BrisDoc Patient care by people who care

NHS

Data Breach Notification Procedure

Version:	Owner:	Created:
1.1	Dr Kathy Ryan (Medical Director)	1st February 2022
Published:	**Approving Director:**	**Next Review**
1st February 2022	Nigel Gazzard (Managing Director)	1st February 2024

Contents

Introduction

Whilst we are committed to protecting the personal data of all individuals there will always be a risk of a data breach.

If there are occurrences of any of the following, they must be notified immediately on discovery to Caldicott Guardian Dr Kathy Ryan and/or IG Lead Deb Lowndes.

- Loss of any personal data.
- Destruction of any personal data other than when authorised by our Records Management Policy, due to the personal data being outside our retention policy.
- Unauthorised disclosure of personal data.
- Corruption of personal data.
- Unauthorised access to personal data.
- Unauthorised alteration of personal data.

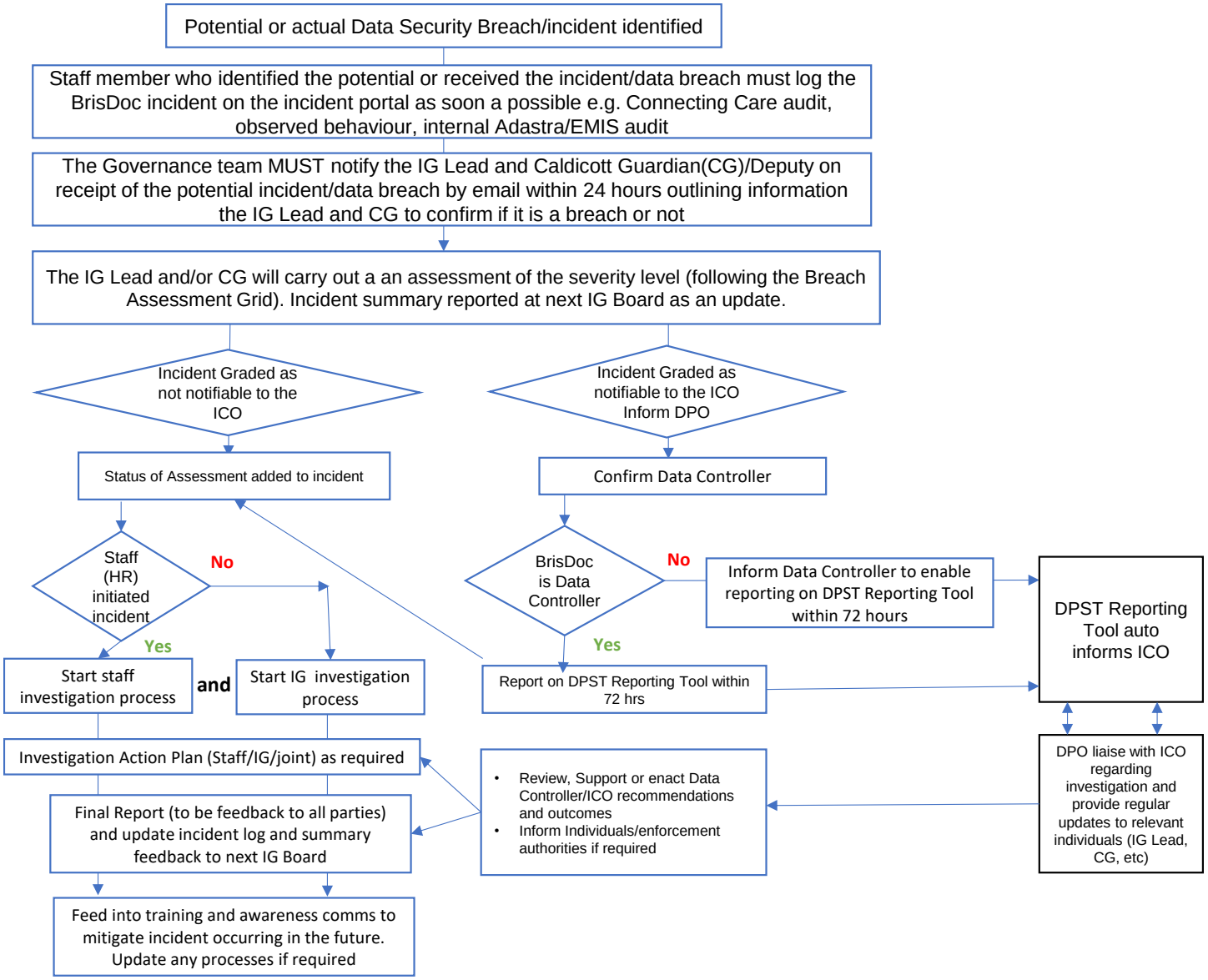
On receipt of notification the following steps will be taken by Caldicott Guardian Dr Kathy Ryan and/or IG Lead Deb Lowndes:

