****

***Document control sheet***

**Health Research Board – Data Subject Access Request Protocol**

|  |  |
| --- | --- |
| **Title:** | Data Subject Access Request Protocol |
| **Document Type:** | Protocol |
| **Reference/version no:**  | 1 |
| **Status:** | Final |
| **Last Updated:** | 12.04.2018 |
| **Sign-off by management team:** | Awaited |
| **Background:** | This policy applies to all HRB staff, service providers, contractors, Peer Reviewers, interns, agency workers and other persons engaged in activities relating to HRB on a permanent or temporary basis (hereinafter referred to as “Data Users”). |

**Data Subject Access Request Protocol**

1. **The purpose of this protocol**
	1. The Health Research Board (“**HRB**”) is firmly committed to complying with our data protection obligations. In this context, and to achieve consistency and excellence of service, we believe that it is important to set out a protocol which must be followed when dealing with a data subject access request.
2. **Right of access to personal data**
	1. Article 15 of the General Data Protection Regulation (EU Regulation 2016/679) (the “**GDPR**”) provides that any living individual about whom we hold personal data (a “data subject”) has a right to obtain **confirmation** as to whether or not their personal data is being processed, and, where that is the case;
		1. **Access** to (and a copy of) the personal data and
		2. The following information should be provided:
* A description of the **purposes** for which the data is held and processed;
* The **categories** of personal data held;
* A description of the **recipients** or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations. Where the personal data is transferred to third countries or international; organisations, the data subject has the right to be informed of the appropriate safeguards used for this transfer;
* Where possible, the envisaged **period** for which the personal data will be stored, or, if not possible, the criteria used to determine that period (i.e. the organisation’s Data Retention Policy);
* The existence of **other rights** such as the right to request rectification or erasure of their personal data or restriction of processing of their personal data or the right to object to such processing;
* The right to lodge a **complaint** with a supervisory authority;
* Where the personal data is not collected from directly the data subject, any available information as to the **source** of the data; and
* Information on the use of any **automated decision-making** by the organisation, including profiling and meaningful information about the logic involved, and the envisaged consequences of this for the data subject.
	1. Every individual about whom we keep personal information has a number of other rights under the GDPR, in addition to the Right of Access. These include:
* The right to have to have any inaccurate data rectified;
* The right, in certain circumstances, to have personal data erased (“right to be forgotten”);
* The right to restrict the processing of your personal data in certain circumstances;
* The right to data portability and to transfer your personal data to a third party;
* The right to object to the processing of your personal data;
* The right not to be subject to automated decision making including profiling;
* The right to receive notification of a data breach, where applicable; and
* The right to lodge a complaint to the Data Protection Commissioner.
1. **Making a data subject access request**

An individual making an access request must: -

* apply to us in writing;
* give any details which might be needed to help us identify him or her and locate all the information we may keep about him/her (e.g., previous addresses, client account numbers);

## What must we do in response to an access request?

* 1. Supply the information to the individual within **30 days** of receiving the request. This time limit begins to run immediately on receipt of the request and cannot be delayed for any reason, for example, while awaiting ID verification. While we cannot provide the information until we receive ID verification, if this is provided by the data subject on day 29 we must be in a position to provide the requested information on day 30 following receipt of the request. It is also essential to note that, having received the access request, we cannot change or delete any personal data which we hold.
	2. Provide the information in a form which will be clear to the ordinary person (e.g., any reference codes or identifying numbers et cetera must be explained).
	3. Ensure that we give personal information only to the individual concerned (or someone acting on his or her behalf and with their authority). For instance, do not provide such information by phone. If we do not keep any information on computer or in a relevant filing system about the individual making the request, we must tell them so within 30 days.

## Exceptions or limitations to the right of access

There are a number of restrictions upon the right of access which generally fall into six groups:

* Article 23 of the GDPR provides that the right of access may not apply in a number of cases, in order to strike a balance between the rights of the individual, on the one hand, and some important needs of civil society, on the other hand, such as the need to investigate crime effectively, and the need to protect the international relations of the State.
* The right of access to medical data and social workers' data is also restricted in some very limited circumstances, to protect the individual from hearing anything about himself or herself which might cause serious harm to his or her physical or mental health or emotional well-being.
* The right of access to examination results is modified slightly.
* The right of access does not include a right to see personal data about another individual, without that other person's consent. This is necessary to protect the privacy rights of the other person. Where personal data consists of expressions of opinion about the data subject by another person, the data subject has a right to that expression of opinion except where that expression of opinion was given in confidence.
* The obligation to comply with an access request does not apply where it is impossible for us to provide the data or where it involves a disproportionate effort.
* The right of access does not include documents subject to legal professional privilege which relate to advice received from our lawyers and documents created for the dominant purpose of being used in legal proceedings.
1. **Our procedure for data subject access requests**
	1. **Notify the DPO**:

Given the very strict time limits for compliance with a data subject access request, it is important that whoever first receives the request **immediately** notifies our Data Protection Officer (“DPO”).

Our DPO is: The Director of Corporate Operations

* 1. **DPO acknowledgment**:

On receipt of the data subject access request, the DPO will immediately reply to the request in writing (by email or letter - depending on the method of communication used by the data subject). This initial acknowledgement of the data subject access request should issue within 48 hours of receipt of the request. If we have any concerns as to the identity of the requestor it is important that the DPO is made aware of this and that he/she asks for further identifying details from the requestor before releasing any information.

* 1. **Diary Process**

At the same time as sending the initial response to the data subject, the date of expiry of the timeframe for delivery of a full response must be entered into the DPO’s diary.

We recommend that a DPO team diary is set-up so that everyone is aware of upcoming deadlines.

* 1. **Further Information**

The DPO may ask the data subject for more information to help us to locate the data sought.

* 1. **Information Collection**

Once the DPO is satisfied that a valid request has been made, she/he will liaise with the relevant people within HRB to carry out to the following:

1. full database search for all personal data sought;
2. if necessary, depending on the type of personal data sought, searches on individual Data Users ’ PCs/laptops; and
3. full hardcopy records search.

If requested to do so by the DPO, all of us within HRBmust do our utmost to comply with the time deadlines which she/he specifies. This will help us to respond quickly to data subject access requests and enable us to comply with our data protection obligations.

* 1. **Information Review**

Once the DPO has gathered all of the information set out above, she/he will review all of the documents to identify any personal data contained therein and will extract any personal data relevant to that data subject only. Under no circumstances should personal data belonging to a third party be released to the data subject. If a document consists of personal data belonging to a number of data subjects, this document will be redacted, and any third-party personal data removed.

The DPO will then fill in the template table (Appendix 1) setting out what personal data is being released and specifying what personal data, if any, is being retained and the relevant exemption of the DPA relied upon to refuse access.

S(he) will then issue a complete table and a covering letter to the data subject, including a copy of the relevant data, in readable format.

In order to identify the types of data that are being requested on a regular basis, the DPO will maintain a log of the data subject access requests to assist us in identifying how we can improve our processes.

* 1. **Release to the Data Subject**

The DPO will fill in a template letter to the data subject; enclose a copy of the proposed data and the table of documents referred to at item 6 above.

Date:

Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**APPENDIX 1**

**DSAR Schedule of Redactions**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **No** | **Description** | **Date** | **Page(s)** | **Reasons for Redactions** |
|  |  |  |  | e.g. Third Party details redacted |
|  |  |  |  | e.g Collateral history redacted  |
|  |  |  |  |  |
|  |  |  |  |  |