DATA PROTECTION PROCEDURES FOR HANDLING REQUESTS FOR ACCESS TO RECORDS

June 2019

Contents

Contents

Procedure for Dealing with Subject Access Requests (SARs)

From the 25th May 2018, both electronic and manual records fall within the access regime outlined in the GDPR and Irish Data Protection Acts 1988 to 2018

1. When a Data Protection (DP) request arrives in the Executive

Data Protection requests are the responsibility of existing DP Decision Makers. When a DP request arrives in a department, it must be sent to the appropriate Decision Maker immediately and a copy sent to the appropriate Consumer Affairs Office.

Upon receipt of the DP request the Decision Maker's staff will:

- **Date stamp the request**; this will be Day 1 of the request.
- Open a file for the request.
- Log the request and record all correspondence with the data subject.
- Enter on the file the deadline for the decision -i.e. 1 month from date of receipt.
- Check that the request comes within the definition of personal data.
- Check that the request contains sufficient information to identify the records being sought.
- After initial examination, if it becomes clear that there is insufficient information to identify the records involved, the Decision Maker should contact the Data Subject, preferably by phone, fax or e-mail in order to clarify the request.
- As the request refers to personal information ensure that the Data Subject has included appropriate identification to establish who they are. Where a request is made by a third party (e.g. parent/guardian) suitable information to confirm that the person making the request is legally permitted to do so must also be included

2. Insufficient information to identify the records requested

If having offered all reasonable assistance, the request remains too vague and the Executive has used all reasonable measures to verify the identity of a data subject who requests access, it will have no option but to refuse the request. (In the case of a complaint to the Data Protection Commissioner, it will be important to have clearly documented evidence of all steps taken in processing the request.)

The Decision Maker shall notify the Data Subject of the Executive's decision in such circumstances. The Decision letter should be copied to the appropriate DDPO/Consumer Affairs Area Office.

3. The Decision Maker should identify and assemble all records covered by the request. They will:

- Identify all records both electronic and manual which contain information (records) which fall under the scope of the request.
- Initiate a search for records stored electronically on the PC Network/Server and other IT media e.g. scanned records. All such documents held in an IT environment should be printed and should be entered chronologically in the file.
- Source and retrieve all manual records covered by the request.
- Aim to complete this work within 7 days from the time the request has been received by the Executive.

- All actions should be logged as well as any other relevant details
- The Decision Maker shall document:
  - the effort involved in finding the records;
  - the locations searched;
  - names of those contacted with regard to locating files;
  - Outcome of any discussions;
  - Details of hours involved.

Once all the records have been assembled the Decision Maker should:

- Number all records chronologically beginning at the back of the file with record number 1. Numbers should be written in the top right hand comer using a black pen.
- Copy all records once numbering is completed
- If access to records or portions of records are being refused, identify the reasons why access is being refused/redacted.

4. When a Request relates to more than one area of the Executive

Each individual area will respond directly to the data subject regarding the SAR relevant to their area.

5. Preparing records for release

Every reasonable attempt should be made by the Executive to suit the individual's wishes regarding access. Normally, Data Subjects seek a copy of the records and these should be issued by registered post.

Staff should be conscious of the quality of records and ensure that photocopies are legible. Particular attention should be paid to handwritten text on records, which are to be photocopied. Material, which is considered to be non disclosable under the regulation, should be redacted.

6. Records which relate to a third party

Having compiled the relevant records the Decision Maker must identify the records, which include the personal information of any person other than the Data Subject and the personal information must be redacted.

7. Restriction of right of access

Individuals have a right of access to their personal data. However, Article 23 of the GDPR states that Member States(individual countries) may restrict by law certain access rights where the restriction is necessary to safeguard:

a) national security;
b) defence;
c) public security;
d) the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;

e) other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation a matters, public health and social security;
f) the protection of judicial independence and judicial proceedings;
g) the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions;
h) a monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority in the cases referred to in points (a) to (e) and (g);
i) the protection of the data subject or the rights and freedoms of others;
j) the enforcement of civil law claims.

Such restrictions are legislated for under the Data Protection Act 2018 and subsequent Regulations under that Act.

8. Restrictions on access to medical data and social work data

The Data Protection (Access Modification) (Health) Regulations, 1989 (S.I. No. 82 of 1989) provide that health data relating to an individual should not be made available to the individual, in response to an access request, if that would be likely to cause serious harm to the physical or mental health of the data subject. A person who is not a health professional should not disclose health data to an individual without first consulting the individual's own doctor or some other suitably qualified health professional.

Equally, the Data Protection (Access Modification) (Social Work) Regulations, 1989 (S.I. No. 83 of 1989) provide that information constituting social work data shall not be supplied by or on behalf of a data controller to the data subject concerned in response to a request if it would be likely to cause serious harm to the physical or mental health or emotional condition of the data subject.

9. Internal consultation

When a request is received for a file which contains records of a client under the care of a health professional e.g. Medical or Psychiatric Consultant, Psychologist, Social Worker etc., the Decision Maker shall consult, if necessary, with the relevant professional.

If a professional certifies that release of the information would be damaging to the Data Subject, the Decision Maker must refuse release.

10. When some or all requested records are not held by the Executive

If the records requested refer to another organisation which is or may be, in the opinion of the Decision Maker, a Data Controller (see definitions), the Decision Maker must advise the Data Subject of their right to apply to that organisation directly.

