ACT Government | ACT Health

POLICY DOCUMENT

Transferring Confidential Information Policy and Procedure

Document number	**AHDPD-06:2023**
Effective date	10 August 2023
Review date	10 August 2024
Author branch	Data Analytics Branch
Endorsed by	Executive Board (Operational)
Audience	All staff and contractors
Version number	1.0

Contents

Policy Statement

In the ACT there is legislation that prescribes how organisations manage and protect the confidentiality and security of the data they collect or store. There are obligations for organisations to protect the sensitive or classified information they hold, and to ensure these data are only accessed by those with a need-to-know. Furthermore, the Australian community expects that any information provided to the government about them will be safe from unauthorised access or disclosure.[1]

The ACT Health Directorate (ACTHD) is committed to safeguarding the security of the information it holds or hosts and maintaining the privacy of individuals represented with data holdings.

Purpose

The *Transferring Confidential Information Policy and Procedure* describes how personal information, personal health information (refer to Glossary) or operationally sensitive information (confidential information that relates to ACTHD business or operations) is to be transferred to internal recipients or externally, to trusted recipients such as those in Australian government organisations or authorised researchers. This policy describes how data are to be transferred once it has been determined that the data can properly be disclosed in accordance with the *Data Disclosure Policy.*

In the context of a Five Safes (Data Sharing Principles) disclosure risk assessment framework (the best practice approach to assessing and managing risks associated with data sharing and release), and as outlined in the *Data Disclosure Policy*, the secure transfer of confidential information forms a critical part of the 'Setting Principle'.[2]

Scope

This policy applies to all ACTHD workers including permanent, temporary, and casual employees, students, external contractors, consultants and volunteers. ACTHD workers are required to comply with all obligations in relation to data and information privacy, protection and management as directed in relevant legislation and policies.

This policy covers all data or digital information held by ACTHD that is shared between Canberra Health Services (CHS) and ACTHD, or held solely by ACTHD that relates to the conduct of ACTHD business or operations. It includes data or information acquired by ACTHD from external sources or provided by any external data custodians.

This policy does not consider how data is internally transferred between systems or applications, including development, test or production environments. It does not include the routine, business-as-usual transfer of data between CHS and ACTHD servers, which is controlled through other arrangements.

1 OAIC Australian Community Attitudes to Privacy Survey 2020

2 Department of the Prime Minister and Cabinet. *Best practice guide to applying data sharing principles.* 2019

This policy does not include other Five Safes (Data Sharing Principles) assessments that need to be undertaken prior to sharing or releasing confidential information. These are addressed in the *Data Disclosure Policy.*

This policy does not consider the statistical safeguards or protections that are to be applied to data prior to transfer that help minimise harm to individuals or organisations should personal information, personal health information or other confidential information be disclosed to unauthorised recipients. These are addressed in the *Statistical Disclosure Controls Policy and Procedure.*

Legislative framework

In the ACT, certain legislation defines personal information and personal health information, and how that information is to be protected and used. Personal information (including sensitive information) is defined under the *Information Privacy Act 2014* (ACT) [3]. This Act contains 13 Territory Privacy Principles that set standards, rights and obligations for the collection, use, disclosure, storage, access, and correction of personal information.

Personal health information is defined under the *Health Records (Privacy and Access) Act 1997* (ACT).[4] There are 12 Health Privacy Principles outlined in this Act that stipulate how personal health information is to be securely collected, stored, accessed, used, disclosed, and managed.

Examples of personal information (including sensitive information) and personal health information can be found within the legislation and in the *Data Breach Policy and Procedure.*

The problem

The Australian Bureau of Statistics defines confidentiality as 'protecting the secrecy and privacy of information collected from individuals and organisations, and ensuring that no data is released in a manner likely to enable their identification'.[5]

Confidentiality of information refers to 'the limiting of access to information to authorised persons for approved purposes.'[6] There may be risks to the confidentiality of personal information or personal health information for patients (consumers), health professionals or other individuals, or risks for ACTHD where operationally confidential information is made available to others without authorisation or adequate protections.

The disclosure of personal information, personal health information or operationally confidential information may be necessary to meet business needs. Circumstances may include transfer as part of an authorised data sharing agreement for a purpose permitted under the relevant legislation, such as the provision of data to the Centre for Health Record Linkage for inclusion in the Master Linkage Key, or to the Australian Institute of Health and Welfare for inclusion in national minimum

3 *Information Privacy Act 2014* (ACT)
4 *Health Records (Privacy and Access) Act 1997* (ACT)
5 Australian Bureau of Statistics. Glossary.
6 Australian Government. Protective Security Policy Framework. *8 Sensitive and Classified Information,* p 1.

data sets or registries. These agencies have robust policies and procedures in place to protect confidentiality, prevent interception or unauthorised access during digital transfer. Transfers of data also occur between ACTHD and CHS. For example, data are regularly shared to enable the effective and timely management of COVID-19 in the ACT.

Email security

Where personal information held by an organisation is accessed or disclosed without authorisation, or is lost, a data breach has occurred.[7] As such, a data breach may occur where personal information or personal health information is accidentally or intentionally disclosed without authorisation, by email or other means, to recipients who do not have authority to view that information.

In their July to December 2022 notifiable data breaches report, the Office of the Australian Information Commissioner stated that human error breaches across all sectors in Australia accounted for the second largest source of data breaches (25%) – after malicious or criminal attack (70%). The top mechanism for human error data breaches was sending personal information to the wrong recipient via email (42%) followed by unauthorised disclosure (unintended release or publication) that accounted for 33% of human error data breaches. [8]

Secure information transfer

There are certain actions that should be implemented to assist in reducing the likelihood of a data breach when transferring confidential files to internal or external recipients:

- Ensure the disclosure is authorised
- Use the safest mode of transfer
- Use protective security markers
- Appropriately manage the data prior to transfer.

These actions are described below.

Authority to disclose

Refer to the *Data Disclosure Policy* which outlines the steps that must be taken to obtain the necessary authorisation to disclose data to approved internal or external recipients. The *Data Disclosure Policy* mandates the completion of a Five Safes (Data Sharing Principles) assessment that is approved by the relevant data custodian. This approved assessment must be documented within the enterprise records management system (Objective).

Mode of transfer

There are mechanisms that minimise disclosure risks during the transfer of confidential information between internal or external recipients. As detailed below, provide direct access to the information where feasible, or use an authorised secure file transfer system.

7 Office of the Australian Information Commissioner. *Part 1: Data breaches and the Australian Privacy Act.*
8 Office of the Australian Information Commissioner. *Notifiable Data Breaches Report: July to December 2022*

Non-permitted modes of transfer

Microsoft Outlook

Microsoft Outlook must not be used to email personal information, personal health information, 'de-identified' data, or operationally confidential information to any recipient. Refer to the *Statistical Disclosure Controls Policy and Procedure* for detailed information about de-identification mechanisms.

Microsoft Outlook must not be used to email personal information, personal health information or operationally confidential information to any recipient.

Two exceptions

1. Email correspondence that is related to clinical care for a particular individual. This would include an email to an individual to advise them about their clinical care, or an email to a health-care provider for an individual or patient in their care. These emails should be sent using the appropriate protective security marking (**OFFICIAL: Sensitive – Personal Privacy**).

While Microsoft Outlook can encrypt an email, this encryption only applies while the email is in transit - any recipient can still read the mail, regardless of the protective security marker applied to the email.

2. Internal business-as-usual emails such as those relating to the performance or work health and safety of staff member/s.

Microsoft OneDrive

This is a cloud storage system that enables files to be shared with ACT Government staff. As this system is not part of ACT Government data management systems, it must not be used for sharing confidential or 'de-identified' files.

Microsoft Teams

Microsoft Teams chat, phone calls and meetings are important business enabling functions. Although Microsoft Teams document management functions can be configured to allow access to external parties, an external party can see all the contents on an individual Teams site. There are no end-user tools enabling the Teams site owners to see what documents or data has been accessed by individual members.

As the Microsoft Teams platform is not part of the ACT Government enterprise records data management system it must not be used to share or disclose confidential or 'de-identified' information.

Microsoft Sharepoint

As Microsoft Sharepoint is not part of the ACT Government enterprise records data management system, it must not be used to share or disclose confidential or 'de-identified' information.

Portable storage devices

Personal information, personal health information or operationally confidential information (including 'de-identified' information) **must not be stored or disclosed** via USB, thumb drive, compact disc, mobile phone, any other portable storage device, or non-government computer.

Most ACT Government computers have been configured so that information cannot be saved to a portable storage device.[9] To prevent the introduction of malicious executable files, USB files inserted into ACT Government computers are configured to only 'read' files.

Exception

The exception is USB devices that are provided to individuals that contain clinical information, such as medical imaging that relates to that person or a person in their care. Most relevant patient information such as imaging, is however, usually available through an online portal.

File sharing websites (Dropbox, Google Drive)

External file sharing websites such as Dropbox, iCloud, Google Drive and other cloud-based services such as Google Docs, Google Sheet and Zoho are not supported by ACT Government IT infrastructure. This includes any related mobile applications. These services must not be used for transporting or sharing data as they are outside ACT Government control and auditing.

IT administrators can use tools to detect the use of unofficial services, including Adobe document cloud, Amazon Drive, Box, Dropbox, Google Drive, HighTail, iCloud, TitanFile, Google Docs, Google Sheets, Zoho Office and many other services.

Paper records

Once a paper record containing personal information, personal health information or operationally sensitive information is disclosed (or misplaced), there may be a loss of control about who accesses that information and for what purpose. The disclosure of confidential information in paper records is not permitted.

Exception

Paper records containing personal information or personal health information may be provided to an individual where this information relates to the clinical care of that individual, or an individual in their care. This would include advice about clinical care, or the provision of a medical certificate, care plan or test results.

Permitted modes of transfer

Provision of direct access

Where recipients are internal to ACTHD, where possible, enable authorised recipients to have direct digital access through a secure portal to the information that is to be shared. This approach limits duplication of records and ensures that the data are only stored and accessed in IT managed environments.

9 ACT Government. OneGov Service Centre. USB Restrictions.

Secure file transfer systems

Where direct access to the information is not feasible, use an ACT Government, ACT Health or another Australian Government-sponsored secure file transfer system. Use this system for transfers of confidential information to internal or external recipients. These systems require user identification through multi-factor authentication processes.

Where direct access to the information is not feasible, use an ACT Government, ACT Health or another Australian Government-sponsored secure file transfer system for transfers of confidential information to internal or external recipients.

Kiteworks is the system supported by ACTHD. Aside from its capacity to manage the secure transfer of large files, it offers other security advantages. For example, if a mistake is identified after sending the files, the attachments can be withdrawn from the sent message. The file links are deactivated so that recipients cannot access the files, but the message itself is not withdrawn. Where necessary, files can also be viewed but not downloaded. In addition, it allows file transfers and recipient access to be audited.

Alternatively, secure file transfer platforms sponsored by Australian Government organisations such as the Australian Institute of Health and Welfare or the Centre for Health Record Linkage can be used for the receipt or external transfer of confidential information.

External agencies can use the ACTHD Kiteworks instance to send confidential information to a business area within ACTHD that holds a Kiteworks licence.

Requesting access to Kiteworks

Licenses are required for Kiteworks at no cost to business areas. To obtain access, use Jira to 'Request application to an application'. Under the 'What application do you require access to', select 'Other'. In the 'Description' section, type in Kiteworks. Also state the length of time the license is required, add ACTGOV user-names and email addresses of those requiring access; or add external user names and email addresses for those who need to upload files.

Passwords

As the Kiteworks platform is housed on infrastructure accredited to hold **PROTECTED** level information, and senders and recipients are authenticated prior to access, it is not necessary to password protect files prior to transmission.

Protective Security Markers

The **OFFICAL: Sensitive - Personal Privacy** protective security marker must be applied to any information that contains personal information or personal health information, including Word documents or spreadsheets that are contained within a secure file transfer.[10] The **OFFICIAL: Sensitive** marker should be used where there is confidential business information. This alerts the recipient to the nature of the information they are about to access and store.

10 ACT Health Records Management. *Dissemination Limiting Marker*.

Data management

There are safeguards that can be implemented prior to the transfer of confidential information to help minimise harm to individuals or organisations should this information be disclosed to unauthorised recipients. These safeguards are:

- the implementation of protective statistical disclosure controls
- utilising the separation principle
- double-checking.

