|  |  |
| --- | --- |
| **TITLE** | The MedLIS Policy on Management of a MedLIS Data Protection Breach |
| **DOCUMENT NUMBER** | ML-BOP-22 |
| **APPROVED BY** | See Q-Pulse |
| **APPROVAL DATE** | 12th April 2021 |
| **EFFECTIVE DATE** | 14th April 2021 |
| **REVIEW DATE** | See Q-Pulse |
| **AUTHOR (S)** | Susan Kelly |
| **REVIEWED BY** | Dr. Miriam Griffin |

**Document Revision History:**

|  |  |  |
| --- | --- | --- |
| **Version No.** | **Date** | **Summary of Changes** |
| **1.0** | **27/09/2019** | **Maintained off-line** |
| **2.0** | **Apr 2021** |  |
| **3.0** |  |  |
| **4.0** |  |  |

**Table of Contents:**

[1.0 Introduction 4](#_Toc69307832)

[1.1 Definitions 4](#_Toc69307833)

[2.0 Identification of a MedLIS Breach 5](#_Toc69307834)

[3.0 Notification of a MedLIS Breach 6](#_Toc69307835)

[4.0 Possible Data Protection Incident or Breach? 7](#_Toc69307836)

[5.0 Data Protection Breach Form 7](#_Toc69307837)

[6.0 Data Protection Incident or Breach 7](#_Toc69307838)

[7.0 Containment and Recovery 7](#_Toc69307839)

[8.0 Compile risk Assessment 8](#_Toc69307840)

[9.0 Large scale or highly sensitive Breach 8](#_Toc69307841)

[10.0 Notifying data subjects 9](#_Toc69307842)

# Introduction

The purpose of this document is to provide guidance on the process that must take place should an incident or breach occur either within the MedLIS system or externally by a third party data processor.

‘**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. Under the General Data Protection Regulation (GDPR), all personal data breaches must be reported to the Data Protection Commissioner with 72 hours of first becoming aware of the breach. The process flow map for the process is shown at the end of this guidance document.

## 1.1 Definitions

**DPO:** Data Protection Officer – Monitor GDPR compliance

**DDPO:** Deputy Data Protection Officer – they are the regional managers in Consumer Affairs and cover the DPO role for HSE organisations. They will inform and provide advice to staff about the data breach process.

**Data Subject Person:** The person whom the personal data relates to. Will be notified of the breach if necessary.

**DPC:** Data Protection Commissioner – The data protection regulator

**Relevant Manager**: The manager of the member of staff who first becomes aware of the incident/ Breach.

**Identifier**: Any member of staff who first becomes aware of the incident.

**Authorisation / Authorised:** Official approval and permission to perform a particular task.

**Breach of Information Security:** The situation where confidential or restricted information has been put at risk of unauthorised disclosure as a result of the loss or theft of the information or, through the accidental or deliberate release of the information.

**Confidential information:** As defined by Irish data protection Law and the GDPR. Information which is protected by Irish and/or E.U. legislation or regulations, MedLIS organisations policies or legal contracts. The unauthorised or accidental disclosure of this information could adversely impact MedLIS, its patients, its staff and its business partners. Some examples of confidential information include:

* Patient / client / staff personal data (Except that which is restricted) Patient /client / staff medical records (Except that which is restricted) Unpublished medical research
* Financial data / budgetary Reports
* Service plans / service performance monitoring reports Draft reports
* Audit reports
* Data covered by Non-Disclosure Agreements Passwords / cryptographic private keys
* Data collected as part of criminal/HR investigation/incident reports.

**Information:** Any data in an electronic format that is capable of being processed or has already been processed.

**Line manager:** The individual a user reports directly to.

**Personal Information:** Information relating to a living individual (i.e. Staff, or patient or client) who is or can be identified either from the information or from the information in conjunction with other information. For example: - an individuals’ name, address, email address, photograph, date of birth, fingerprint, racial or ethnic origin, physical or mental health, sexual life, religious or philosophical beliefs, trade union membership, political views, criminal convictions etc.

# Identification of a MedLIS Breach

All MedLIS users should be aware of who to report a MedLIS breach to should they have to report such a breach or incident. Early recognition and reporting of breaches is essential to ensure a timely response to the incident/ minimise the damage that the incident can cause and ensure that the 72 hr time limit for reporting to the DPC is achieved.

MedLIS has also procured the auditing software P2Sentinel that Cerner provides. This auditing solution tracks access to confidential patient data in Cerner Millenium.

P2Sentinel is a third-party application to Cerner Millennium that records audit event logs of access to patient information and activities of Cerner Millennium users. Reports include low level detail such as user details, patient information and event types which describe the actions performed by the user (View, Open Chart, Search etc). Access to the P2Sentinel application is managed by the MedLIS Back Office team and is not currently available to resources external to this team. Data is retained on the servers and is never archived or deleted. Access to scheduled monthly reports is restricted to authorised personnel which typically sit within Health Information Management Services. Ad hoc requests can be placed and must be approved in writing by the organisations authorised person. All requests must be logged through the MedLIS back office.

