# Human Services Dataset Data Breach Policy

Summary: This policy sets out procedures for responding to data breaches in connection with the Human Services Dataset

# Document approval

The Human Services Dataset Data Breach Policy has been endorsed and approved by:

Jessica Stewart

Executive Director, Family and Community Services Insights, Analysis and Research (FACSIAR)

Approved: 1 July 2021

# Document version control

| | |
|---|---|
| Distribution | Public |
| Document name: | Human Services Dataset Data Breach Policy |
| Version: | Version 3.0 – July 2021 – changes following governance transition to FACSIAR |
| This document replaces | Version 2.0 – June 2020 – Document reviewed and approved by Director (22 June 2020)<br>Version 1.0 – July 2018 – Approved by Executive Director |
| Document status: | Revised |
| Authoring unit: | FACSIAR |
| Date: | 1 July 2021 |
| Next Review Date: | 12 months from version date, or earlier if there are legislative or significant operational changes. |

# Table of contents

# 1 Purpose of policy

## 1.1 Background and policy links

This policy provides guidance for responding to a data breach in connection with the Human Services Dataset (HSDS). It sets out procedures for managing a data breach, including:

- providing examples of situations considered to constitute a data breach
- the steps involved in responding to a data breach
- providing notification to the NSW Privacy Commissioner as required by the Public Interest Direction[1] and Health Public Interest Direction[2] (the PIDs) and
- the considerations around notifying persons whose privacy may be affected by the breach.

While this policy has broad application across FACS Insights Analysis and Research (FACSIAR) activities, it is principally relevant to the FACSIAR HSDS Governance and Privacy Project Team's (Project Team) central role in coordinating the collection, use and disclosure of Personal Information and Health Information for the HSDS.

The HSDS is enabled by the Public Interest Directions (PIDs) made by the NSW Privacy Commissioner on 13 July 2018. The PIDs set out the responsibilities and requirements with respect to data breaches in connection with the HSDS. The terms of the PIDs have been included in this policy where relevant.

Effective data breach management, including notification of data breaches, assists FACSIAR in:

- reducing harm to individuals
- mitigating loss of more data
- reducing the possibility of future breaches
- managing the reputation of the Department of Communities and Justice (DCJ) and its partner agencies.

# 2 Scope and application

This policy applies to all staff (ongoing, temporary and casual) working at FACSIAR, the Data Linkage Centre (including the Centre for Health Record Linkage (CHeReL)), Australian Government Linkage Agency (including the Australian Bureau of Statistics), NSW Data Analytics Centre, Approved

[1] Made under section 41(1) of the *Privacy and Personal Information Protection Act 1998* (NSW).
[2] Made under section 62(1) of the *Health Records and Information Privacy Act 2002* (NSW).

Analysts, contracted entities and consultants engaged by FACSIAR to perform services in connection with the HSDS.

# 3 Legislation

This policy supports compliance with the following legislation:

- Public Interest Direction made under *section 62(1) of the Health Records and Information Privacy Act 2002* (NSW)
- Public Interest Direction made under *section 41(1) of the Privacy and Personal Information Protection Act 1998* (NSW)
- *Privacy and Personal Information Protection Act 1998* (NSW)
- *Health Records and Information Privacy Act 2002* (NSW)

# 4 What is a data breach?

A data breach occurs when there is unauthorised access to, unauthorised disclosure of or a loss of the HSDS. It includes any actual or suspected:

- impairment, compromise or damage to the privacy, confidentiality, reliability or integrity of the HSDS
- flaw or vulnerability of any kind in the security controls or other measures used to protect the HSDS
- misuse or loss of, interference with or unauthorised access to, modification of or disclosure of the HSDS
- breach of any privacy laws
- collection, use or disclosure of the HSDS for a purpose other than an Approved Purpose and in accordance with the PIDs
- unauthorised re-identification of any of the HSDS
- breach of any other obligations relating to the protection, security and non-disclosure of Personal or Health Information.

