INPDR Data Protection Policy

File name: INPDR Data Protection 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	

INPDR Data Protection Policy

Introduction:

The purpose of this document is to provide a concise policy statement regarding the Data Protection obligations of the International Niemann Pick Disease Registry (INPDR). This includes obligations in dealing with Personal Data, in order to ensure that the organisation complies with the requirements of the relevant UK legislation, principally the Data Protection Act 1998 and the General Data Protection Regulation.

Rationale:

INPDR must comply with the Data Protection principles set out in the relevant legislation. This policy applies to all Personal Data collected, processed and stored by INPDR in relation to NPD patients, its staff, and suppliers or service providers in the course of its activities. INPDR makes no distinction between the rights of Data Subjects who are employees, and those who are not. All are treated equally under this policy.

Scope:

The policy covers both Personal and Sensitive Personal Data held in relation to Data Subjects by INPDR. The policy applies equally to Personal Data held in manual and automated form.

All Personal and Sensitive Personal Data will be treated with equal care by INPDR. Both categories will be equally referred to as Personal Data in this policy, unless specifically stated otherwise.

This policy should be read in conjunction with:

- The Data Subject Rights policy;
- The Personal Data Retention Policy and related Retention Periods List;
- The Data Protection Impact Assessment template;
- The Engaging Data Processors Policy;
- The Personal Data Security Policy
- The Personal Data Breach Management Policy;
- Procedures and standards for securing and encrypting Personal Data stored on portable equipment and removable storage media;
- INPDR's entry on the ICO Public Register.

INPDR as a Data Controller:

In the course of its daily organisational activities, INPDR acquires processes and stores Personal Data in relation, for example, to:

- NPD patients;
- Employees;
- Suppliers.
- Users / External researchers

In accordance with the legislation, Personal Data must be acquired and managed fairly. Not all staff members will be expected to be experts in data protection legislation. However, INPDR is committed to ensuring that all of its staff members who handle Personal Data have sufficient awareness to anticipate and identify a Data Protection issue, and to ensure that should an issue arise, the Data Protection Officer is informed, and appropriate corrective action is taken.

Due to the nature of the functions carried out by INPDR, there is regular and active exchange of Sensitive Personal Data between INPDR and healthcare service providers relating to their NPD patients.

This policy provides the guidelines for this exchange of information, as well as the procedure to follow in the event that a INPDR staff member is unsure whether such data can be disclosed. In general terms, the staff member should consult with the Data Protection Officer to seek clarification.

Any formal, written request by a Data Subject for a copy of their Personal Data (a Subject Access Request) will be referred, as soon as possible, to the Data Protection Officer, and will be processed as soon as possible.

It is intended that by complying with these guidelines, INPDR will adhere to best practice regarding the applicable Data Protection legislation.

In the course of its role as Data Controller, INPDR engages a number of Data Processors to process Personal Data on its behalf. In each case, a formal, written contract is in place with the Processor, outlining its obligations in relation to the Personal Data, the specific purpose or purposes for which it is engaged, and the understanding that it will process the data in compliance with Data Protection legislation.

The Data Protection Principles:

The following key principles are set out in the UK and European legislation and are fundamental to the INPDR data protection policy.

In its capacity as Data Controller, INPDR ensures that all data shall:

1. Be obtained and processed fairly and lawfully.

For data to be obtained fairly, the Data Subjects must, at the time the data are being collected, have readily available to them:

- The identity of the Data Controller (INPDR);
- The purpose(s) for which the data is being collected;
- The person(s) to whom the data may be disclosed by the Data Controller;
- Any other information that, in the specific context, is necessary so that the processing may reasonably be considered fair.

INPDR will meet this obligation in the following way.

- The informed consent of the Data Subject will be sought before their data is processed;
- INPDR will ensure that collection of the data is justified under one of the other lawful processing conditions – for example, for medical purposes, performance of the INPDR's functions conferred under law and in the public interest, legal obligation, contractual necessity, etc.;
- Where required, the informed consent of the Data Subject will be sought before their data is processed;
- Processing will be carried out only as part of INPDR's legitimate activities, and will safeguard the rights and freedoms of the Data Subject;
- The Data Subject's data will not be disclosed to a third party other than to a party contracted to INPDR and operating on its behalf, except where required or authorised by law or where patient consent has been obtained.

2. Be obtained only for one or more specified, legitimate purposes.

INPDR will obtain data for purposes which are specific, lawful and clearly stated. Data Subjects will have the right to question the purpose(s) for which INPDR holds their data, and INPDR will be able to clearly state that purpose or purposes.

INPDR's contracts with Data Processors will ensure that should a Data Processor cease to trade, the data concerned will be returned to INPDR in its entirety, to ensure its safety, as well as continuity of service provision within the terms of the specified purpose.

3. Not be further processed in a manner incompatible with the specified purpose(s).

Any use of the data by INPDR will be compatible with the purposes for which the data was acquired.

4. Be kept safe and secure.

INPDR will employ high standards of security in order to protect the Personal Data under its care. This applies equally to all data, whether directly under the control of INPDR or being processed on its behalf by Data Processors.

Appropriate technological and procedural security measures will be taken to protect against unauthorised access to, alteration of, destruction, or disclosure of all Personal Data held by INPDR. The specific measures to be employed will be kept under regular review having regard to the development of technology, the evolving nature of INPDR's activities and the changing nature of security risks.

