for that re-identification. This is true even though the additional information that would be necessary to re-identify is kept separately and securely.

If JCHR will process only “pseudonymized data” then the data subjects would have had to have already received notification of processing as part of the study consent process, before JCHR could process that data. If however, JCHR will process any “personal data” that is not pseudonymized, then the data subjects must provide actual consent for this processing in addition to providing consent for study participation. This additional notification and consent is similar to the process required of additional notification and authorization as it relates to HIPAA. The section below regarding “Rights of the Data Subjects” provides more information on these documents.

4.1.1. What About Special Categories of Data?

“Special Categories” of data can reveal racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data (includes samples), biometric data (includes images) for the purpose of uniquely identifying a natural person, *data concerning health* (much of what we collect) or data concerning a natural person’s

sex life or sexual orientation. In other words, essentially everything we do with qualifying EEA data subjects or their data will be in a special category because we are collecting health information by the very nature of what we do. When this data will be processed, the data subjects must have additional provisions included in the GDPR Privacy Notice and Consent (see the templates for more information).

4.2. When Doesn't GDPR Apply?

When no living people residing in the EEA (or their personal data) will be targeted for the research, and no EEA companies will be part of the research, then GDPR does not apply.

Also, if personal data from the EEA will be included, but it will be fully anonymized, then it wouldn't apply either. "Anonymized" is stricter than the de-identification methods implemented in the US under HIPAA provisions as it must mean that all direct (and indirect) identifiers have been removed in such a way as to make the identification of a person *impossible*. This means that anonymization is completely irreversible.

5. JCHR'S RESPONSIBILITIES UNDER GDPR

JCHR will typically be a "controller" as the JCHR protocol will determine the purpose and means of processing any "personal data" for research purposes (i.e., we are often the Sponsor and/or the prime recipient of funding to conduct a study). However, JCHR is also a "processor" as it provides Coordinating Center services to process "personal data" collected by other institutions that reside in the EEA. Regardless of which role will be primary to JCHR, the important take away is that JCHR must ensure (1) appropriate contracts are in place that cover the required provisions of data protections for EEA data subjects, and (2) the appropriate GDPR notice is provided to, and/or consent is obtained from, data subjects in the EEA. These two steps will demonstrate the "lawful basis" that is required for GDPR compliance as JCHR can only share EEA data subjects' "personal data" when it is a required part of our contractual obligations, and with adequate notice or consent to specific "personal data" processing (to obtain the data from the EEA in the first place).

Further, JCHR has the obligation to comply with the principles of GDPR, protect the rights of the data subjects; manage, document and audit processing, evaluate Personal Data Breaches, and report breaches to data subjects and agencies as applicable.

5.1. GDPR Principles

The general GDPR principles state that personal data shall be:

- Processed lawfully, fairly, and in a transparent manner
- Collected for specific, legitimate, and explicit purposes (and that additional processing can only be done if the additional purposes are compatible with the original purposes)
- The minimal necessary data to achieve purposes
- Accurate and kept up to date (with steps to address inaccurate data)
- Stored in accordance with a specified limit or end date
- Processed with integrity and confidentiality

5.2. Rights of the Data Subjects

The data subjects have the right to be notified of privacy and provide consent to processing regarding their rights, including:

- Contact details of the controller(s), Data Protection Officer(s), and representative(s) as applicable
- The categories of data to be processed
- From where the data will originate
- Why the data is needed for the study
- The legal basis for processing
- Who may receive the data and the categories of data they may receive
- Intent to transfer personal data outside of their resident country
- The data subject's right to:
 - Access, obtain copies, request rectification, and request erasure of personal data
 - Restrict or object to processing and/or withdraw consent
 - Make a complaint to the agency in their country and/or us
- Understanding any automated decision making (e.g., randomization, cohort assignment)
- Any secondary research purposes
- Personal data storage time limits

5.3. Managing and Auditing for Compliance

In order to ensure that the required principles have been applied, that the rights of the data subject are protected, and that compliance has been secured, the JCHR PD/PI must follow the “REQUIRED PD/PI ACTIONS” specified below.

A mechanism in place for ensuring that all applicable studies are in fact submitted to the JCHR Research Compliance Committee (RCC) will include the review by the DPO of every JCHR/Sponsor New Study and JCHR/Sponsor Amendment application submitted to the JCHR IRB. Any study that falls under GDPR will not be approved by the JCHR IRB until the study team has submitted the Determination Letter from the RCC.