Practically, it may include such things as:

- unauthorised use, access to or modification of data or information systems (e.g. sharing of user login details (deliberately or accidentally) to gain unauthorised access, or make unauthorised changes to data or information systems)
- compromised user account (e.g. accidental disclosure of user login details through phishing)
- failed or successful attempts to gain unauthorised access to the HSDS or its information systems
- accidental loss or theft of data or equipment on which such data is stored (e.g. back-up data), equipment failure or malware corruption

- disruption to or denial of IT services.

Other examples specific to the HSDS under the PIDs include:

- The Data Linkage Centre, Data Analytics Entity or an Approved Analyst uses any data, for a purpose other than an Approved Purpose (e.g. accesses the data for a project other than the one they are approved to use the data for, or, an Approved Analyst downloads data to their local drive)
- A person (whether deliberately or not) is able to ascertain the identity of an individual in the data for analysis, which results in Personal Information being revealed
- An entity or person involved in the HSDS fails to protect Personal or Health Information in the manner required under section 12 of the *Personal Privacy and Information Protection Act 1998 Act* (NSW) or Health Privacy Principle 5 under the *Health Records and Information Privacy Act 2002* (NSW), or in accordance with the PIDs. (e.g. the systems or locations where any Tier One and Tier Two Data are located are compromised or subject to any unauthorised access, which results in a privacy breach.)
- If the Data Linkage Centre fails to replace an individual's Identifier Information with an arbitrary PPN before releasing that information to the Data Analytics Entity or an Approved Analyst (e.g. an Approved Analyst identifies personal information during checking process)
- If data is released to a researcher or the broader public and that data includes any Personal Information or Health Information. (e.g. if the Data Analytics Entity or an Approved Analyst does not undertake, or fails to complete correctly, the Information Protection Gates process, which results in Personal Information or Health Information being disclosed).

# 5 Responding to a data breach

When a person (staff, researchers, private contractors and consultants) detects or suspects a data breach, they must immediately notify the Director of the FACSIAR Project Team using the Data Breach Incident Report Form (**Appendix A**).

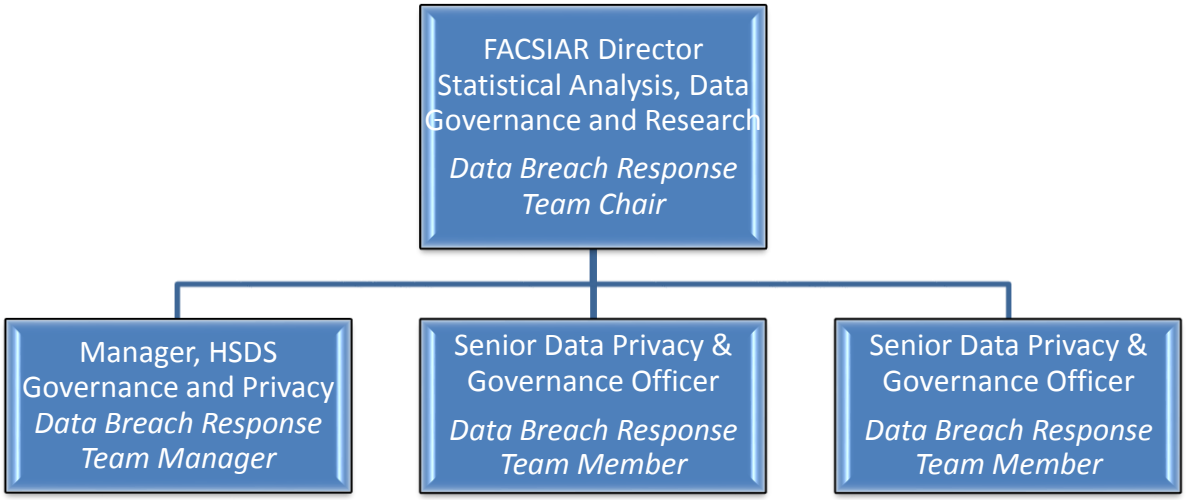
There are five key steps required in responding to a data breach:

1. Contain the breach
2. Evaluate the associated risks
3. Consider notifying affected individuals
4. Notify the NSW Privacy Commissioner
5. Prevent a repeat.

Each step is set out in further detail below. The first four steps should be carried out concurrently where possible. The last step provides recommendations for longer-term solutions and prevention strategies.