- The board of directors and our DPO will be notified.
- Consideration will immediately be given to the extent of the breach and the risk to any individual will be assessed. A report will be written as to the findings.
- A decision will be taken as to what steps can be taken to mitigate the effects of the breach.
- The report will be provided to the board of directors.
- If the breach is likely to result in a high risk of adversely affecting the data subject's rights and freedoms the data subject will be notified without delay. If it is decided not to notify the data subject a record will be made of the decision and the reasons for making the decision. The record will be made in the Data Breach Register.
- If the data breach is likely to result in a risk to rights and freedoms of the data subject the Information Commissioner will be notified without undue delay and not later than 72 hours of becoming aware of the occurrence of the data breach. If it is decided not to make a report to the ICO a record will be made of the decision and the reasons for making the decision in the Data Breach Register.

Reporting a Breach

This document should be circulated to all staff so that they can easily identify a breach and be aware that strict time limits apply, even during weekends and bank holidays.

Appendix 1 - IG/Data Security Breach Assessment Reporting and Management



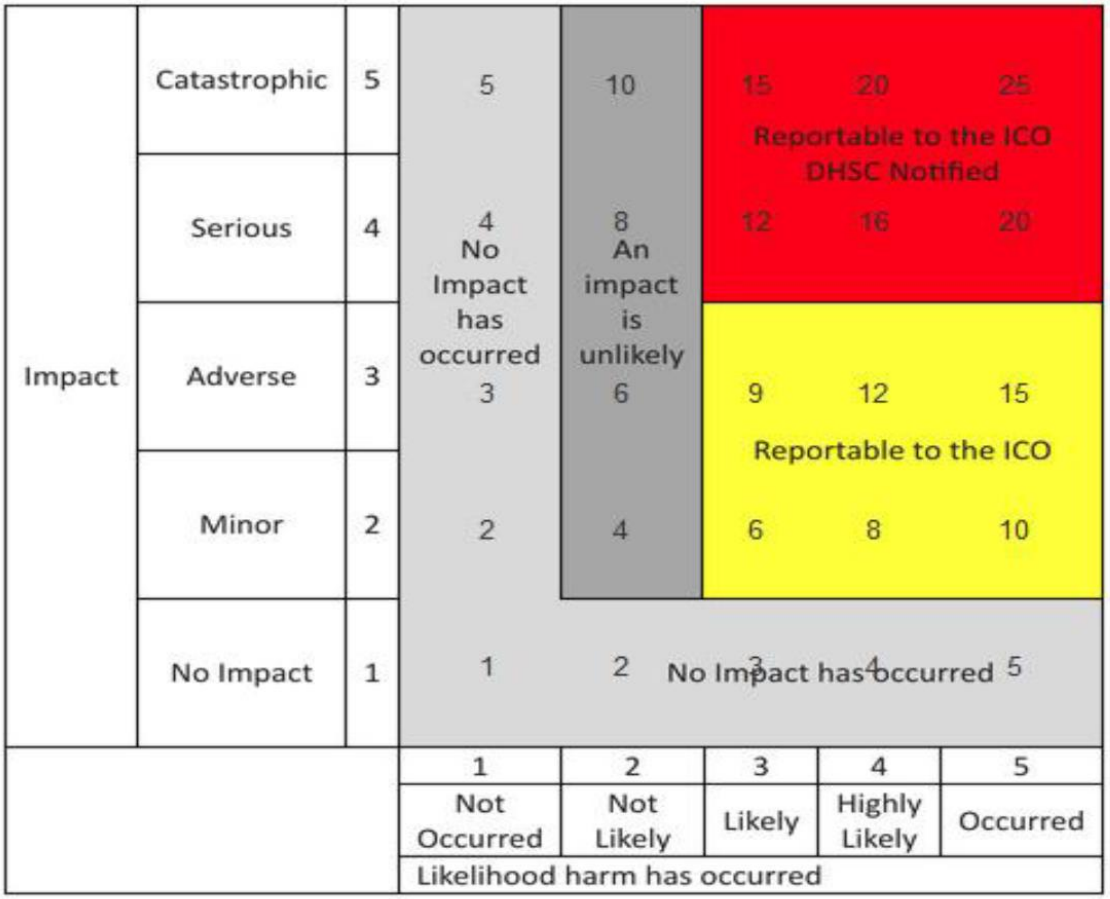
Process

Use appendix two to assess impact.

