**DATA BREACH RESPONSE POLICY**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Version:** | **Review date:** | **Edited by:** | **Approved by:** | **Comments:** |
| v1 | 28/01/2019 | Sultan Mohamed | Munira Mohamed |  |
| v2 | 16/12/2019 | Sultan Mohamed | Munira Mohamed | DPO details added |
| v3 | 20/06/2022 | Sultan Mohamed | Munira Mohamed | Minor changes |
| v4 | 01/10/2024 | Sultan Mohamed | Munira Mohamed | revised |
|  | October 2026 |  |  | Next review |
|  |  |  |  |  |

**DATA BREACH RESPONSE POLICY**

**Introduction**

The purpose of the policy is to establish the goals and the vision for the breach response process. This policy defines to whom it applies and under what circumstances, and it will include the definition of a breach, staff roles and responsibilities, standards and metrics, as well as reporting mechanisms. The policy shall be well publicised and made easily available to all personnel whose duties involve data privacy and security protection.

Theintention for publishing a Data Breach Response Policy is to focus attention on data security and data security breaches and how our established culture of openness, trust and integrity should respond to such activity.

**Data Security Vision**

Sheerwater Health Centre will ensure personal information relating topatients**,** employees, partners and the company is protected from illegal disclosure and misuse.

**Scope**

This policy applies to all who collect, access, maintain, distribute, process, protect,   
store, use, transmit, dispose of, or otherwise handle personally identifiable   
information of Sheerwater Health Centre patients and staff. This includes permanent and temporary employees of Sheerwater Health Centre including contractors, apprentices, volunteers and Partner Organisations.

**Enforcement**

Any Sheerwater Health Centre employees, contractors, apprentices or volunteers found in violation of this policy may be subject to disciplinary action, up to and including termination of employment or Partnership Contracts.

**Definition**

A data breach is a security incident in which sensitive, protected or confidential data is copied, transmitted, viewed, stolen or used by an individual unauthorised to do so.

**Policy**

1. Any individual who suspects that a theft, breach or exposure of Sheerwater Health Centre protected or sensitive data has occurred must IMMEDIATELY provide a description of what occurred via e-mail or telephone to the Practice Manager.
2. The practice Manager will IMMEDIATELY conduct a cursory investigation of the reported thefts, data breaches and exposures to confirm if a theft, breach or exposure has occurred.

1. If a theft, breach or exposure has occurred, the Practice Managerwill IMMEDIATELY limit further access to that resource.
2. Within 24 hours of becoming aware of the breach The Practice Manager will call and chair a virtual incident response meeting.

As a minimum the team will include members (where relevant) from:

* GP lead
* Reception Lead
* Nurse Lead
* Additional individuals as deemed necessary by the Practice Manager

1. The Incident Response Team will or deputise a Forensic Team to;

Analyse the breach

Determine the root cause

Determine the volume ad types of data involved

Determine the impact on internal / external individuals

Determine the impact on external organisations

Document the breach discussion

List the breach in the Practice Breach Register

Liaise with the Data Protection Officer for advice

**GP Practice Data Protection Officer Support Service**

**Provided by A J Spinks Ltd**

**DPO ADDRESS**

**DPO EMAIL** [ajspinksltd.surreyheartlandsdpo@nhs.net](mailto:ajspinksltd.surreyheartlandsdpo@nhs.net)

**DPO TELEPHONE NUMBER 0203 887 6923**

Develop a communication plan

* 1. Notify the ICO of a breach within 72 hours of discovery (if applicable)

