Data Security and Protection Breaches Incident Reporting Procedure

Policy Created: March 2021

Last Reviewed: August 2026

Next Review: August 2027 (or sooner if significant changes in legislation, guidance, or organisational activities occur)

Reviewed by: Laurence Clark

Responsible Officer: Liam Vernon (Data Security and Protection Lead)

Approved by: CEO

Main Contact for Queries: info@pathwaysassociates.co.uk

1. Introduction

Pathways Associates CIC has a responsibility to ensure that any data security breach or information governance incident is reported, investigated and managed quickly and effectively. When a breach involves personal data and creates a risk to the rights and freedoms of an individual, UK GDPR requires Pathways to assess the incident and, where necessary, report it to the Information Commissioner's Office (ICO).

Because Pathways delivers some services under NHS contracts, we also use the Data Security and Protection Toolkit (DSPT) Incident Reporting Tool when required by contract or commissioner expectation. However, Pathways is **not part of the NHS**, and therefore only reports incidents to NHS Digital or the Department of Health and Social Care (DHSC) when contractually required or when DSPT guidance explicitly applies.

This procedure explains how staff, volunteers, contractors and partner organisations must record, report and support the investigation of any data security or protection incident. It forms part of Pathways' wider incident reporting process and supports our commitment to safe, lawful and transparent handling of personal information.

Pathways keeps a record of all personal data breaches, whether or not they require notification to the ICO. These records are maintained by the Information Governance (IG) Team.

Pathways is **not subject to the Network and Information Systems (NIS) Regulations 2018**, and therefore does not report incidents under that legislation.

2. Purpose

The purpose of this procedure is to ensure that all data security and protection breaches are reported consistently, investigated appropriately and managed in line with UK GDPR, the Data Protection Act 2018, DSPT requirements and Pathways' contractual obligations.

This procedure applies to all Pathways employees, volunteers, contractors and any third party authorised to process data on behalf of Pathways.

3. Definitions

Personal Data Breach

A personal data breach is any security incident that results in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data. Under UK GDPR, a breach is considered reportable when it creates a **risk to the rights and freedoms of an individual**, not only when data is accessed by an unauthorised person.

Personal Data

Personal data is any information relating to an identifiable living person. This includes names, contact details, identification numbers, location data, online identifiers, and any information relating to physical, psychological, social or economic identity.

Special Category Data

Special category data includes information relating to racial or ethnic origin, political opinions, religious beliefs, trade union membership, genetic data, biometric data, health, sex life or sexual orientation. For breach reporting purposes, Pathways also treats information relating to vulnerable adults or children, criminal convictions, communicable diseases, sexual health and mental health as special category data.

Types of Breach

Breaches fall into three categories: Confidentiality breaches involve unauthorised access or disclosure. Integrity breaches involve unauthorised alteration of data. Availability breaches involve loss of access or destruction of data.

4. Roles and Responsibilities

Chief Executive Officer

The CEO has overall responsibility for ensuring that Pathways has effective systems for reporting and managing data security incidents.

Data Security and Protection Lead

The Data Security and Protection Lead provides advice on grading and categorising incidents, supports investigations and acts as the point of contact for the ICO when a breach requires notification.

Senior Information Risk Owner (SIRO)

The SIRO reviews incidents, ensures senior oversight and confirms any external reporting required under DSPT or contractual obligations.

Information Governance Team

The IG Team coordinates investigations, maintains the incident log, liaises with the Data Security and Protection Lead, SIRO and IT, and ensures lessons learned are recorded and acted upon.

IT Services

IT Services alert the IG Team when a cyber-security or technical incident occurs and support investigation and remediation.

5. Data Security Breach / Incident Investigation Process

All staff must report any suspected or actual data security incident **as soon as it is discovered**, even if they are unsure whether it qualifies as a breach. Reports must be made to the IG Lead, Data Security and Protection Lead or IG Team immediately.

Once reported, the incident is logged and assessed using Pathways' risk-grading process. Incidents are graded based on the severity of potential harm to individuals and the likelihood of that harm occurring. Grading focuses on the impact on the individual, not the organisation.

If the incident poses a **high risk to the rights and freedoms of an individual**, Pathways must notify the ICO within **72 hours** of becoming aware of the breach. This may also require notification through the DSPT Incident Reporting Tool if contractually required.

Pathways must also notify affected individuals when the breach is likely to result in significant harm, such as identity theft, fraud, discrimination, reputational damage or financial loss.

Some incidents may not require ICO notification if effective containment measures remove the risk. Examples include encrypted data, recovery from a trusted partner or situations where Pathways can nullify the impact.

All incidents, whether notifiable or not, are recorded in Pathways' incident log.

6. Reporting

Pathways includes a summary of notifiable incidents in its annual governance reporting when required by contract or commissioner

expectation. Incidents reported through DSPT may be shared by NHS Digital with other national bodies for monitoring and trend analysis. Pathways therefore ensures that no identifiable personal information is included in DSPT submissions.

Data security incidents are also reported to the Information Governance Group for oversight, discussion and learning.

7. Lessons Learned

Lessons learned from incidents are shared with staff through briefings, training and internal communications. Staff involved in incidents may be required to complete additional training or receive further support. The IG Team ensures that lessons learned inform updates to policies, procedures and training materials.

8. Training and Awareness

This procedure is available to all staff and published on the Pathways website. All staff, including temporary and contracted workers, must comply with UK GDPR, the Data Protection Act 2018, the NDG Data Security Standards and the common law duty of confidentiality. Annual Data Security Awareness training is mandatory for all staff.

9. Monitoring and Review

Performance is reviewed annually and used to inform future improvements. This procedure is reviewed every two years or sooner if required due to legislative changes, new guidance, significant incidents, emerging vulnerabilities or organisational changes.

Appendix: Guide to Notification of Data Security & Protection Incidents

Likelihood that an adverse effect has occurred

No.	Likelihood	Description
1	Not occurred	There is absolute certainty that there can be no adverse effect. This may involve a reputable audit trail or forensic evidence.
2	Not likely, or any incident involving vulnerable groups even if no adverse effect occurred	This must be selected when there is no evidence proving that no adverse effect has occurred.

No.	Likelihood	Description
3	Likely	It is likely that an adverse effect will occur as a result of the breach.
4	Highly likely	There is almost certainty that an adverse effect will happen at some point in the future.
5	Occurred	There is a reported occurrence of an adverse effect arising from the breach.

If the likelihood is low and the incident is not reportable to the ICO, no further details are required.

Severity of the adverse effect on individuals

No.	Effect	Description
1	No adverse effect	There is absolute certainty that no adverse effect can arise from the breach.
2	Potentially some minor adverse effect, or any incident involving vulnerable groups even if no adverse effect occurred	Selected when there is no absolute certainty. Minor adverse effects may include inconvenience or cancellation of a procedure without additional suffering.
3	Potentially some adverse effect	May include release of confidential information causing embarrassment or preventing someone from doing their job, such as a cancelled procedure that prolongs suffering but does not cause a decline in health.
4	Potentially pain and suffering or financial loss	There has been reported suffering, decline in health, financial detriment, loss of funds or loss of employment.
5	Death or catastrophic event	A person dies or suffers a catastrophic occurrence.