HosPortal

CONNECTED HEALTHCARE SOLUTIONS

Data Breach Response Plan

Version 2

June 2020

1. HosPortal Data Breach Response Plan

Purpose

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

Definition of a data breach

For the purpose of this Plan, a data breach occurs when personal information held by HosPortal is lost or subjected to unauthorised access, modification, disclosure, or other misuse or interference.

Personal information as defined in the Privacy Act 1988 is 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.

Data breach involving personal information that are likely to cause individuals serious risk of harm must be reported to the affected individuals and the Office of the Australian Information Commissioner (OAIC) as required by the Notifiable Data Breach (NDB) scheme.

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.

Data breach response personnel

All breaches will be managed by the Privacy Officer, currently Seema Pun, a Director of the business, who will engage internal and external resources to address personnel management, legal, customer interface and technical issues associated with the breach.

Responding to data breaches

HosPortal will follow the process set out below and in **Attachment A** when there is a data breach relating to personal information. However, depending on the nature of the breach, appropriate course of action will be taken following an assessment of the risks involved. Therefore, the following steps may need to be modified.

Suspected or known data breach

When a HosPortal employee or contractor becomes 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 to the Privacy Officer.

The Privacy Officer 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 HosPortal.

HosPortal executive team will determine HosPortal's response.

Depending on the seriousness of the breach, HosPortal executive team will direct appropriate resources to undertake the response process set out below and in further detail in **Attachment A**.

Contain the breach

The staff member or the Privacy Officer will take immediate steps to contain the breach, which may include:

- Stopping the unauthorised practice
- Recovering records
- Shutting down systems that has been breached
- Addressing weaknesses in physical or electronic security

Assess the risks associated with the breach

The staff member or the Privacy Officer will complete a data breach assessment report. The data breach assessment report template is in **Attachment B**.

Notification and review of the breach

The staff member or the Privacy Officer will submit a completed Data Breach Assessment Report to the executive team who will coordinate notification, if required, of affected individuals and/or OAIC and HosPortal Connect's internal review of the data breach.

Documentation

Throughout the data breach response process, the response team will:

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

Reporting

HosPortal's handling of personal information is an agenda item on the HosPortal weekly meeting and includes report of any privacy complaints against HosPortal Connect and internal data breaches.

Attachment A: Data Breach Response Process

(reproduced from OAIC Data breach preparation and response)

Maintain information governance and security - APP 1 and 11

Entities have an ongiong obligation to take reasonable steps to handle personal information in accordance with the APPs. This includes protecting personal information from misuse, interference and loss, and from unauthorised access, modification or disclosure.

Suspected or known data breach

A data breach is unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information that an entitiy holds.

Contain

An entitiy's first step should be to contain a suspected or known breach where possible. This means taking immediate steps to limit any further access or distribution of the affected personal information, or the possible compromise of other information.

Assess

Entities will need to consider **whether the data breach is likely to result in serious harm** to any of the individuals whose information was involved. If the entity has reasonable grounds to be believe this is the case, then it must notify. If it only has grounds to suspect that this is the case, then it must conduct an **assessment** process. As part of the assessment, entities should consider whether remedial action is possible.

Organisations can develop thier own procedures for conducting an assessment. OAIC suggests a three-stage process:

- **Initiate:** plan the assessment and assign a team or person
- **Investigate:** gather relevant information about the incident to determine what has occured
- **Evaluate:** make an evidence-based decision about whether serious harm is likely. OAIC recommends that this be documented.

Entities should conduct this assessment expeditiously and, where possible, within 30 days. If it can't be done within 30 days, document why this is the case.

Take remedial action

Where possible, an entity should take steps to reduce any potential harm to individuals.

This might involve taking action to recover lost information before it is accesssed or chaning access controls on compromised customer accounts before unauthorised transactions can occur.

If remedial action is successful in making serious harm no longer likely, then notification is not required and entities can progress to the review stage.

Is serious harm still likely?

NO

YES

Notify

Where serious harm is likely, an entity must prepare a statement for the Commissioner (a form is available on the Commissioner's website) that contains:

- the entity's identity and contact details
- a description of the breach
- the kind/s of information concerned
- recommended steps for individuals

Entities must also notify affected individuals, and inform them of the contents of this statement. There are three options for notifying:

- **Option 1:** Notify all individuals
- **Option 2:** Notify only those individuals at risk of serious harm if neither of these options are practicable:
- **Option 3:** Publish the statement on the entity's website and publicise it

Entites can provide further information in their notification, such as an apology and an explanation of what they are doing about the breach.

In some limited circumstances, an exception to the obligation to notify the Commissioner or individuals may apply.

Review

Review the incident and take action to prevent future breaches. This may include:

- Fully investigating the cause of the breach
- Developing a prevention plan
- Conducting audits to ensure the plan is implemented
- Updating security/response plan
- Considering change sto policies and procedures
- Revising staff training practices

Entities should also consider reporting the incident to other relevant bodies, such as:

- Police or law enforcement
- ASIC, APHRA or the ATO
- Professional bodies
- Your financial services provider

Entities that operate in multiple jurisdictions may have notification obligations under other breach notification schemes, such as the EU General Data Protection Regulation.

Attachment B: Data Breach Assessment Report

This template will be used to assess data breaches of personal information as defined by the Privacy Act. HosPortal will take all reasonable steps to complete the assessment expeditiously within 30 days after the day HosPortal becomes aware of a data breach or suspected data breach.

Description	Details
Description of the breach	[*Provide a short description of the breach, including the data and time the breach was discovered; the duration; and location of the breach*]
Type of information involved	[*Provide details of the type of information involved*]
How the breach was discovered	[*Describe how the breach was discovered and by whom*]
Cause and extent of breach	[*Describe 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* • *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 the persons could circumvent the security technology or methodology*]
Remedial action	[*Insert details of the steps HosPortal has taken to reduce any potential harm to individuals*]
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, HosPortal is not required to prepare a statement to the OAIC*]
Who will be notified of the breach?	[*Select the following options*:] [*Option 1*] HosPortal has determined that the data breach is likely to result in serious harm to individuals and therefore HosPortal will:

Description	Details
	• provide a statement to the OAIC containing a description of the breach, the type 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 HosPortal's website and publicise it [*choose this option only if the first two options are impracticable*] [*Option 2*] HosPortal 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	[*Describe 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 HosPortal's comprehensive review of the data breach*]
Names of the response staff	[*Insert names and roles of the response staff*]
Date	[*Insert date*]