The measures used will cover the securing of data on INPDR's internal systems, on hosting service providers' systems, in transit between INPDR and other entities, especially entities from which patient data is obtained or shared with, as well as the use and deployment of external storage devices such as smartphones, tablet computers, USB sticks and CDs.

INPDR will ensure that it is kept aware of the identities of any hosting service providers or other sub-contractors who may be used by Data Processors to process Personal Data and the physical location of all copies of data. As part of data sharing agreements, Data Processors will be contractually required to inform INPDR in advance of any proposed changes to these arrangements and afford it an opportunity to register any objections or concerns it may have.

5. Be kept accurate, complete and up-to-date where necessary.

INPDR will:

- ensure that administrative and IT validation processes are in place to conduct regular assessments of data accuracy;
- Conduct periodic reviews and audits to ensure that relevant data is kept accurate and up-to-date;
- Conduct regular assessments in order to establish the need to keep certain Personal Data.

6. ***Be adequate, relevant and not excessive in relation to the purpose(s) for which the data were collected and processed.***

INPDR will ensure that the data it processes in relation to Data Subjects are relevant to and sufficient for the purposes for which those data are collected. Data which are not relevant to such processing will not be acquired or maintained. The same principle will apply with regard to provision of data to outside organisations for research purposes, i.e. the data provided will be proportionate to, and not go beyond, the requirements and validity (in terms of methodology and expectation of outputs) of the research.

7. ***Not be kept for longer than is necessary to satisfy the specified purpose(s).***

INPDR will identify a matrix of Personal Data categories, with reference to the appropriate data retention period for each category. The matrix applies to data in both a manual and automated format.

Once the relevant retention periods have elapsed, INPDR undertakes to verifiably destroy, erase, irreversibly anonymise, or otherwise put this data beyond use.

8. ***Be managed and stored in such a manner that, in the event a Data Subject submits a valid Subject Access Request, seeking a copy of their Personal Data, this data can be readily retrieved and provided to them.***

INPDR has implemented a Subject Access Request procedure by which to manage such requests in an efficient and timely manner, within the timelines stipulated in the legislation.

Data Subject Access Requests

All data subjects, including patients and INPDR staff, have the right of access to data which have been collected concerning them.

There are specific timescales within which INPDR must respond to the Data Subject, depending on the nature and extent of the access request. These are outlined in the Subject Access Request process document.

INPDR staff will ensure that all such requests are forwarded to the Data Protection Officer, who will be responsible for processing them in an efficient and timely manner. It should be noted that before health related data is provided in response to an access request, the appropriate health professional must be consulted and the data must not be provided if the treating clinician considers it would be likely to cause serious harm to the physical or mental health of the data subject.

Registration

INPDR is among the categories of Data Controller required to register with the ICO.

INPDR'S registration details will be reviewed by the Data Protection Officer for completeness and accuracy at least annually on the registration renewal. In addition, data protection impact assessments of new projects will include checks that the processing envisaged is within the scope of the registration description, and if necessary amending the registration before commencing any new types of Personal Data processing.

It should be borne in mind that it is an offence under the Data Protection Acts for a registered Data Controller to process Personal Data in any way which is not within the scope of its registered details.

Implementation

As a Data Controller, INPDR ensures that any entity to which the processing of Personal Data on its behalf is sub-contracted (a Data Processor) does so in a manner compliant with the Data Protection legislation, in particular with regard to the obligations to safeguard such data from unauthorised disclosure, alteration or destruction, or any other unlawful processing.

Failure of a Data Processor to manage INPDR's data in a compliant manner will be viewed as a breach of contract, and may be pursued through the courts.

Failure of INPDR staff to process Personal Data in compliance with this policy may result in disciplinary proceedings.

Definitions

For the avoidance of doubt, and for consistency in terminology, the following definitions will apply within this Policy.

Data	includes both automated and manual data. Automated Data means data held on computer, or stored with the intention that it will be processed on computer. Manual Data means paper-based data that is processed as part of a relevant filing system, or which is stored with the intention that it will form part of a relevant filing system.
Personal Data	any information relating to an identified or identifiable living individual; 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.
Sensitive Personal Data	Personal Data relating to: racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, mental or physical health, sexual life, commission or alleged commission of a crime, and information relating to criminal prosecutions, whether the accused was acquitted or convicted, biometric data, genetic data.
Data Controller	a legal or natural person who, either alone or with others, determines the purpose and means of the processing of Personal Data;
Data Subject	an individual who is the subject of Personal Data, i.e. to whom the data relates either directly or indirectly.
Data Processor	a legal or natural person who processes Personal Data on behalf of a Data Controller on the basis of a formal, written contract. This

	definition does not include employees of the Data Controller, processing such Data in the course of their employment.
Data Protection Officer	a legal or natural person appointed by INPDR to monitor compliance with the appropriate Data Protection legislation, to deal with Subject Access Requests, and to respond to Data Protection queries from staff members and service recipients
Relevant Filing System	Any set of information in relation to living individuals which is not processed by means of equipment operating automatically (computers), and that is structured, either by reference to individuals, or by reference to criteria relating to individuals, in such a manner that specific information relating to an individual is readily retrievable.