## 5.1 Data Breach Response Team

The Data Breach Response Team's structure, members and their contact details are outlined below.




| Data Breach Response Team member | Contact details |
|---|---|
| **Merran Butler**<br>**Director**<br>**Statistical Analysis, FACSIAR** | P: 02 97162192<br>M: 0491225032<br>E: merran.butler@facs.nsw.gov.au |
| **Data Breach Response Team mailbox** | dataprivacy@facs.nsw.gov.au |

When FACSIAR becomes aware of an actual or suspected data breach, the Director will convene the FACSIAR Data Breach Response Team to respond to identified data breaches. Additional members of the Data Breach Response Team may be appointed by the Director or Manager as required. If the Director is unavailable, the Manager will be responsible for taking this action.

The Data Breach Response Team is to be called on within one business day of FACSIAR being aware of an actual or suspected data breach. The Director will liaise with the person who reported the data breach in to commence investigations.

## 5.2 Step one – contain the breach

When a data breach is suspected or detected, the first priority is to take immediate actions to limit any further access to or distribution of the affected data, or any further compromise of the rest of the HSDS.

For example, the person who suspects or detects the data breach may shut down the system that has been breached, suspend the activity that led to the breach, and/or revoke or change access codes or passwords. The person may also try to recover any lost data.

All staff, researchers, contractors and consultants engaged in connection with the HSDS are under obligations to notify and assist FACSIAR with respect to any suspected or actual data breach.

## 5.3 Step two – evaluate the associated risks

The Data Breach Response Team and the person who reports the data breach will undertake an assessment of the type of data involved in the breach and the risks associated with the breach.

Some types of data are more likely to cause harm if they are compromised. For example, data that contains Personal Information and Health Information (Tier One data) will be more significant than data from which identifier information has been removed and replaced with arbitrary PPNs (Tier Two data).

As the HSDS contains linked data, the risk of re-identification could be significant in a data breach, with potential resultant harm for the individuals being re-identified.

Factors to consider include:

- **Who is affected by the breach?** The Data Breach Response Team assessment will include reviewing whether individuals and/or agencies that provide the data for the HSDS (Data Partner agencies) have been affected by the breach, how many have been affected and whether any of the individuals have personal circumstances which may put them at particular risk of harm and the ability to identify them.
- **What was the cause of the breach?** The Data Breach Response Team assessment will include reviewing whether the breach occurred as part of a targeted attack or through inadvertent oversight. Was it a one-off incident or does it expose a more systemic vulnerability? What steps have been taken to contain the breach? Has the data been recovered? Is the data encrypted or otherwise not readily accessible?
- **What is the foreseeable harm to the affected individuals?** The Data Breach Response Team assessment will include reviewing what possible use there is for the data. For example, could it be used for identity theft, threats to physical safety, financial loss, or damage to reputation? Who is in receipt of the data? What is the risk of further access, use or disclosure, including via media or online?

## 5.4 Step three – consider notifying affected individuals/participating agencies

FACSIAR recognises that notification to individuals and participating agencies affected by a data breach can assist in mitigating any damage for those affected and reflect positively on DCJ's reputation.

Notification demonstrates a commitment to open and transparent governance, consistent with FACSIAR's approach. FACSIAR adopts the approach that if the data breach creates a real risk of serious harm to an individual, the affected individual and participating agencies should be notified.

Prompt notification in these cases can help to avoid or lessen the damage by enabling the individual or participating agency to take steps to protect themselves.

There are occasions where notification can be counter-productive. For example, information collected may be less sensitive and notifying individuals about a privacy breach, which is unlikely to result in an adverse outcome for the individual may cause unnecessary anxiety and de-sensitise individuals to a significant privacy breach.

Factors the Data Breach Response Team will consider when deciding whether notification is appropriate include:

- What is the risk of harm to the individual and participating agencies?
- What steps have been taken to date to avoid or remedy any actual or potential harm?
- What is the ability of the individual and participating agencies to take further steps to avoid or remedy harm?
- Even if the individual and participating agencies would not be able to take steps to rectify the situation, is the information that has been compromised sensitive, or likely to cause humiliation or embarrassment for the individual?
- Are there any applicable legislative provisions or contractual obligations that require FACSIAR to notify affected individuals and participating agencies?
- The logistics of notifying affected individuals and participating agencies will depend in large part on the type and scale of the breach, as well as immediately practical issues such as having contact details for the affected individuals.

Affected individuals and participating agencies should be notified directly – by telephone, letter, email or in person. Indirect notification – such as information posted on FACISAR's website, a public notice in a newspaper, or a media release – should generally only occur where the contact information of affected individuals are unknown, or where direct notification is prohibitively expensive or could cause further harm.

The notification advice will be tailored to the circumstances of the particular breach. It may include:

- information about the breach, including when it happened
- a description of what data has been disclosed
- assurances (as appropriate) about what data has not been disclosed
- what FACSIAR is doing to control or reduce the harm
- what steps the person and participating agencies can take to further protect themselves and what FACSIAR will do to assist people with this
- contact details for FACSIAR Data Breach Response Team
- information about the right to lodge a privacy complaint with the NSW Privacy Commissioner.

## 5.5 Step four – notify the NSW Privacy Commissioner

The Deputy Secretary, Strategy, Policy and Commissioning, in their capacity as Data Custodian[3] of the HSDS, is required to notify the NSW Privacy Commissioner of any data breach in connection with the HSDS.

Once the Data Breach Response Team becomes aware of a potential or actual data breach, the Deputy Secretary must be briefed on the circumstances and the remedial action taken to contain the breach. Having confirmed the breach, the Deputy Secretary is required to notify the NSW Privacy Commissioner within 48 hours of when the breach is confirmed. Any briefing to the Deputy Secretary should include correspondence for this purpose.

The correspondence should contain similar content to that provided to individuals and participating agencies. The Personal Information about the affected individuals is not required. It may be appropriate to include:

- a description of the breach
- the type of Personal or Health Information involved in the breach
- FACSIAR's response to the breach
- what assistance has been offered to affected individuals and participating agencies
- whether the breach has been notified to other external contact(s).

The Data Custodian is also required to report annually to the NSW Privacy Commissioner on all actual and potential data breaches that involve Personal and Health Information.

[3] The Secretary has currently delegated the responsibility as Data Custodian to the Deputy Secretary.

## 5.6 Step five – prevent a repeat

The Data Breach Response Team will further investigate the circumstances of the breach to determine all relevant causes and consider what short or long-term measures could be taken to prevent any reoccurrence.

Preventative actions could include:

- an additional security audit of both physical and technical security controls
- a review of policies and procedures
- a review of employee training practices
- a review of contractual obligations with contracted service providers.

# 6 Mandatory Data Breach Notification Scheme

The Notifiable Data Breaches (NDB) scheme under Part IIIC of the *Privacy Act 1988* (Cth) (Privacy Act) establishes requirements for entities in responding to data breaches. The NDB scheme is aimed primarily at Australian Government agencies and private sector organisations regulated by the Privacy Act.

In the event of a data breach involving the HSDS, contracted service providers will also be subject to the Privacy Act and the NDB scheme.

# 7 Roles and responsibilities

The main roles and responsibilities for the implementation of this policy are as follows:

## 7.1 Data Custodian

The Deputy Secretary of the Department of Communities and Justice (DCJ) as Chair of the Stronger Communities Data Partnership (SCDP), has overriding custodianship, control and responsibility for the HSDS. In May 2020, the Secretary delegated responsibility as Data Custodian of the HSDS to the Deputy Secretary Strategy, Policy and Commissioning. The Data Custodian is responsible for ensuring an appropriate response to data breaches and notifying the NSW Privacy Commissioner.

## 7.2 FACSIAR Director

The FACISAR Director has overall responsibility for implementing this policy. The FACISAR Director also convenes the Data Breach Response Team and liaises with the person(s) and/or entity affected by a data breach.

## 7.3 Data Breach Response Team

The Data Breach Response Team, led by the FACSIAR Director, investigates data breaches, assesses risks and mitigates any impacts arising from data breaches. This includes drafting briefings and correspondence to the Data Custodian and NSW Privacy Commissioner, and conducting reviews of processes and systems to prevent a repeat of the incident.

# 8 Monitoring, evaluation and review

It is the responsibility of the FACSIAR HSDS Governance and Privacy Team to monitor and update this policy as required. This policy will be reviewed every year, or when any significant new information, legislative or organisational change warrants amendments to this document.

# 9 Support and advice

You can get advice and support about this policy from the HSDS Governance and Privacy Project Team who has carriage of this document.

Email: dataprivacy@facs.nsw.gov.au

If you are reviewing a printed version of this document, please refer to our website to confirm that you are reviewing the most recent version of the policy.

Following any subsequent reviews and approval this policy will be uploaded to our website and all previous versions removed.

# 10 Definitions

The table below is a list of terms, keywords and/or abbreviations used throughout this document.

| Term | Definition |
|---|---|
| Approved Analyst | A person (including a researcher or analyst) that:<br>a) has been approved by the Data Custodian to provide Analytical Services for and on behalf of the Project Team; and<br>b) is under a contractual obligation to comply with the PPIP Act and HRIP Act to the extent modified by a relevant Public Interest Direction. |

| Term | Definition |
|---|---|
| Approved Purpose | Any activity, task, work, step, process or measure that facilitates or enables the Project Objectives. |
| Data Analytics Entity | A data analytics entity or function that is operated by a Public Sector Agency, which complies with the NSW Cyber Security Policy, and that is engaged by the Project Team to undertake Analytical Services of the Project, such as the DAC (as defined in section 4 of the *Data Sharing (Government Sector) Act 2015* (NSW)) or such other entity that is under a contractual obligation to comply with the PPIP Act and HRIP Act to the extent modified by the Public Interest Directions.<br><br>This includes, for example Taylor Fry Consulting Actuaries and the NSW DAC. |
| Data Linkage Centre | A data linkage service or function that is operated by a Public Sector Agency that is compliant with the current NSW Cyber Security Policy, and that is engaged by the Project Team to undertake data linkage for the Project, such as the Centre for Health Record Linkage (CHeReL) or such other entity that is under a contractual obligation to comply with the PPIP Act and HRIP Act to the extent modified by the PIDs/ |
| DCJ | The Department of Communities and Justice |
| Data Custodian | Currently, the Deputy Secretary Strategy, Policy and Commissioning |
| Health Information | The meaning of Health Information is given in section 6 of the HRIP Act. In the HRIP Act, Health Information means:<br><br>(a) personal information that is information or an opinion about:<br>i. the physical or mental health or a disability (at any time) of an individual, or<br>ii. an individual's express wishes about the future provision of health services to him or her, or<br>iii. a health service provided, or to be provided, to an individual, or |

| Term | Definition |
|---|---|
| | (b) other personal information collected to provide, or in providing, a health service, or<br>(c) other personal information about an individual collected in connection with the donation, or intended donation, of an individual's body parts, organs or body substances, or<br>(d) other personal information that is genetic information about an individual arising from a health service provided to the individual in a form that is or could be predictive of the health (at any time) of the individual or of a genetic relative of the individual, or<br>(e) healthcare identifiers.<br><br>For the purpose of this policy, Health Information includes information set out in Part A of Schedule 1 of the *Public Interest Direction under section 62(1) of the HRIP Act*. |
| Human Services Data | Data or information (which may include Personal Information and Health Information) within a Participating Agency's or its contractors' or agent's records or system in connection with a Public Sector Agency's or other government agencies' interaction with, or provision of supports, services or programs to, an individual. |
| HRIP Act | *Health Records and Information Privacy Act 2002* (NSW) |
| Information Protection Gates | The privacy verification process and checks that will be undertaken by the Data Analytics Entity or an Approved Analyst in accordance with the PIDs and before information held by the Data Analytics Entity or an Approved Analyst is externally released or disclosed to:<br>a) ensure compliance with the PIDs;<br>b) ensure that only de-identified information is released or disclosed to a third party; and<br>c) prevent re-identification of information by a third party, including a Participating Agency. |

| Term | Definition |
|---|---|
| Personal Information | The meaning of Personal Information is given in section 4 of the PPIP Act.<br><br>In the PPIP Act, Personal Information means information or an opinion (including information or an opinion forming part of a database and whether or not recorded in a material form) about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion.<br><br>*As an example, Personal Information can be considered to be information that identifies you. Personal Information could include :*<br><br>• *a record which may include your name, address and other details about you*<br>• *photographs, images, video or audio footage*<br>• *fingerprints, blood or DNA samples.*<br>*Source: https://www.ipc.nsw.gov.au/*<br><br>For the purpose of this policy, Personal Information includes the information set out in Part A of Schedule 1 of the *Public Interest Direction under section 41(1) of the PPIP Act*. |
| PPIP Act | *Privacy and Personal Information Protection Act 1998* (NSW) |
| Public Interest Direction | Public Interest Directions (PIDs) can be made by the NSW Privacy Commissioner under section 41 of the Privacy and Personal Information Protection Act 1998 (PPIP Act) or section 62 of the *Health Records and Information Privacy Act 2002* (HRIP Act) to waive or make changes to the requirements for a public sector agency to comply with an Information Protection Principle (IPP) or a Health Privacy Principle (HPP) respectively. The NSW Privacy Commissioner issued two Public Interest Directions for the TFM Project, which are referenced in point 3 of this policy. |
| Tier One Data | Human Services Data that has not been through any de-identification process to remove any Personal Information and Health Information. |

| Term | Definition |
| --- | --- |
| Tier Two Data | Data derived from Tier One Data that has Identifier Information removed and been allocated a PPN in accordance with the PIDs. |
| Tier Three Data | Aggregated Tier Two Data that has been through the Information Protection Gates process in accordance with the PIDs. |

# Appendix A: Data breach incident report form

This form is used to inform FACSIAR of a data breach incident relating to the Human Services Dataset.

Beforecompleting this form we recommend that you read the Human Services Dataset Data Breach Policy.

This form is to be sent to: dataprivacy@facs.nsw.gov.au

**PERSON MAKING NOTIFICATION**

| | |
|---|---|
| **Name** | |
| **Role** | |
| **Phone number** | |
| **Email** | |
| **Organisation name** | |

**ORGANISATION DETAILS** *(IF DIFFERENT FROM PERSON MAKING NOTIFICATION)*

| | |
|---|---|
| **Organisation name** | |
| **Authorised Representative** | |
| **Phone number** | |
| **Email** | |

**DETAILS OF THE DATA BREACH**

| | |
|---|---|
| **Date the breach occurred*** | |

**You may provide your best estimate if the exact date is not known*

| | |
|---|---|
| **Date the breach was discovered** | |

| | |
|---|---|
| **Cause of the data breach** | ☐ Accidental loss or theft of data<br>☐ Use of data for a purpose other than an approved purpose<br>☐ Unauthorised use, access to or modification of data or information systems<br>☐ Personal information is present in the data used for analysis (Tier 2 data) |

| | |
|---|---|
| | ☐ Personal information is present in any data released externally (Tier 3 data)<br>☐ An individual is identifiable in any data released externally (Tier 3 data)<br>☐ Compromised user account<br>☐ Compromised systems<br>☐ Malicious or criminal attack<br>☐ Human error<br><br>**Other (please describe):** |

**Describe how the data breach was identified**

| |
|---|
| |

**Describe how the data breach occurred**

| |
|---|
| |

**Describe kind or kinds of Personal Information involved in the data breach**

| |
|---|
| |

In addition, please select any categories that apply:

☐ Health information

☐ Other sensitive information

| **Number of individuals affected by the data breach*** | |
|---|---|

**You may provide your best estimate if the exact number is not known*

**What is the risk of harm to the affected individuals?**

| |
|---|
| |

## REMEDIAL ACTIONS

**Describe any remedial actions your organisation has taken up to date to correct what has occurred.**

**Describe any actions your organisation has taken, or is intending to take, to prevent reoccurrence.**

**Has feedback been provided to any staff member(s) involved in the incident?**

**If so, what feedback was provided, on what date and by whom?**