During routine internal audits of GDPR applicable protocols, the DPO (or designee) shall review the correspondence, contracts, applicable protocol monitoring, GDPR Privacy Notice and Consents, and database access and privileges at a minimum.

6. REQUIRED PD/PI ACTIONS

6.1. Vendor Qualifications

When GDPR applies to a JCHR activity, JCHR must ensure that all of its vendors and contracts are compliant as they too are considered processors. Some specific questions have been incorporated into the templates of the SOP QM 107: Vendor Qualification to help support PD/PIs with the evaluation of vendors. The Quality Assurance team can also perform vendor qualifications to support the JCHR study teams. NOTE: If the vendor is not an independent contractor, and thus will not be a direct party to the contract, then any vendor employee that

JCHR will be obtaining personal data for (e.g., name, license, etc.), will have to sign the Research Personnel GDPR Privacy Notice and Consent to allow for that processing.

6.2. Requesting a Contract with an Institution Outside of the US

There are several regional and country specific regulations that need to be addressed in contracts and in consent forms. For this reason, it is imperative that the applicable teams at JCHR know when a proposal to include an entity in another country on study-related activities is being considered. The JCHR PD/PI must therefore clearly communicate by completing and sending the International Review Request Form {[LINK](#)} and the completed Personal Data Register {[LINK](#)} to the following email address *prior* to contract negotiations with international entities:

- RCC@jaeb.org

The RCC will use this information to support JCHR's understanding of and compliance with applicable regulations and laws, and the Contracts team will use this information to ensure that required elements of the Contracts Checklist are included (as well as any new elements added), as applicable. **NOTE: The form is required for all activities that propose working with a foreign entity (e.g., vendor, site, collaborator, etc.), not just an EEA entity.** If a protocol has started and the PD/PI would like to add additional vendors, collaborators, or establish sites in countries that were not assessed in the previous submission, then the PD/PI will be required to submit an additional International Review Request Form.

It is the responsibility of the PD/PI to obtain the applicable GDPR privacy notice and consents for all data subjects, whether they be human subject participants or research personnel (if they are not a direct party to the contract).

6.3. Obtaining a GDPR Determination

Prior to initiating contract negotiations or JCHR IRB new study submissions, the JCHR PD/PI must submit the International Review Request Form and all applicable attachments to the Research Review Committee (RCC). This form serves several purposes including enabling the RCC to monitor data processing, ensure adequate contract language implementation, and ensure provisions for adequate privacy notification and consent for data subjects. It further fulfills the requirement of a tracking mechanism of all data processing by protocol, for future audit and inspection (i.e., a register).

Additionally, the form and its attachments are reviewed by the RCC to allow the committee to perform additional required functions, such as confirming that all of the GDPR principles have been applied, and completing a Data Protection Impact Assessment (DPIA). If the RCC does not feel that all requirements and provisions have been met, the DPO or an RCC designee will work with the responsible PD/PI to achieve compliance. Once these tasks have been completed, the PD/PI will receive a Determination Letter from the RCC, which must be attached to the JCHR IRB New Study xForm. Any study that appears to fall under the scope of the GDPR will not be approved by the IRB if the RCC Determination Letter is not attached. The RCC also has provided a Data Flow Diagram Template {[LINK](#)} for PD/PI completion.

6.4. Managing an Amendment to GDPR-Related Activities

If an amendment to a protocol or other related materials changes the processing activities that were previously reviewed and accepted by the RCC, then another International Review Request Form submission must be made to the RCC with this updated information. A new RCC Determination Letter will be provided and must be submitted with the JCHR IRB Study Amendment xForm.

6.5. Creating GDPR Privacy Notice and Consents for the Data Subjects

Like with HIPAA, GDPR requires additional information beyond the general study consent be provided to people as applicable. For human subject participants, if personal data will be processed that is not completely pseudonymized, explicit consent must have been obtained in addition to the study consent. Further elements must be included when that personal data is in a sensitive category.

In addition, any data subjects providing personal data that are not direct parties to a contract (e.g., research personnel) must give consent via a GDPR privacy notice and signed consent before JCHR can process their personal data (e.g., CVs, licenses, financial disclosure information).

