## Data Breach Response Plan

| | |
|---|---|
| Training of staff to identify a data breach | All staff have annual training in Privacy including being able to identify and act on a potential data breach.<br><br>A data breach is a circumstance where confidential information about a person or persons is accessed by an unauthorised person or is stolen or lost. This can be unintentional or malicious and can include loss of physical equipment such as a laptop with personal information on it or unauthorised access being granted to some-one to another person's information or inadvertent disclosure due to human error or disclosure induced by fraud or scamming activities.<br><br>Training enables staff to know how to identify a data breach or potential data breach, who to report it to, when it should be reported and what other actions to take to protect patients' personal information. |
| Notifying a suspected breach | Any member of staff who believes a data breach may have occurred is required to notify the practice principal either orally (followed by a confirming email) or by email, as soon as possible after forming the belief that this has occurred |
| The data breach response team including external partners | Once the notification is received the practice principal will<br><br>1. Decide by telephone if the matter is something the practice can manage alone or whether any other person needs to be involved<br><br>2. If appropriate, the external IT provider should be advised as soon as possible.<br><br>3. Advise any cyber security insurance provider or general liability provider<br><br>4. Notify medicolegal insurance provider. |
| How plan applies to different types of breaches | The nature of the practice's response will differ according to the circumstances in which the suspected breach occurred and the nature of the breach.<br><br>The practice principal needs to determine if the breach raises the possibility of a serious risk to a person's life or health. If so the practice principal must immediately contact the person at potential risk of harm to advise of the risk<br><br>If there is no immediate risk to a person's life or health the assessment must identify if this is a reportable breach. A reportable breach occurs if the breach could result in serious harm to a person. |
| How assessment of breaches will occur | The assessment must consider –<br><br>1. How the breach occurred;<br><br>2. Has the breach been contained;<br><br>3. If the breach has not been contained what actions need to be taken to contain the breach;<br><br>4. What actions can be taken to ensure the breach does not occur again<br><br>5. Is the breach reportable<br><br>The assessment and actions taken should be completed within 30 days |

| | |
|---|---|
| How affected persons will be notified | If the number of persons impacted by the breach are few enough, notification should be by telephone by the practice principal<br><br>The information to be provided is:<br><br>• the fact that a data breach has occurred, that the patient's information has been accessed by a third party,<br><br>• brief details of how it occurred,<br><br>• details of the information accessed,<br><br>• details of what steps the practice has taken to contain the breach,<br><br>• any suggestions the practice can make as to steps the patient can or should consider taking to protect their interests<br><br>• details of what changes to information storage or management the practice is making to avoid the breach occurring in the future,<br><br>• a commitment to follow up with each person when the event has been fully investigated about any further action taken<br><br>A record should be kept of the contact with contact details<br><br>If the number of persons is too large to be done by telephone the notification should be by email by the practice principal in conjunction with liability insurance advice |
| Reporting to OAIC or other bodies | If the matter is a reportable breach the OAIC should be notified in writing as soon as possible (and no later than 30 days) advising what steps have been taken to contain the breach and notify affected persons |
| Record keeping for breaches | A separate file must be created by the practice principal for any suspected breach and all emails and memos and correspondence should be saved to the file |
| Requirements under agreements with third parties | The practice principal is to consider all obligations to notify third parties of the suspected breach including the OAIC, state privacy entities, insurers, |
| Reviewing of plan and testing of plan | This plan should be reviewed at least every two years or if there are any new IT system programs introduced into the practice or significant changes in how information is stored |
| Post breach review assessment | After a breach has occurred the practice must review what has occurred by reference to this plan. |