NATIONAL BLOOD AUTHORITY
AUSTRALIA

DATA BREACH RESPONSE PLAN

February 2018

NBA Data Breach Response Plan

Purpose

The purpose of the NBA Data Breach Response Plan is to set out procedures and lines of authority for the NBA in the event that the NBA experiences a data breach (or suspects that a data breach has occurred). This Plan is intended to enable the NBA to contain, assess and respond to data breaches in a timely fashion and to mitigate potential harm to affected individuals.

What is a data breach?

For the purposes of this Plan, a data breach occurs when information held by the NBA is lost or subjected to unauthorised access, modification, disclosure, or other misuse or interference. In this Plan, the terms 'data' and 'information' are used interchangeably and should be taken to mean both data and information.

A data breach that involves information that is 'personal information' as that term is defined in the *Privacy Act 1988* (Privacy Act) (i.e. information or an opinion about an identified individual, or an individual who is reasonably identifiable whether the information or opinion is true or not, or recorded in a material form or not) may also constitute a breach of the Privacy Act, depending on whether the circumstances giving rise to the data breach also constitute a breach of one or more of the Australian Privacy Principles (APPs) or a registered APP code.

Data breaches involving personal information that are likely to cause individuals to be at serious risk of harm must be reported to the affected individual(s) and the Australian Information Commissioner in accordance with the requirements of the Notifiable Data Breaches scheme introduced by the *Privacy Amendment (Notifiable Data Breaches) Act 2017*.

Data breaches may arise from:

- loss or unauthorised access, modification, use or disclosure or other misuse;
- malicious actions, such as theft or 'hacking';
- internal errors or failure to follow information handling policies that cause accidental loss or disclosure; and
- not adhering to the laws of the states and territories or the Commonwealth of Australia.

Interaction of the Plan with other laws and policies

Assessing and responding to a data breach may involve the consideration of a number of overlapping policies and legal requirements. For example, a data breach may involve:

- criminal activity which may require referral to the Australian Federal Police;
- a security incident which may require consideration of the Australian Government Protective Security Policy Framework and the NBA's Protective Security Policy;
- fraud against the Commonwealth, which may require consideration of the NBA's Fraud and Corruption Control Plan;
- a disclosure of information about the NBA by a staff member or contractor that may trigger an investigation under *Public Interest Disclosure 2013*; and
- a suspected breach of the Australian Public Service Code of Conduct that may trigger an investigation under the *Public Service Act 1999*.

The NBA Executive will determine the appropriate approach to dealing with a data breach, taking into account all of the NBA's legal obligations, with advice from the Legal Counsel and/or General Counsel as necessary.

Jurisdictional arrangements

Where jurisdictional stakeholders have been provided with data in accordance with an Information Framework Agreement (IFA), they are required to sign the conditions of data release section of the data request form, and in so doing commit to storing and using the data in accordance with the obligations outlined. If the jurisdiction or the NBA becomes aware of or suspects that the conditions of the IFA have been breached, the NBA will initiate the process below.

Responding to data breaches

The NBA will follow the process set out below and in **Attachment A** if there is a data breach relating to personal information for patients, clinicians, health providers or jurisdictions.

When a data breach has occurred or is suspected to have occurred, the NBA will initiate the following process. However, it should be noted that there is no single method of responding to a data breach and in some cases the following steps may need to be modified. Data breaches must be dealt with on a case-by-case basis, by undertaking an assessment of the risks involved, and using that risk assessment to decide the appropriate course of action.

Suspected or known data breach

1. When an NBA employee or contractor become aware or suspects that there has been a data breach, they will notify their manager who will assess the risk, document the event and report in the first instance to the Deputy General Manager.
2. The Deputy General Manager will notify:
    - the NBA's Privacy Officer who will include details of the breach in a data breach register that will contain a brief description of the nature of the breach, how it occurred, the date of the breach, the date of discovery and the date of notification to the NBA (for an external breach); and
    - the NBA Chief Executive (and other senior managers as required) to determine the NBA's response.
3. If the data breach relates to information that the NBA has received from a jurisdiction/stakeholder, the Deputy General Manager will notify the jurisdiction/stakeholder which supplied the data, if the data is identifiable at a health provider or lower level. Each state and territory will have its own process that must be adhered to and the NBA will provide assistance and support in completing these processes.
4. Depending on the seriousness of the breach, the NBA Chief Executive may appoint a staff member or a response team comprising personnel with the necessary expertise (e.g. security, ICT, data, legal etc.) to undertake the response process set out below and in further detail in **Attachment A**.