Reports Audit reports can be provided in one of two ways:

1. Scheduled monthly reports

• Several reports are generated monthly containing the previous months audit data

• Reports are saved to local secure share drive for authorised users to retrieve

• Reports are filtered by user location and provided to relevant site

• Scheduled reports are provided for:

Excessive person searches by Hour

Failed Logins

Same Last Name as Patient

Same Name as Patient

2. Ad hoc requests

• Any user can request an ad hoc report specific to a user, a patient or a combination of both

• All requests must be approved by site specific authorised personnel

• Reports are saved to local secure share drive for the requester to retrieve



# Notification of a MedLIS Breach

Your organisations DPO as well as the MedLIS manager for your organisation must be notified of the potential breach and will have to sign the Data Breach Incident Report form. Your line manager will be informed and any immediate action required will be decided upon. The local MedLIS manager will inform the national MedLIS back office manager who can suspend access to the system for that particular user until further investigation has been carried out.

It is the responsibility of the organisations DPO to manage a breach that is incurred by a third party processor. The third party data processor has a responsibility to complete the External Data Breach Incident Report form and return it immediately to the organisations DPO. The relevant manager will then follow the process below.

# Possible Data Protection Incident or Breach?

Your organisations DPO will identify if the incident in question is potentially a data protection breach or incident. If it is definitely not a data protection incident or breach no further action is needed. If you organisations DPO or designated data protection manager identifies the incident as a data breach then a data protection breach form must be completed.

# Data Protection Breach Form

Data breach incident forms are available from <https://www.hse.ie/eng/gdpr> and should be completed as soon as possible when the incident is verified. All of the sections on the form must be completed by the staff member who identifies the incident and their line manager. The form must be sent to their DPO (DDPO for HSE organisations) and also, in the event of an information systems security breach, to the OoCIO.

# Data Protection Incident or Breach

Your DPO or the HSE DDPO will decide if it is a data protection Incident or a Data Protection Breach and advise accordingly.

**Incident**

Data Protection Incident should be logged with your organisations DPO or the DDPO in the case of the HSE organisations. Corrective actions should be advised. The incident should also be recorded by HR department. The users line manager should liaise with the DPO/ DDPO and in consultation with him/her, advise of corrective action that should be made to prevent the incident recurring. Implementing of corrective actions should be carried out as soon as possible. The users line manager should also log the incident and ensure the corrective actions are implemented and any additional actions implemented that were advised by the DPO/ DDPO

**Breach**

The Data Protection Breach should be logged by your DPO/ DDPO and corrective actions advised. The DPO/ DDPO should log the breach with the DPC and advise of any corrective actions that have taken place.

# Containment and Recovery

The users line manager should try to recover any data or file that has been compromised to mitigate as much risk as possible. Containment involves limiting the scope and impact of the breach of data/information. While the relevant manager must take the lead, advice and guidance is available from the DPO/ DDPO and OoCIO.

The DDPO will:

• Establish who needs to be made aware of the breach and inform them of what they are expected to do to assist in the containment and recovery exercise. For example, communication dept. Gardaí, management team etc.

The line manager should:

• Establish whether there is anything that can be done to recover losses and limit the damage the breach can cause. For example, changing access codes to server rooms or medical records libraries/ examining physical access etc.

• Implement the changes prescribed by the DDPO

The OoCIO will:

 • Have a role in containment and recovery from an information systems point of view. For example, this might entail isolating a compromised section of the network or remotely wiping a mobile device.

# Compile risk Assessment

In assessing the risk arising from the data breach to the data privacy rights and freedoms of the data subject, the relevant manager should, in consultation with the DPO/ DDPO consider what would be the potential adverse consequences for individuals, i.e. how likely it is that adverse consequences will materialise and, in the event of materialising, how serious or substantial are they likely to be.

In assessing the risk, the following points should be considered:

• What type of information/data is involved?

• How sensitive is the information/data?

• Are there any security mechanisms in place (e.g. password, protected, encryption)?

• What could the information/data tell a third party about the individual?

• How many individuals are affected by the breach?

• Have all of the data subjects affected by the breach been identified and are their contact details available?

• Is the breach likely to adversely affect the data privacy rights and freedoms of the data subjects concerned?

# Large scale or highly sensitive Breach

If the breach affects a large number of people or significantly poses a risk to the rights and freedoms of the data subjects involved then the DPO/ DDPO should escalate the issue to the DPC. If not, the DPO/ DDPOs should give instruction to the local relevant managers on corrective actions and how to prevent the breach from happening in the future.

# Notifying data subjects

The relevant manager, following a discussion with the DPO/ DDPO, should notify the data subjects as appropriate and should, in clear and plain language (written or verbal):

•Outline what has occurred with their personal data and apologise for the incident;

•Provide name and contact details for further information;

•Describe the likely consequences of the personal data breach;

•Describe the measures taken or proposed to be taken by the relevant manager to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects;

•Confirm that the DPC has been notified of the breach;

•Record notification to data subject.

**Please note; Data Protection Breaches have to be reported to the Data Protection Commissioner. In that regard the Area Consumer Affairs/Regional Consumer Affairs officers are the only HSE officers designated to report a breach to the Data Protection Commissioner. See below details of same**

