INPDR Personal Data Breach Policy

File name: INPDR Personal Data Breach 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

The purpose of this document is to provide a concise policy to be followed in the event that INPDR becomes aware of a loss of personal data. This includes obligations under law namely the General Data Protection Regulation (GDPR).

Rationale

The response to any breach of personal data can have a serious impact both on the persons whose data has been affected and on INPDR'S trust and reputation.

The consequential impact of a major data breach can be immeasurable. For INPDR, in particular, loss of access to patient data could prevent it from performing its functions. Therefore, exceptional care must be taken when responding to data breach incidents. Not all data protection incidents result in data breaches, and not all data breaches require notification. This procedure is intended to assist staff in developing an appropriate response to a data breach based on the specific characteristics of the incident.

Scope

The policy covers both personal and sensitive personal data held 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 associated INPDR Data Protection Policy and supporting documents listed below.

- INPDR'S top-level Data Protection Policy
- INPDR'S Data Subject Rights Policy
- INPDR'S Personal Data Retention Policy
- INPDR'S Personal Data Breach Incident Log
- INPDR'S procedures and standards for securing and encrypting Personal Data stored on portable equipment and removable storage media;
- Breach Notification Guidance, Information Commissioners Office (https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/)

What constitutes a personal data breach?

A personal data breach is defined in the GDPR as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed".

Examples of incidents which might result in a breach include:

- Loss of a laptop, memory stick or mobile device that contains personal data
- Lack of a secure password on PCs and applications
- Emailing patient data to someone in error
- Leaving employee files unsecure
- Sharing system login names and passwords
- Failure of a door lock or some other weakness in physical security which compromises personal data

What happens if a breach occurs?

Actual, suspected, or potential breaches must be reported immediately to INPDR'S Data Protection Officer (DPO). ***Any employee who becomes aware of a likely data breach and fails to notify the DPO may be subject to INPDR'S disciplinary procedure.***

A team comprising the DPO and other relevant staff will be established to assess the breach and determine its severity. Depending on the risks to the Data Subjects affected, the ICO, relevant regulatory bodies and, if necessary, the data subjects will be informed as quickly as possible following detection.

INPDR will then implement changes to procedures, technologies or applications to prevent a recurrence of the breach. Consideration should also be given to informing other organisations which may be able to help prevent or mitigate harm or loss to the data subjects, such as the Police, financial institutions, etc.

When will the Office of the ICO be informed?

Personal data breaches must be reported to the ICO in accordance with the ICO guidance (https://ico.org.uk/for-organisations/report-a-breach/). The assessment of the risks arising from a breach should be made by the DPO. Where, for example, the personal data concerned is encrypted to a high standard of security and it is certain that the relevant encryption passwords or keys remain secure, it can be concluded there is no risk of unauthorised disclosure and that therefore no risk to the persons whose data is affected arises. Such incidents should still, however, be recorded on the incident log.

Where the breach may give rise to a high risk to the rights and freedoms of the data subjects, they must be informed directly and without undue delay of the loss of their data. The principle is that each data subject should have the opportunity to consider the consequences of the loss of his or her data individually and the measures he or she wishes to take in response. To assist them in this, INPDR will provide them with its assessment of the risk to their privacy and make recommendations to the data subjects which may minimise the risks to them.

The initial report describing the circumstances must be made to the ICO without undue delay and where feasible within 72 hours of INPDR becoming aware of the incident. Where a report is not made within 72 hours, an explanation for the delay must also be provided to the ICO.

If the IPO decides to request a more detailed written report, it will expect the report to cover at least the following points:

- *the amount and nature of the personal data that has been compromised;*
- *the action being taken to secure and / or recover the personal data that has been compromised;*
- *the action being taken to inform those affected by the incident or reasons for the decision not to do so;*
- *the action being taken to limit damage or distress to those affected by the incident;*
- *a chronology of the events leading up to the loss of control of the personal data;*
- *and the measures being taken to prevent repetition of the incident.*

Data Loss Incident logging

All data breaches will be recorded in an incident log. The log will maintain a summary record of each incident which has given rise to a risk of unauthorised disclosure, loss, destruction or alteration of personal data. The record will include a brief description of the nature of the incident.

Even incidents in which it was decided not to report the matter to the data subjects or the ICO - for example, if an encrypted email attachment containing personal data was sent to the wrong person - should be logged. In such cases, an explanation must be logged as to why the incident was deemed not to be reportable. Such records will be provided to the ICO upon request.

In every instance, reportable or not, a review along the lines outlined above should be carried out with particular emphasis on the prevention of similar future incidents and ensuring the implementation of the necessary actions arising.

Definitions

“Data Subject” means a living individual who is the subject of the Personal Data, i.e. to whom the data relates either directly or indirectly.

“Personal Data” means 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, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

End of Document