Contain

5. The staff member/response team will take immediate steps to contain the breach, which may include:
    - if the breach is the result of an ICT security incident (i.e. an event that affects the confidentiality, integrity or availability of the NBA's information, systems and infrastructure), notify the Information Technology Security Adviser to implement response in accordance with the NBA's Protective Security Policy;
    - stopping the unauthorised practice;
    - recovering records;
    - shutting down system that has been breached;
    - revoking or changing computer access privileges;
    - addressing weaknesses in physical or electronic security; and

- alerting building security.

Assess

6. The staff member/response team will complete a data breach assessment in accordance with the Data Breach Assessment Report template at **Attachment B**.

Notification and Review

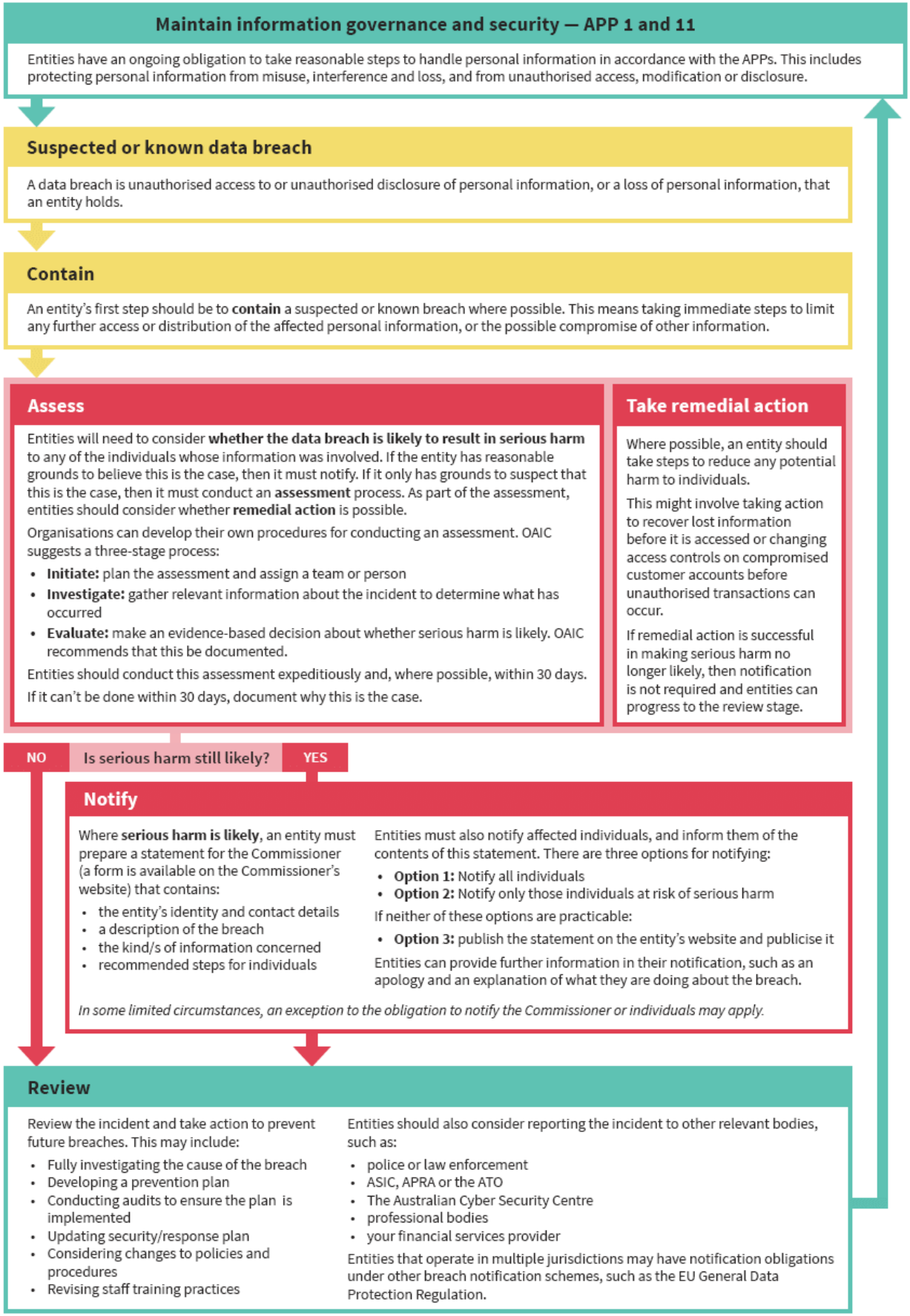
7. The staff member/response team will submit the completed Data Breach Assessment Report to the Chief Executive who will coordinate notification (if required) of affected individuals and/or the Australian Information Commissioner and the NBA's internal review of the data breach.