**Appendix 1**

Grading a personal data breach

**Appendix 2**

Breach Notification Form

**Appendix 1**

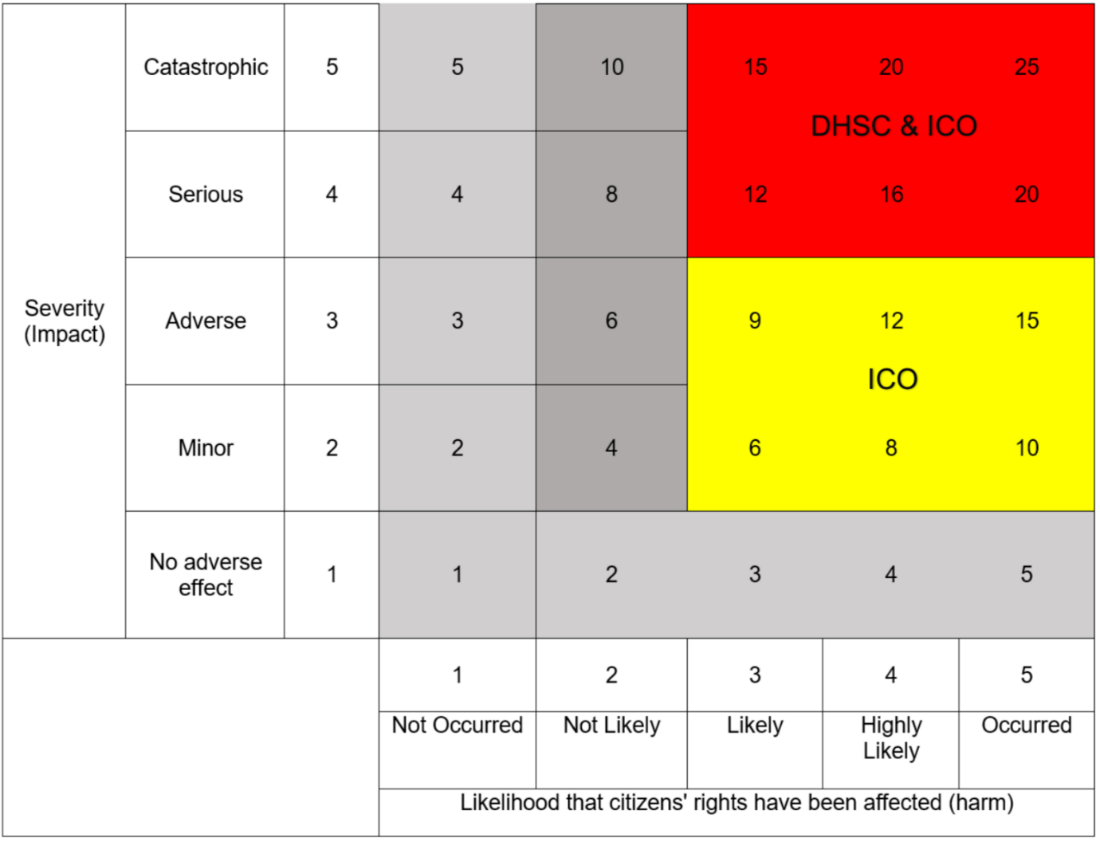
# **Grading a Personal Data Breach**

## **Establish the likelihood that adverse effect has occurred**

|  |  |  |
| --- | --- | --- |
| **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. |

## **Grade the potential severity of the adverse effect on individuals**

|  |  |  |
| --- | --- | --- |
| **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 |



**Appendix 2**

**Breach notification form**

This form is to be used when data controllers wish to report a breach of the Data Protection Act to the ICO. It should not take more than 15 minutes to complete.

1. **Organisation details**
2. Name of your organisation
3. Data controller’s registration number
4. Contact details

Name

Job title

Email address

Contact tel number

Postal address)

1. **Details of the data protection breach**
2. Describe the incident in as much detail as possible.
3. When did the incident happen?
4. How did the incident happen?
5. If there has been a delay in reporting the incident please explain your reasons for this.
6. What measures are in place to prevent an incident of this nature occurring?
7. Please provide extracts of any policies and procedures considered relevant to this incident, and explain which of these were in existence at the time this incident occurred. Please provide the dates on which they were implemented.
8. **Personal data placed at risk**
9. What personal data has been placed at risk?
10. How many individuals have been affected?
11. Are the affected individuals aware that the incident has occurred?
12. What are the potential consequences and adverse effects on those individuals?
13. Have any affected individuals complained to the organisation about the incident?
14. **Containment and recovery**
15. What action have you taken to minimise/mitigate the effect on the affected individuals?
16. Has the data placed at risk now been recovered? If so, please provide details of how and when this occurred.
17. What steps has you taken to prevent a recurrence of this incident?
18. **Training and guidance**
19. What training does the organisation provide its staff on the requirements of the Data Protection Act and GDPR?
20. Please confirm if training is mandatory for all staff.
21. Had the staff members involved in this incident received training and if so when?
22. As the data controller, does the organisation provide any detailed guidance to staff on the handling of personal data in relation to the incident you are reporting? If so, please provide any extracts relevant to this incident here.
23. **Previous contact with the ICO**
24. Have you reported any previous incidents to the ICO in the last two years?
25. If the answer to the above question is yes, please provide: brief details, the date on which the matter was reported and, where known, the ICO reference number.
26. **Miscellaneous**
27. Have you notified any other (overseas) data protection authorities about this incident? If so, please provide details.
28. Have you informed the Police about this incident? If so, please provide further details and specify the Force concerned.
29. Have you informed any other regulatory bodies about this incident? If so, please provide details.
30. Has there been any media coverage of the incident? If so, please provide details of this.

**Sending this form**

Send your completed form to [casework@ico.org.uk](mailto:casework@ico.org.uk), with ‘DPA breach notification form’ in the subject field, or by post to: The Information Commissioner’s Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF. Please note that we cannot guarantee security of forms or any attachments sent by email.

**What happens next?**

You will be contacted within seven calendar days to provide:

* a case reference number; and
* information about our next steps

If you need any help in completing this form, please contact the ICO helpline on **0303 123 1113** or **01625 545745** (operates 9am to 5pm Monday to Friday)