

**ORGANISATION NAME**

**Data Breach Response Policy**

**July 2018**

**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**

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

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

**Enforcement**   
Any **ORGANISATION NAME** 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 **ORGANISATION NAME** protected or sensitive data has occurred must IMMEDIATELY provide a description of what occurred via e-mail to **CONTACT EMAIL** or by calling **CONTACT TELEPHONE NUMBER**
2. This e-mail address and phone number are monitored by **CONTACT NAME**
3. **CONTACT NAME** 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, **CONTACT NAME** will 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

**DPO NAME**

**DPO ADDRESS**

**DPO EMAIL**

**DPO TELEPHONE NUMBER**

Develop a communication plan

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

**Appendix 1**

Doncaster LMC Organisational Standards Monitoring Tool

**Appendix 2**

Doncaster LMC Breach Notification Form

**Appendix 1**

**Doncaster LMC Organisational Standards Monitoring Tool – Data Breaches**

|  |  |
| --- | --- |
|  | **Metric** |
| **Goal** | Statement of organisional goal.  **We will respond to all data breaches according to this policy.** |
| **Measurement of Success** | How is the goal going to be measured?  **All data breach investigations are documented.**  **All data breaches are recorded in our Practice Data Breach Register.** |
| **Type of Measurement** | Delete as appropriate  Implementation |
| **Formula** | How is the measurement of success calculated?  **% of data breaches where this policy has been followed.** |
| **Target** | What is your threshold for defining success (e.g. 90%)  **100% of data breaches managed according to this policy** |
| **Evidence** | What evidence needs to be collected to prove success?  **Record of the true number of data breaches.**  **Record of how many data breaches have documentation of investigation.**  **Record of how many data breaches are recorded in our Practice Data Breach Register.** |
| **Source** | Where is the evidence above located?  **Data Breach Register is on Practice Manager’s Desktop computer.**  **Documentation of investigations are on Practice Manager’s Desktop Computer.** |
| **Frequency** | How often does this monitoring need to take place?  **Yearly – Every August.** |
| **Accountability** | Who is responsible for the success?  **Practice Manager** |
| **Stakeholders** | Who are the key stakeholders?  **GP Partners** |
| **Reporting** | How is the output of this tool going to be fed back to key stakeholders?  **Once yearly at a Partnership meeting** |

**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)