Evidence and record keeping

The response team will ensure that throughout the data breach response process, the NBA will:

- ensure that evidence is preserved that may be valuable in determining the cause of the breach, or allowing the NBA to take appropriate corrective action; and
- keep appropriate records of the suspected breach are maintained, including the steps taken to rectify the situation and the decisions made.

Attachment A: Data breach response process (reproduced from https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme)



Attachment B

Data Breach Assessment Report

This template is primarily designed to meet the requirements of assessment of data breaches of personal information as defined by the Privacy Act. A data breach involving other kinds of information may require a different approach.

Under the Privacy Act, the NBA must notify affected individuals and prepare a statement for the Information Commissioner if the data breach is likely to result in serious harm to any of the individuals whose information was involved. The purpose of this Report is to:

- enable the NBA to document its assessment of a data breach;

- to inform the decision of whether to notify affected individuals and/or the Information Commissioner; and

- to inform the NBA's review of the data breach and the taking of actions to prevent future breaches.

This assessment must be completed expeditiously and within 30 days if possible.

Description	Details
Description of the breach	[***Provide a short description of the breach, including the date and time the breach was discovered and the duration and location of the breach.***]
Type of information involved	[***Insert the type of information involved.***]
How the breach was discovered	[***Insert details about how the breach was discovered, and by whom.***]
Cause and extent of breach	[***Insert details about the cause and the extent of the breach.***]
List of affected individuals	[***List the affected individuals, or describe the class of individuals who are or may be affected by the data breach.***]
Is the breach likely to result in serious harm to any of the individuals to whom the harm relates?	[***Evaluate whether the breach is likely to result in serious harm to any of the individuals to whom the information relates, having regard to:*** • ***the kind of information involved;*** • ***the sensitivity of the information;*** • ***whether the information is protected by one or more security measures, and the likelihood of those measures being overcome;*** • ***the persons, or the kinds of persons, who have obtained, or who could obtain, the information; and*** • ***if a security technology or methodology was used in relation to the information and designed to make the information unintelligible or meaningless to persons who are not authorised to obtain the information, the likelihood that***

Description	Details
	persons could circumvent the security technology or methodology. ***Seek advice from the Privacy Officer if required.***]
Remedial action	[***Insert details of the steps the NBA has taken to reduce any potential harm to individuals, e.g. by recovering lost information before it is accessed or changing access controls on compromised systems.***]
Is or will the remedial action result in making serious harm no longer likely?	[***State whether the remedial action will result in making serious harm no longer likely. If serious harm is no longer likely, the NBA is not required to prepare a statement to the Information Commissioner or to notify affected individuals.***]
Who will be notified of the breach?	[***Select from the following options.***] [***Option 1***] The NBA has determined that the data breach is likely to result in serious harm to individuals and therefore the NBA will: • provide a statement to the Information Commissioner containing a description of the breach, the kind of information concerned and the recommended steps for individuals. • will [***select one of the following options***] notify all affected individuals / notify affected individuals at risk of serious harm / publish the statement on the NBA's website and publicise it [***choose this option only if the first two options are impracticable***] [***Option 2***] The NBA has determined that notification of the data breach is not required because it is not likely to result in a serious risk of harm to any individuals.
Preliminary recommendations	[***Include any recommendations on actions that could be undertaken to contain the breach, remediate the breach or prevent future breaches of a similar nature – these recommendations will feed into the NBA's comprehensive review of the data breach.***]
Names of response team members	[***Insert the names and roles of response team members. The make-up of the response team will be determined by the Chief Executive, having regard to the skills required to respond to the breach.***]
Date	[***Insert date.***]