11. Records held by individuals/organisations under 'contract for services'

Where information/personal data is held by another organisation funded by the HSE (e.g. Section 38/39 agencies), any application under the GDPR should be made, by the Data Subject, to that organisation.

12. Final Review

The data subject is entitled to know whether or not their personal data is being processed. Where personal data concerning the individual in question, who has made a subject access request, is being processed, a copy of their personal information should be supplied to that individual along with other additional information as follows:

- Purpose(s) of the processing;
- Categories of personal data;
- Any recipient(s) of the personal data to whom the personal data has or will be disclosed, in particular recipients in third countries or international organisations and information about appropriate safeguards;
- The retention period or, if that is not possible, the criteria used to determine the retention period;
- The existence of the following rights –
    - Right to rectification
    - Right to erasure
    - Right to restrict processing
    - Right to object – and to request these from the controller.
    - The right to lodge a complaint with the DPC
- Where personal data is not collected from the data subject, any available information as to their source;
- The existence of automated decision making, including profiling and meaningful information about how decisions are made, the significance and the consequences of processing.

It is a requirement of the GDPR that information must be provided in an intelligible format. It is therefore strongly recommended that all service areas prepare a glossary of terms, including abbreviations and acronyms commonly used, which individuals cannot reasonably be expected to understand, and that can be supplied as a 'standard' document with relevant SAR responses.

If a thorough search has been conducted and it has been found that no personal information about the individual exists, then the Decision Maker should write to the individual to advise this. The letter should explain the extent of the investigations, particularly the involvement of any other areas within the HSE. It is essential that a rigorous process is followed before a negative response is given.

13. Right of complaint to the Data Protection Commissioner

There is no provision for Internal Review of the decision of the Executive, any person may complain to the Data Protection Commissioner about the way their request was handled or any other matter. The Commissioner's address is:
info@dataprotection.ie

Canal House
Station Road Portarlington
Co. Laois
Ph: 057 8684800

14. Contact Details

Deputy Data Protection Officer West, (excluding voluntary agencies) **Consumer Affairs, Merlin Park University Hospital, Galway.** • **CHO 1 – Cavan, Donegal, Leitrim, Monaghan, Sligo** • **Community Healthcare West – Galway, Mayo, Roscommon** • **Mid-West Community Healthcare – Clare, Limerick, North Tipperary.** • **Saolta Hospital Group**	Email: ddpo.west@hse.ie Phone: 091-775 373
Deputy Data Protection Officer Dublin North-East (excluding voluntary hospitals and agencies) **Consumer Affairs, HSE Dublin North East, Bective St., Kells, Co Meath.** • **Midlands, Louth, Meath Community Health Organisation** • **Community Health Organisation Dublin North City & County** • **CHO 6 – Dublin South East, Dublin South & Wicklow** • **RCSI Hospital Group** • **National Children's Hospital**	Email: ddpo.dne@hse.ie Phone: Kells Office: 046-9251265 Cavan Office: 049-4377343
Deputy Data Protection Officer Dublin mid-Leinster (excluding voluntary hospitals and agencies) **Consumer Affairs, HSE, Third Floor Scott Building, Midland Regional Hospital Campus, Arden Road, Tullamore, Co. Offaly.** • **Dublin Midlands Hospital Group** • **Ireland East Hospital Group** • **Community Healthcare Dublin South, Kildare & West Wicklow**	Email: ddpo.dml@hse.ie Phone: Tullamore Office: 057-9357876 Naas Office: 045-920105
Deputy Data Protection Officer South (excluding voluntary hospitals and agencies) **Consumer Affairs, HSE South, Ground Floor East, Model Business Park, Model Farm Road, Cork. Eircode: T12 HT02** • **Cork & Kerry Community Healthcare** • **CHO 5 – Carlow, Kilkenny, South Tipperary, Waterford & Wexford** • **UL Hospital Group** • **South South-West Hospital Group**	Email: ddpo.south@hse.ie Phone: Cork Office: 021 – 4928538 Kilkenny Office: 056 -7785598.

Glossary of Terms

As with any legislation, certain terms have particular meaning. The following are some important definitions:

Data means information in a form, which can be processed. It now includes both automated data and manual data.

GDPR means General Data Protection Regulation

Automated data means, broadly speaking, any information on computer, or information recorded with the intention of putting it on computer.

Manual data means information that is kept as part of a relevant filing system, or with the intention that it should form part of a relevant filing system.

Relevant filing system means any set of information that, while not computerised, is structured by reference to individuals, or by reference to criteria relating to individuals, so that specific information relating to a particular individual is readily accessible.

Personal data means data relating to a living individual who is or can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of the data controller

Processing means performing any operation or set of operations on data, including:

- obtaining, recording or keeping the data,
- collecting, organising, storing, altering or adapting the data,
- retrieving, consulting or using the data,
- disclosing the information or information by transmitting, aligning, combining, blocking, erasing or destroying the data.

Data Subject is an individual who is the subject of personal data.

Data Controller is a person or entity who, either alone or with others, controls the contents and use of personal data.

Data Processor is a person who processes personal information on behalf of a data controller, but does not include an employee of a data controller who processes such data in the course of his/her employment.

Sensitive personal data relates to specific categories of data which are defined as data relating to a person's racial origin, political opinions, religious or other beliefs, physical or mental health, sexual life, criminal convictions or the alleged commission of an offence and trade union membership.