Appendix 2 – IG/Data Security Breach Assessment Grid

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	In cases where there is no evidence that can prove that no adverse effect has occurred this must be selected.
3	Likely	It is likely that there will be an occurrence of an adverse effect arising from the breach.
4	Highly likely	There is almost certainty that at some point in the future an adverse effect will happen.
5	Occurred	There is a reported occurrence of an adverse effect arising from the breach.

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	A minor adverse effect must be selected where there is no absolute certainty. A minor adverse effect may be the cancellation of a procedure but does not involve any additional suffering. It may also include possible inconvenience to those who need the data to do their job.
3	Potentially some adverse effect	An adverse effect may be release of confidential information into the public domain leading to embarrassment or it prevents someone from doing their job such as a cancelled procedure that has the potential of prolonging suffering but does not lead to a decline in health.
4	Potentially Pain and suffering/ financial loss	There has been reported suffering and decline in health arising from the breach or there has been some financial detriment occurred. Loss of bank details leading to loss of funds. There is a loss of employment.
5	Death/ catastrophic event.	A person dies or suffers a catastrophic occurrence


Impact
Catastrophic
5
Serious
4
Adverse
3
Minor
2
No Impact
1
5
10
15
20
25
Reportable to the ICO
DHSC Notified
4
8
12
16
20
No Impact has occurred
An impact is unlikely
3
6
9
12
15
Reportable to the ICO
2
4
6
8
10
1
2
3
4
5
No Impact has occurred
1
2
3
4
5
Not Occurred
Not Likely
Likely
Highly Likely
Occurred
Likelihood harm has occurred

Appendix 3- DPO Data Breach Notification Procedure

If you decide to seek the advice from the DPO of a data breach:

1. Notify the DPO as soon as possible (including weekends) as there is a window of 72 hours to report a breach to the ICO, if the breach is reportable.

2. Mitigate the breach as far as possible, for example recovering the lost or disclosed data.

3. Send to the DPO on dpo@affinityresolutions.co.uk:

- The date of the breach
- The date you became aware of the breach
- A brief account of the breach
- Details of the data which has been lost/disclosed
- The number of data subjects affected
- If the data subject(s) is aware of the breach
- If any other organisation is aware of the data breach
- Any steps taken to mitigate the breach
- If sending supporting documentation, consider redacting personal information.

Appendix 4 – Personal Data definition

Personal Data Breach

As per Article 4(12) of the GDPR, a “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.

The traditional view that a personal data breach is only reportable when data falls into the wrong hands is now replaced by a concept of a ‘risk to the rights and freedoms of individuals’ under Article 33 of GDPR. These types of breaches are graded as per the guidance from NHS Digital using a risk scoring 5x5 matrix and maybe notifiable to the Information Commissioners Office (ICO) if they attain a grade as described in the guidance.

Personal data

This is data defined as any information relating to an identified or identifiable living individual.’ An “Identifiable living individual” means a living individual who can be identified, directly or indirectly, by reference to:

(a) an identifier such as a name, an identification number, location data or an online identifier, or

(b) one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual.

All paper records that relate to a living individual and any aspect of digital processing such as IP address and cookies are deemed personal data. GDPR also introduces geographical data and biometric data to be classified as personal data.

Special Categories of Personal Data

Under GDPR, these are: 6

• racial or ethnic origin

• political opinions

• religious or philosophical beliefs

• trade union membership

• the processing of genetic data

• biometric data for uniquely identifying a natural person

• data concerning health

• data concerning a natural person's sex life or sexual orientation

For data security breach reporting purposes, special categories of data also include:

• Vulnerable children

• Vulnerable adults

• Criminal convictions/prisoner information

• Special characteristics listed in the Equality Act 2010 where not explicitly listed in this guidance and it could potentially cause discrimination against such a group or individual

• Communicable diseases as defined by public health legislation

• Sexual health

• Mental health

Change Register

Date	Version	Author	Change Details
Feb-22	1.0	D Lownsdes / DPO	After DPO review of all policies new procedure as drafted by DPO. Additional material as a result of recent incident
Mar-22	1.1	D Lownsdes	Additional appendices added