Responding to a data breach

Summary

For healthcare organisations, understanding your obligations in the event of a data breach will help you respond effectively to an accidental or malicious threat to the security of personal health information.

Quick guide

- If you experience a data breach, you will need to act quickly to minimise harm to patients and your practice.
- Even a single breach of patient privacy has the potential to cause serious harm and you may be legally required to notify patients and government agencies of the breach.
- Being prepared and having a data breach response plan can help you respond appropriately if you do experience a breach.

Data breaches

A data breach occurs when there is unauthorised access to or disclosure or loss of personal information held in your practice.

Data breaches can involve cyber-attacks including hacking or ransomware attacks, or can involve human error, such as sending information to the wrong email address, or losing a device that holds patient information.

All private sector health service providers that hold health information, such as private hospitals, day surgery centres and medical practitioners and practices, must comply with the *Privacy Act 1988* including reporting requirements under the Notifiable Data Breaches scheme.

Discovering a data breach

The longer a data breach goes undetected, the more likely it is that personal information has been compromised and the harder it is to take steps to prevent harm.

Practices should have systems in place to discover data breaches early. Staff training and dedicated monitoring systems including security scans and audits, or intrusion detection and prevention systems, can help you proactively detect any breaches and ensure you are prepared and have time to respond.

For more information see Avant's factsheet Preventing data breaches and seek advice from your IT provider.

Responding to a breach

Data breaches can sometimes go undetected for weeks or even months. This puts the organisation immediately at a disadvantage in responding to a breach.

We recommend that you have a data breach policy and response plan in place so that you can respond quickly (within 24 hours) if a data breach occurs. Ensure your staff are aware of the plan and know what to do if there is a breach. Test and review your data breach response plan regularly.

The Data breach preparation and response guide from the Office of the Australian Information Commissioner (OAIC) helps organisations understand what is expected of them when preparing for, and responding to, a data breach.

The OAIC guide suggests following four steps when responding to a data breach:

1. Contain the breach and try to prevent any further compromise
2. Assess the breach, risk of harm and possibility of remediation
3. Notify as necessary (Notifiable data breaches scheme/My Health Record)
4. Review your response and consider actions to prevent future breaches.

The steps may not always occur in the same order; for example, containing a breach and minimising the risk of harm may mean notifying those affected immediately, depending on the potential risk.

1. Contain the breach

Once you know or suspect a breach has occurred, take steps to contain the breach where possible.

This might include taking steps to recall an email, wipe a missing portable device, or de-activate a staff member's authority to access the system.

If the breach involves a cyber-attack you may need to move quickly and get expert advice to minimise the damage. See Avant's factsheet on Responding to a cyber security incident for more detailed guidance.

2. Assess the breach

Assess the breach and try to understand the extent of the breach and risk of harm to potentially affected individuals.

Start this assessment as quickly as possible. If you suspect you have experienced a notifiable data breach (as explained further below), you need to take reasonable steps to assess the breach within 30 days.

Appoint a staff member to undertake the assessment. This may be your practice manager or another suitable senior staff member.

The assessment should include:

- the type of personal information involved in the breach
- the circumstances of the breach, including its cause, extent and how long the data may have been exposed
- the nature of likely harm to affected individuals, and if this harm can be removed through remedial action.

You may need to engage an IT consultant to assist with this assessment. They should be able to confirm the extent of any unauthorised access, as well as help to address any persisting vulnerabilities.

3. Notify

Depending on the circumstances you may be required to inform individuals whose personal information has been affected as well as one or more organisations about the breach.

Data breach notification under the Notifiable Data Breaches Scheme

Under the Notifiable Data Breaches (NDB) scheme, you will be required to notify affected individuals and the OAIC about a breach if:

- the breach could lead to serious harm to an individual whose personal information is involved, and
- you are unable to undertake remedial action to prevent the likelihood of serious harm.

Avant has developed a flow chart to help you decide whether the breach is one that you need to notify.
See 'Responding to a data breach flow chart' on page 4.

For more information on how to make a notification and what information to include, see the OAIC's Guide to the Notifiable Data Breach Scheme.

If the breach involves a third-party provider, you will often need to co-ordinate your response and compliance with the NDB scheme. This is discussed further in the OAIC's Guide to the Notifiable Data Breach Scheme.

Serious harm
The test for notifying under the NDB scheme is whether a reasonable person would consider the breach would be likely to result in serious harm to an individual whose information was exposed.

'Serious harm' requires more than distress or upset. However the OAIC takes a broad view of harm, which could include physical, psychological, emotional, financial or reputational harm. See the OAIC website's Part 4: Notifiable Data Breach (NDB) Scheme for further guidance.

Likely to result
The phrase 'likely to result' means the risk of serious harm to an individual is more probable than not (rather than possible).

Data breach notification for My Health Record

If the data breach potentially affects the My Health Record (MHR), your practice must notify the Australian Digital Health Agency (ADHA) and the Office of the Australian Information Commissioner (OAIC) of any:

- actual or suspected unauthorised collection, use, or disclosure of health care information in an individual's MHR, or
- events or circumstances that have compromised or have the potential to compromise the security or integrity of the MHR system.

Your obligations under the My Health Records Act 2012 are separate from and stricter than those under the Privacy Act – as outlined in *Table 1* below.

The MHR obligation applies only to information contained within the MHR. It does not apply to information that has been downloaded from the MHR and incorporated into your local practice records. Any breach related to your practice records would need to be considered under the NDB scheme.

Table 1 below summarises the differences between notification under the MHR and NDB scheme.

