INPDR data retention policy

File name: INPDR data retention policy

	Name	Title	Signature	Date
Author	Conan Donnelly	Registry Manager		6th March 2020
Reviewer				
Authoriser				

Effective Date	6th March 2020
Review Date	

Version	Date	Author	Changes
0.1	6th March 2020	Conan Donnelly	

Introduction to Data Retention and the obligations and requirements of INPDR:

The Data Protection Act 1998 states that Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes". Similar provision is made in Article 5 of the General Data Protection Regulation. Personal data may also be retained if there is a separate statutory obligation to do so - for example, employment law requires records to be kept of hours worked and holidays taken.

It is clear that different data has different specific purposes and retention periods, such as medical research records, or financial data that is subject to audit.

Data cannot be retained just because we want to keep it or that we may possibly have some unspecified use for it in the future. Failure to preserve records for long enough or retaining personal data beyond the necessary period creates risks for INPDR, its staff and its service users. These include:

- Risks of non-compliance with legal obligations, including data protection, working time, health & safety, Revenue, etc;
- Flawed decisions, based on out-of-date and inaccurate data;
- Increased storage costs and greater security risks;
- Greater effort and difficulty in responding to data subjects' requests for access to copies of their data.

Aims/Objectives:

- To ensure INPDR complies with legislative requirements
- To clarify the types of records maintained and the type and location of their storage
- To stipulate the length of time data of each type will be retained
- To document roles and responsibilities within the organisation

Guidelines:

INPDR processes large amounts of Sensitive Personal Data relating to Niemann Pick Disease patients.

INPDR also processes a variety of other Personal Data relating, for example, to its own staff and the health professionals with whom it works.

INPDR may also process information on Data Subjects' religious, ethnic, ideological or Trade Union affiliations, by virtue of storing information on the organisations of which the Data Subjects are members.

Destruction of Personal Data on expiry of retention period:

INPDR will engages in a robust destruction policy. Personal Data and organisational data of all types that is no longer required will be efficiently and verifiably destroyed.

January of each year is designated INPDR's "Data Management Month".

During this month the following tasks will be performed:

- This policy document and each Section Retention Schedule will be reviewed and updated as required.
- The respective data owners will identify Personal Data requiring deletion.
- The Data Protection Officer will monitor the deletion/destruction of Personal Data.
- Hard-copy records may be destroyed using the services of an approved 3rd party service provider.
- Electronic records are reviewed on a regular basis and deleted once the term of the relevant retention period has expired.
- Organisation of shared folders will be reviewed and updated.
- A record of data destruction will be maintained for verification purposes.

Destruction of paper records

- Documents will be shredded at the relevant INPDR location and disposed of in a secure manner by INPDR's own staff using, if necessary, a reputable agency to assist in same. Records will not be taken offsite for destruction.
- A record will be kept on the date of destruction and the reputable agency who will dispose of the data will provide a certificate of compliance with Data Protection Obligations.

Destruction of end-of-life computer storage media (Compact Discs, Hard Disc Drives, External Storage devices, USB memory sticks, end-of-life equipment, etc.)

- When the media or equipment concerned have reached the end of their useful lives, they will be destroyed in house and disposed of in a secure manner using a reputable agency to assist in same. Computer equipment and storage media will not be taken offsite for destruction.
- A record will be kept on the date of destruction and the reputable agency who will dispose of the data will provide a certificate of compliance with Data Protection Obligations

Deletion of computer-based records

- This could be information stored in a structured way, such as the patient information management system; or unstructured data, such as correspondence saved as word processor files, or as attachments to or in the body of emails.
- These records will be deleted in accordance with the relevant retention periods above, depending on the nature of the Personal Data concerned.
- If INPDR is unable to delete an individual record for technical reasons the Data Subject's details will be anonymised.
- Great care must be taken to keep track of any backups made of Personal Data and the media used - for example, removable media such as tapes or external disc drives, or cloud-based backup services - to ensure these records are also only retained for as long as required and that any copies of data are properly deleted or destroyed when their retention periods have expired.

Roles and Responsibilities:

The Data Protection Officer will monitor the implementation of this policy. Appropriate staff members will be designated owners of categories of data and these designations will be recorded in the Personal Data Inventory. They will be responsible for identifying data to be destroyed and reporting new types of Personal Data that INPDR may from time to time begin collecting.

Related Policies and Documents:

- INPDR Data Protection Policy
- INPDR Data Subject Rights Policy
- INPDR Personal Data Breach Management Policy
- INPDR Personal Data Breach Incident Log
- INPDR Personal Data Inventory

End of document