Avant factsheet/case study:

Responding to a data breach

Healthcare organisations need to be prepared for both cyber and traditional threats to the security of the personal health information they hold. Even a single breach of patient privacy has the potential to cause serious harm and may be notifiable under the mandatory data breach notification scheme. Being prepared to identify and respond to a breach quickly can help to protect your patients' confidential information and maintain your practice's reputation in the event that a breach occurs at your practice.

Discovering a data breach

Unfortunately, many organisations only become aware of a security compromise when notified by a third party, before it has been detected by the organisation itself. This puts the organisation immediately on the back foot in responding to a breach.

If your practice does suffer a data breach, ideally you want to discover it early and be able to respond promptly. Training and having systems such as security scans and audits to proactively detect any breaches are effective ways of ensuring you are prepared and have time to respond.

Responding to a data breach

We recommend that you have a data breach policy and response plan in place so you can respond quickly (within 24 hours) if a data breach occurs. You should test and review your data breach response plan regularly.

The Office of the Australian Information Commissioner (OAIC) has a guide to managing data breaches which includes a checklist to determine whether your response plan addresses relevant issues.

The OAIC guide suggests responding to a data breach broadly involves four steps. In practice, there are some additional steps which may be appropriate:

- contain the breach and make a preliminary assessment
- evaluate the breach, risk of harm and possibility of remediation
- notify as necessary
- consider other responses
- restore trust and manage any reputational damage
- evaluate your response and consider actions to prevent future breaches.

The process is not necessarily linear and the steps do not necessarily occur in order. For example containing a breach may mean notifying those affected immediately, depending on the potential risk.

1. **Contain the breach**

   Take steps to contain the breach where possible. This might include shutting down your system (in the case of malware or hacking), taking steps to retrieve a portable device that has been left somewhere, or de-activating a staff member's authority to access the system.

2. **Evaluate the breach and risk of harm**

   If you suspect there has been a breach, you need to assess within 30 days whether or not a 'notifiable breach' has occurred.

   A breach will be notifiable if:

   - there is unauthorised access to, unauthorised disclosure or loss of personal information held at your practice where unauthorised access or disclosure is likely to occur; and
   - the breach is likely to result in serious harm to one or more individuals; and
   - your practice has been unable to prevent the likely risk of harm with remedial action.

   You should appoint a staff member to undertake an assessment of the breach. This may be your practice manager or another suitable senior staff member.

   The assessment should include:

   - a preliminary assessment of the type of information involved, the cause or causes, the extent of the breach

- assessment of the risks and nature of harm to affected individuals
- whether remedial action can be taken to remove the risk of harm
- consideration of whether it is a data breach that needs to be notified to the OAIC and affected individuals or a My Health Record (MHR) data breach that needs to be notified to the MHR System Operator (the Australian Digital Health Agency) as well as the OAIC.

You may need to engage an IT consultant to assist in conducting an assessment and confirm the extent of any authorised access, as well as address any persisting vulnerabilities.

Serious harm

Serious harm may include serious physical, psychological, emotional, financial or reputational harm. It is more than distress or upset. It could include:

- identity theft
- significant financial loss
- threats to physical safety
- workplace or social bullying or marginalisation
- humiliation, damage to reputation or relationships.

Consider:

- whose information was involved in the breach and whether the information is otherwise publicly available
- the kind or kinds of information
- the sensitivity of the information
- whether the information is protected by one or more security measures (e.g. password protected or encrypted) and the likelihood that those measures could be overcome (consider how easy the password might be to guess; does the attacker hold an encryption key?)
- the persons or kinds of persons who have obtained or who could obtain the information (e.g. hackers attacking your system vs leaving a flash drive containing patient records at another medical practice where you work)
- the nature of the harm (see serious harm above)
- any other relevant matters (likelihood of harm occurring and anticipated consequences for individuals).

Remedial action

In assessing the risk of harm, you also need to consider whether positive steps can be taken to avoid or reduce the risk of harm.

Remedial action will depend on the circumstances of the case and the nature of the breach. It requires you to be satisfied that the action taken has prevented the risk of harm occurring to potentially affected individuals.

You should take such steps if you can. If remedial action can be taken to prevent serious harm occurring as a result of a data breach, mandatory notification to the OAIC under the notifiable data breach scheme is not required (unless it involves a MHR breach).

3. Notify

If the breach is a notifiable data breach you must notify the OAIC and affected individuals (unless an exception applies). See further our Notifiable data breaches flowchart and Data breach notification under the Notifying a data breach under the Notifiable Data Breach scheme.

If the breach is a MHR data breach you must notify the MHR System Operator (the Australian Digital Health Agency) and the OAIC.

Doctors have a professional obligation to disclose adverse events to patients. This includes where there has been an error leading to a data breach. It is good medical practice to inform the patient about an error leading to a data breach even if it does not need to be notified to the OAIC.

Depending on the nature of the incident you may wish to make a voluntary notification to the OAIC to obtain their advice and assistance on how to best respond to the breach.

4. Consider other responses

If you need to shut down your system or a natural disaster such as a fire or flood has damaged your files, consider whether you can continue to treat patients while your system is shut down?

Depending on how your system has been compromised, consider changing passwords, updating anti-virus software, encrypting portable devices.

You may also wish to contact the Australian Cyber Security Centre, who can assist in managing cybersecurity incidents.

If the breach appears to be the result of criminal activity, it will generally be appropriate to notify police.

If the breach is a deliberate act by a staff member, you may need to take disciplinary action against them, in accordance with your practice's policies and procedures.

If the breach involves a third party provider, contact the provider and discuss ways to contain the breach and prevent future breaches.

You may need to notify relevant insurers. Your insurance policy may include steps you must follow in the case of a breach.

Document the steps you have taken to respond to the breach.

5. **Restore trust and manage any reputational damage**

   Privacy and security breaches attract media interest and a timely response to a data breach may assist in maintaining your reputation and your relationship with your patients.

   Your data breach response plan should include a communications plan that covers how to deal with media inquiries and external stakeholders. In the case of a significant breach, consider obtaining advice from a public relations company.

6. **Evaluate your response and consider action to prevent future breaches**

   Consider whether the breach is an isolated event or suggests a systemic issue, and whether changes need to be made to prevent future breaches. Changes may include:

   - audit of IT and physical security
   - review of your practice's policies and procedures
   - staff training and refreshers
   - review of third party service providers.

   Review how you responded to the breach and consider whether you need to make any change to your data breach response plan. Ensure you regularly test your data breach response plan.

Learn more

Avant resources

Data breach – all you need to know

Office of the Australian Information Commissioner

OAIC Data breach preparation and response – a guide to managing data breaches in accordance with the Privacy Act 1988 (Cth)

OAIC Guide to mandatory data breach notification in the My Health Record system

Office of the Australian Information Commissioner Identifying eligible data breaches

Office of the Australian Information Commissioner Assessing a suspected data breach

Australian Cyber Security Centre

For more information or immediate advice, call our Medico-legal Advisory Service (MLAS) on 1800 128 268, 24/7 in emergencies.