Table 1

	My Health Record	Notifiable Data Breach
What type of breach?	• Actual or suspected, unauthorised collection, use or disclosure of health information in an individual's MHR. • Events or circumstances that have compromised or have the potential to compromise the security or integrity of the MHR system.	• Unauthorised access to or unauthorised disclosure of personal information. • Loss of personal information where unauthorised disclosure is likely.
When to notify?	• Must be notified even if the breach has been rectified or remedial action has been taken.	• Not required to report if remedial action prevents likelihood of serious harm.
Who notify?	• Notify ADHA and OAIC • ADHA to notify affected individuals	• Notify OAIC and affected individuals

4. Review your response and consider action to prevent future breaches

You may need to take additional steps to finalise your response, such as:

- 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 further action against them, in accordance with your practice's policies and procedures.
- You may need to notify relevant insurers, as your insurance policy may include steps that you must follow in the case of a breach.

Document the steps you have taken to respond to the breach. Consider whether the breach is an isolated event or suggests a systemic issue, and whether you need to make changes to prevent future breaches or improve your ability to respond. Changes may include:

- audit of IT and physical security
- changing passwords, updating patches and anti-virus software, encrypting portable devices
- reviewing your practice's policies and procedures (including information security policy, privacy policy, disaster recovery plan or data breach response plan)
- staff training and refreshers
- reviewing arrangements with third-party service providers.

When reviewing information management and data breach responses, you can refer to the OAIC's Guide to Securing Personal Information.

Additional resources

Office of the Australian Information Commissioner

OAIC Data breach preparation and response guide

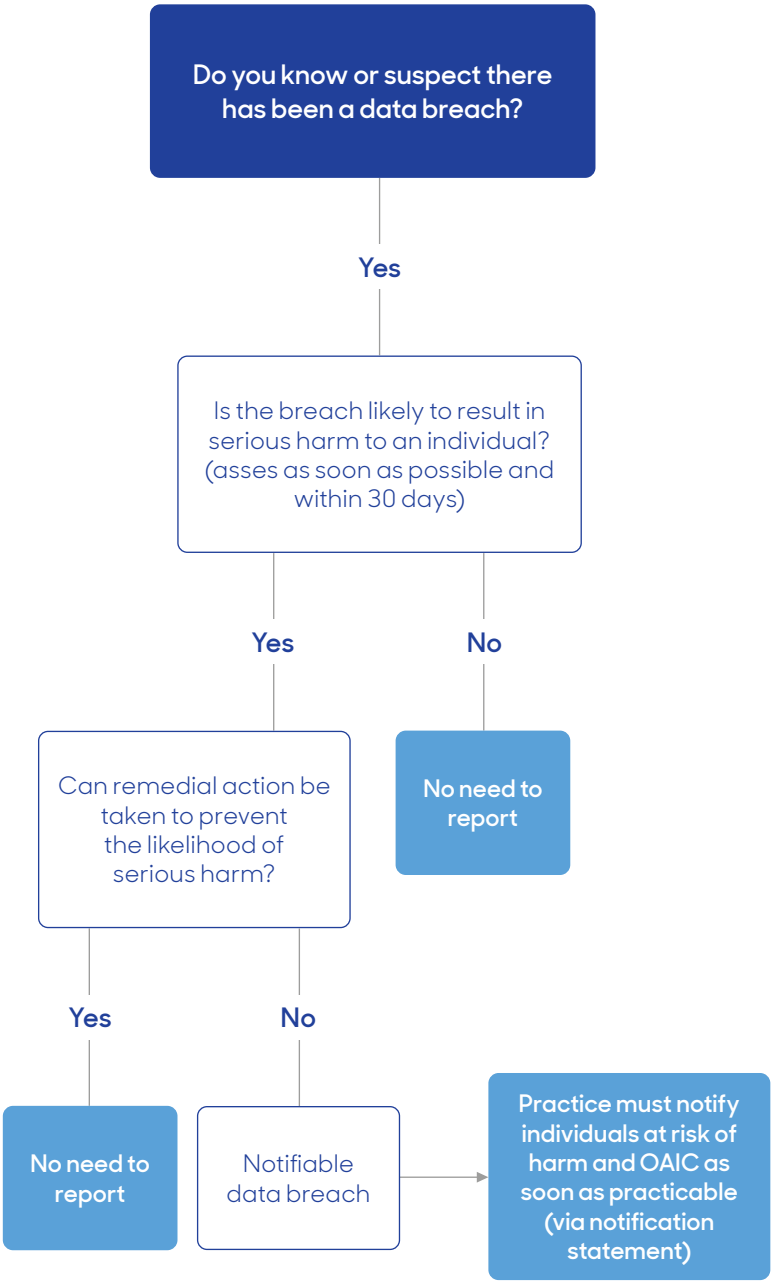
OAIC Guide to mandatory data breach notification in the My Health Record system

For more information or immediate medico-legal advice, call us on **1800 128 268**, 24/7 in emergencies.
avant.org.au/mlas

avant.org.au/avant-learning-centre

Notifiable data breach

Organisations covered by the Privacy Act 1988 are required to notify individuals likely to be at risk of serious harm because of a data breach, and to notify the Office of the Australian Information Commissioner.



A data breach is:

- Unauthorised access to or unauthorised disclosure of personal information or
- Lost personal information and likely unauthorised access or disclosure

Likely to result in serious harm

Consider:

- Type of information and sensitivity
- Protections in place to prevent disclosure
- Persons who have obtained or could obtain data
- Nature of harm and number of people affected

Serious harm can be psychological, emotional, physical, reputational or financial.

Notification statement

Must include:

- Identity and contact details of practice
- Description of data breach
- Kind of information involved
- Recommendation about steps to take in response to breach