The GDPR Participant Privacy Notice and Consent Template {[LINK](#)}, and the GDPR Research Personnel Privacy Notice and Consent Template {[LINK](#)} include all required elements to guide the PD/PI with the successful incorporation as applicable. The tracked templates must be included with the International Review Request Form submission to the RCC. Remember that the research personnel can sign one consent for JCHR processing, and don't necessarily need to sign one for each protocol, since the processing is the same (i.e., assess qualifications).

NOTE: It is likely that a facility in the EEA will have their own template and/or need to translate the RCC-approved template. This is permissible so long as the JCHR PD/PI is still able to fulfill the obligations of the controller by (1) having a detailed process for how this will be done, (2) identifying a qualified individual to check the consent forms for accuracy, and (3) determining how the actual obtaining of the notice and consent will be monitored. These processes may be audited by the RCC as applicable, even if the study is not a US regulated study.

6.6. Reporting a Possible Data Breach or Noncompliance With GDPR

In accordance with the IT Operations Manual, if there is a suspected data or security breach, then the RCC shall be notified within twenty four (24) hours of JCHR's identification of the breach. The RCC will maintain a log of Security and Data Breaches reported and any corresponding corrective actions and responses provided. For more information on the management and reporting of a qualifying data breach, see SOP IT 406.1: IT Operations Manual.

6.7. Completion of GDPR-Related Primary Activities

When the primary processing of personal data is complete (e.g., only anonymized data, or pseudonymized data in accordance with original consent will be processed), then the PD/PI shall notify the RCC of the completion of primary activities. This can be done by simply emailing the RCC at RCC@jaeb.org. Additional information may be requested to process the completion and

a confirmation of closure will be sent. If at any time in the future other processing is being considered that was not initially approved, then the PD/PI must make an additional submission to the RCC for review and determination prior to initiating the new activities.

7. RESEARCH COMPLIANCE COMMITTEE (RCC)

7.1. Structure and Composition of the RCC

The Research Compliance Committee (RCC) consists of the Deputy Director, the Chief Information Officer (CIO), the Chief Research Compliance Officer (CRCO) fulfilling the role of Data Protection Officer (DPO), the Director and Deputy Director of Clinical Research Quality Assurance, the Software Quality Assurance Manager, the Clinical Research Quality Assurance Manager (QA Manager), and the Director of Grants and Contracts Administration. The RCC is responsible for the management and evaluation of research compliance at JCHR as a whole, but with a specific emphasis on General Data Protection Regulation (GDPR) compliance, as guided by the DPO.

The RCC meets monthly, or more frequently as applicable. Topics include quality and compliance-related issues, exploration of whether those issues present an increase in the likelihood or impact of risk areas, and how to best manage risk areas. The RCC shall have sufficient managerial, communication, and interpersonal skills to plan, implement, and assess research compliance and quality, with assistance from subject matter experts (e.g., legal). Members of the RCC also serve as the internal audit team and have the education, experience, and training to conduct internal audits. The audit team shall remain independent of the studies they audit. The auditors have the authority to document deficiencies found in their review of the systems and processes in place for conducting compliant clinical trials.

The organizational structure can be found in the JCHR Organizational Chart available at www.jaeb.org. The functional roles of JCHR staff can be found in Functional Descriptions of Project-Specific and General Oversight Positions at JCHR provided in the Quality Manual.

7.2. RCC Conflict Management

The RCC shall minimize bias where it could be presented based on dual roles. Where conflict is identified, such as when the Deputy Director is also the JCHR PD/PI on a study, he/she cannot be part of the team that audits that study and cannot review or sign-off on that audit as leadership. Further, the CRCO (functioning as DPO) reports to the Executive Director but the Executive Director cannot modify the salary of, conduct disciplinary actions against, or terminate the CRCO without the express approval of the Board of Directors. This structure allows the CRCO to perform the core roles of the position with the independence that those roles require, without fear of retaliation.

7.3. GDPR Function of the RCC

The Research Compliance Committee (RCC) is specifically responsible for management and oversight as it relates to General Data Protection Regulation (GDPR) requirements. The RCC shall meet as often as needed to perform GDPR Study Reviews, or evaluate any immediate threats to privacy, confidentiality, or security.

7.3.1. GDPR Monitoring and Oversight

International Review Request Applications shall be submitted to the RCC prior to the start of contract negotiations and JCHR IRB New Study submissions. The RCC shall not cause undue delay in making GDPR assessments. The RCC will document the assessments on the Data Protection Impact Assessment (DPIA) form {[LINK](#)}. The DPIA form is used to demonstrate the review of the principles of personal data processing, the GDPR privacy notice and consent appropriateness, and the management of risk, by protocol. Additional documentation may be found in the RCC Meeting Minutes. Once the DPIA has been completed, an RCC Determination Letter will be provided to the JCHR PD/PI.

7.3.2. Breach and Data Noncompliance Management

Any individuals that identify or become aware of a possible breach or data noncompliance will notify the RCC. The RCC shall log all notifications on the Breach and Data Noncompliance Log for tracking purposes. This log shall include responses and corrective actions. In the event that a data subject needs to be notified of a qualifying breach, the DPO will contact the data subject directly if JCHR has already processed the data subject's contact information as part of the study. If however, JCHR has not received this information as part of the original processing, it will not be requested by the DPO so that JCHR is not processing more personal data than is absolutely necessary (e.g., name and email address). In this circumstance, the DPO shall notify the Institution (processor) that established the original relationship with the data subject to collect personal data, and that institution will be responsible for notifying the data subject. All related correspondence shall be maintained by the RCC. For more information on the management and reporting of a qualifying data breach, see SOP IT 406.1: IT Operations Manual.

7.3.3. CAPAs

In accordance with SOP QM 103: Corrective and Preventive Actions, CAPAs will be required as needed to address and prevent issues.

7.3.4. Data Subject Inquiry Management

The DPR Group has been appointed by JCHR to serve as the Data Protection Representative as required by GDPR. In the event that a data subject contacts the DPR Group, they will notify the DPO within twenty-four (24) hours by emailing DPO@jaeb.org. The DPR Group shall only provide enough information to allow the DPO to assess the situation and respond accordingly. Such information shall include the study identifier (e.g., ABC123) as applicable, but shall not include any identifying information about the data subject if not absolutely necessary. Once a response is drafted by the DPO, the DPO shall provide the response to the DPR Group, who will then provide the response to the data subject. The DPR Group will continue to serve as the go-between until the issue is resolved so that JCHR is not processing more personal data than is absolutely necessary (e.g., name and email address). Responses shall be provided to the data subject within thirty (30) days. The RCC shall maintain a Data Subject Inquiry Log.

7.3.5. GDPR Auditing

In addition to internal audits of studies processing personal data, the RCC shall perform reviews of contracts, correspondence, and monitoring activities. Overall GDPR compliance will be evaluated no less than annually. The main forum for this annual evaluation will be the Annual Research Compliance Review. This review will include a review of applicable policies and procedures, IRB applications to confirm that all applicable studies were in fact submitted to the RCC, reviews of Breach and Data Noncompliance management, data subject inquiries, and reporting to agencies and data subjects. For more information, see the Quality Manual.

7.4. Retention of RCC Records

The RCC must maintain all relevant records for at least ten (10) years, or at least three (3) years after the completion of a specific research activity referenced therein (i.e., notification of closure), whichever is longer. The RCC may not destroy any materials without the written (e.g., email) confirmation of the DPO. The following is a list of some of the documents that are included in this retention:

- RCC meeting agendas and minutes
- Applications and supporting documents submitted for RCC review
- CAPA documentation
- Correspondence
- Policies and procedures
- RCC Checklists (DPIAs)
- Materials reviewed
- Determination letters

Records are accessible for inspection and copying by authorized representatives of regulatory agencies at reasonable times and in a reasonable manner.

7.5. Other Applicable Policies and Procedures

Data processing must be done in accordance with JCHR policies and procedures. For more information regarding how these policies and procedures related to GDPR, please refer the following:

- The HRPP Policy Manual
- The Quality Manual
- SOP CG 701: Elements of Standard Contracts
 - Attachment: Contracts Checklist
- SOP CT 201: Clinical Trial Management Overview and General Principles
 - Attachment: Foreign Sites in a Clinical Trial Instruction Guide
- SOP HR 502: Computing Policy Manual
- SOP IT 401.6: Data and File Protections
- SOP IT 401.7: Public Datasets
- SOP IT 401.8: Data Transfer
- SOP IT 405.1: Information Access Policy
- SOP IT 406.1: IT Operations Manual