Data Breach Policy

Policy	
Applies to:	All staff & stakeholders
Date Issued:	07/03/2023
Status	Ratified
Version	2.0
Date for Review	07/03/2025

Document Change Record

Version	Date	Author	Status	Comment
1.0	01/10/2020	Philip Angell	Issued	Initial Version
2.0	07/03/2023	Philip Angell	Issued	Full review and change to Disciplinary section

Contents

1 Background

Data security breaches are increasingly common occurrences whether caused through human error or via malicious intent. As the amount of data and information grows and technology develops, there are new ways by which data can be breached. The Organisation needs to have in place a robust and systematic process for responding to any reported data security breach, to ensure it can act responsibly and protect personal data which it holds.

2 Purpose

The aim of this policy is to standardise Medical Clinics Limited's (the Organisation) response to any data breach and ensure that they are appropriately logged and managed in accordance with the law and best practice, so that:

- incidents are reported swiftly and can be properly investigated
- incidents are dealt with in a timely manner and normal operations restored
- incidents are recorded and documented
- the impact of the incident is understood, and action is taken to prevent further damage
- the ICO and data subjects are informed as required in more serious cases
- incidents are reviewed, and lessons learned

3 Definition

Article 4 (12) of the General data protection Regulation ("GDPR") defines a data breach as:

"***a breach of security leading to the unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed."***

The Organisation is obliged under the GDPR to act in respect of such data breaches. This procedure sets out how the Organisation will manage a report of a suspected data security breach.

The aim is to ensure that where data is misdirected, lost, hacked or stolen, inappropriately accessed or damaged, the incident is properly investigated and reported, and any necessary action is taken to rectify the situation.

A data security breach can come in many forms, but the most common are as follows:

- Loss or theft of paper or other hard copy

- Data posted, e-mailed or otherwise sent to the incorrect recipient
- Loss or theft of equipment on which data is stored
- Inappropriate sharing or dissemination – staff accessing information to which they are not entitled
- Hacking, malware or data corruption
- Information is obtained by deception
- Equipment failure, fire or flood
- Unescorted visitors accessing data
- Non-secure disposal of data

In any situation where staff are uncertain whether an incident constitutes a breach of security, either report it to the Data Protection Officer (DPO), the Senior Information Risk Owner (SIRO), or your line manager. If there are IT issues such as the security of the network being compromised, IT should be informed immediately.

4 Scope

This Organisation-wide policy applies to all Organisation information, regardless of format, and is applicable to all officers, members, visitors, contractors, partner organisations and data processors acting on behalf of the Organisation.

5 Applicability

This policy is applicable to and designed for use by all staff.

6 Responsibilities

Information Users

The GDPR applies both to Data Controllers (the Organisation itself) and to Data Handlers. Therefore, all information users are responsible for reporting actual, suspected, threatened or potential information security incidents and for assisting with investigations as required, particularly if urgent action must be taken to prevent further damage.

Managers

Line Managers are responsible for ensuring that staff in their area act in compliance with this policy and assist with investigations as required.

Lead Responsible Officers

Lead responsible officers (DPO, SIRO and IG lead) will be responsible for overseeing management of the breach in accordance with the Data Breach Management Plan

(See Appendix a). Suitable further delegation may be appropriate in some circumstances.

7 Reporting a Breach

Internal

Suspected data security incidents / breaches should be reported promptly to the DPO as the primary point of contact on 01273 030733, email Philip.angell@nhs.net.

The report must contain full and accurate details of the incident including who is reporting the incident, and what classification of data is involved. The Data Breach Report Form should be completed as part of the reporting process. Once a data breach has been reported an initial assessment will be made to establish the severity of the breach.

All data security breaches will be centrally logged by the DPO to ensure appropriate oversight in the types and frequency of confirmed incidents for management and reporting purposes.

External

Article 33 of the GDPR requires the Organisation as a data controller to notify the ICO only when the breach is likely to result in a risk to the freedoms and rights of natural persons. Such a breach also must be communicated to the data subject (with certain exceptions). Notification must be made without undue delay and within 72 hours of becoming aware of it. If the Organisation fails to do so, it must explain the reason for the delay.

Article 33(5) requires that the Organisation must maintain documentation on data breaches, their nature and remedial action taken.

A report to the ICO must contain information to the nature of the breach, categories of data, number of data records, number of individuals affected, name and contact details of the DPO, likely consequences of the breach and action taken.

8 Data Breach Management Plan

The Organisation's response to any reported data security breach will involve the following four elements:

A. Containment and Recovery

B. Assessment of Risks

C. Consideration of Further Notification

D. Evaluation and Response

Each of these four elements will need to be conducted in accordance with the checklist. An activity log recording the timeline of the incident management should also be completed.

9 Disciplinary

Officers, members, contractors, visitors or partner organisations who act in breach of this policy may be subject to disciplinary procedures or other appropriate sanctions.

Depending on the severity and frequency of data breaches caused by responsible individuals the organisation has defined punitive measures for these offenses:

1. Redo the IG course on Educare
2. Meeting with line manager to discuss improving data protection awareness & IG course Educare
3. Meeting with Senior management and HR to discuss ongoing issue + IG course educare
4. Meeting with Senior management and HR to implement improvement plan, follow up meetings to ensure a change in behaviour
5. Official warning

These measures will only be employed in situations where the breaches were avoidable and not when there were no possible steps, on the part of the individual, to prevent the breach.

The organisation encourages a blame free culture and as such multiple offenses are required to move to the more severe reprimands. It is always a worse offence to purposely not report a breach than cause the breach itself. The IG Committee believes in transparency around processes and as such has made this list of measures available to all employees. This is so all employees are aware of what is expected of them.

10 References

- The GDPR

  https://gdpr-info.eu/

Appendix a – Data breach management plan

See Data Breach Flow Chart

Data Breach identification for end users: