**Data Breach Crisis Management Plan**

**Guidance Notes**

Dealing with a data breach, under a very strict time limit of 72 hours, is a very stressful experience. At Briefed we have helped many businesses who are facing this type of situation and it is clear that to get through the situation as close to unscathed as possible, you need to have set up a plan in advance. Your professional reputation and your practice may be at risk. To get the best result in defending yourself during an investigation, you need to know exactly what to do in the event of a breach and how to get in touch with the right people to help you. You do not want to waste precious hours trying to figure out where to start.

This policy document simply outlines the process you should consider; you can add information and other protocols that are required for your practice.

**THIS TEMPLATE IS FOR GENERAL INFORMATION ONLY AND SHOULD NOT BE RELIED UPON AS LEGAL ADVICE. IF YOU REQUIRE SPECIFIC LEGAL ADVICE ABOUT A SECURITY BREACH OR OTHER DATA PROTECTION MATTERS, PLEASE CONTACT AN APPROPRIATE LEGAL PROFESSIONAL.**

**Data Breach Crisis Management Plan**

**[The Healthcare] Practice**

**Date Prepared:**

**Date Reviewed:**

The deadline for reporting a data breach to the Information Commissioner’s Office is 72 hours.

Note that the clock starts running from the moment you are or should have been aware of the potential breach.

Create a list of emergency contacts and their contact details. Depending on the type of breach, you may have to contact different people, therefore it is useful to have this information already collated.

**Sources of assistance**

|  |  |
| --- | --- |
| Do you have access to specialist GDPR advice?  (Your clinic/hospital may have a support contract that you are entitled to access) | Company  Contact name  Phone number  Email address  Out of hours phone |
| Do you need PR assistance in relation to media attention? | Name of contact  Company name  Phone number  Email address  Out of hours phone |
| Can your IT providers help? | Name of contact  Company name  Phone number  Email address  Out of hours phone |
| Do you need to obtain legal advice? | Name of Solicitor/Barrister  Firm  Phone number  Email address  Out of hours phone |

**Immediate action – containment**

Steps which should be completed immediately upon the discovery of a data breach:

1. Take steps to mitigate the issue: e.g. if hacked, lock down your laptop; if you lose your phone, activate remote wiping; if you lose a record, take steps to try to retrieve.

Have any technical systems been affected?

* Emails
* Cloud or server storage
* Practice management systems
* Mobile devices
* Home or office’s internet access.

If data has been lost or stolen, are there any safeguards in place such as encryption or remote wiping?

What can you do to prevent further loss or consequences?

1. Identify what information has been lost/breached and who the data subjects are.
2. Notify appropriate parties as above.
3. Seek emergency advice from IT/PR/GDPR experts.
4. What other steps should you take?

**Investigate – Record details of the data breach**

Record the incident in as much detail as possible – you will need this to aid your defence.

1. What was the breach?
2. When did it occur?
3. How did it occur?
4. Were any delays incurred in becoming aware of the breach?
5. Reason for delays.
6. Exactly what data has been breached?
7. Is it personal data? Is special category information involved?
8. How many data subjects are affected?
9. Are you able to contact the data subjects if you need to?

**Risk Assessment – You need to assess the risk to the affected data subjects**

1. Are any of the data subjects at risk as a result of the breach?
2. Could the data be used to a detrimental effect?
3. What steps could be taken to deal with those effects?
4. Should the breach be reported to the individual? What steps do you need to take to do this?
5. Does the matter need to be reported to the ICO? How are you going to make that decision?

**Notification**

Consider who needs to be notified of the breach

|  |  |
| --- | --- |
| Data subjects |  |
| Clinics/hospitals | Name  Phone number  Email  Out of hours phone |
| General Medical Council | Name  Phone number  Email  Out of hours phone |
| Patients who are the subjects of the data breach | Name  Phone number  Email  Out of hours phone |
| Police  Cyber Crime Unit | Local police station  Phone number  Email  Out of hours phone  Reference number |
| Referring doctors and any other relevant healthcare professional | Name  Phone number  Email  Out of hours phone |
| IT provider | Name  Phone number  Email  Out of hours phone |
| Information Commissioner’s Office | Breach submission form – <https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/>  Phone number – 0303 123 1113 |
| Professional indemnity or cyber insurers | Name  Phone number  Email  Out of hours phone  Policy number |
| Relevant trust/local authority | Name  Phone number  Email  Out of hours phone  Name of data subject  Case reference number |
| Insert as appropriate |  |

**Communications**

1. Ensure that every person provided with information about the incident understands the need for confidentiality.
2. Ensure that there is a clear communication strategy with a central point of contact.
3. All communications relevant to the incident should be restricted to an agreed group of people to avoid any unintended waiver of privilege or other unplanned disclosure of information.

**Post-event Evaluation**

|  |  |
| --- | --- |
| Why did the breach occur? |  |
| What measures have been taken to prevent recurrence? |  |