Statistical disclosure controls

Prior to sharing, certain statistical disclosure controls can be applied to cells within an **aggregate dataset** (information is grouped into categories where values are combined) or to **unit record data** (or **microdata**: each record contains information about a data provider)[11] to manage disclosure privacy and confidentiality risks. Refer to the *Statistical Disclosure Controls Policy and Procedure* for detailed information about how to assess and manage re-identification risks where data are disclosed to authorised internal or external recipients.

Separation principle

This is a technique used to protect the identities of individuals within a dataset or extract during the linking and merging of integrated datasets.[12] The technique can be applied during routine unit record (microdata) file transfers to mitigate harm should the data become accessible to an unauthorised recipient.

Where it is necessary to include personal information in a file transfer to meet a business need, separating the personal information (personal identifiers) from the 'content' (for example - personal health, geographic location, financial or other information that relates to the individual) and sending two separate transmissions should be considered. Transmissions should be sent to two different authorised people so that no single recipient receives or has access to both files. Personal identifiers and a unique identification number are transmitted in one secure transfer. The same unique identifier and the 'content' data are transmitted in a second separate and secure transfer. While this does not prevent a data breach if either file transfer is sent to an unauthorised recipient, it does limit the potential for harm to affected individuals.

To add extra security, each unique identifier should be pseudonymised or randomly generated for each disclosure use case. Do not disclose a re-identifiable number (such as a medical record or Medicare number).

Where the separation principle is applied, files containing personal information are stored in a different location (with different access arrangements) to the content data.

11 Australian Bureau of Statistics Glossary

12 Australian Government. National Statistical Services. *The Separation principle.*

Double checking

Ask a colleague to check the intended recipients against those included in the transmission, prior to sending. Together, check that you have included the correct email addresses for the recipients when using secure file transfer systems.

If you make a mistake

Refer to the *Data Breach Policy and Procedure* on the Policy Register that outlines the steps that must be undertaken when a data breach occurs – where, for example, personal information or personal health information is sent to the wrong recipient or there was no authority to disclose the information.

Records Management

All staff are responsible for documenting information about file transfers on the enterprise records management system (Objective). This includes filing data requests and authorisations for release. It also includes the storage of data received from a secure transfer on an enterprise-managed IT system within an appropriate IT-managed repository or server.

Personal information, personal health information or confidential information should not be stored on computer desktops, portable devices or personal drives.

Roles and Responsibilities

Position	Responsibility
All staff	Adherence to this and related policies and procedures
Data custodians	Authorise data disclosures as appropriate
Cyber Security Hub	Up-to-date technical advice

Evaluation

Outcome Measures	Method	Responsibility
Where a data breach occurs during the transfer of confidential information, harm to affected individuals will be minimised through appropriate management of data prior to sending.	Data Breach Register reports	Director, Data Strategy and Governance All staff

Glossary

Term	Definition
Consumer – as defined in the *Health Records (Privacy and Access) Act 1997 (ACT)*	An individual who uses, or has used, a health service.
Personal health information – as defined in the *Health Records (Privacy and Access) Act 1997 (ACT)*	Personal health information, of a consumer, means any personal information, whether or not recorded in a health record— (a) relating to the health, an illness or a disability of the consumer; or (b) collected by a health service provider in relation to the health, an illness or a disability of the consumer.
Personal information – as defined in the *Information Privacy Act 2014 (ACT)*	Information or an opinion about an identified individual, or an individual who is reasonably identifiable— (i) whether the information or opinion is true or not; and (ii) whether the information or opinion is recorded in a material form or not; but (b) does not include personal health information about the individual.
Sensitive information – as defined in the *Information Privacy Act 2014 (ACT)*	Sensitive information, in relation to an individual, means personal information that is— (a) about the individual's— (i) racial or ethnic origin; or (ii) political opinions; or (iii) membership of a political association; or (iv) religious beliefs or affiliations; or (v) philosophical beliefs; or (vi) membership of a professional or trade association; or (vii) membership of a trade union; or (viii) sexual orientation or practices; or (ix) criminal record; or (b) genetic information about the individual; or (c) biometric information about the individual that is to be used for the purpose of automated biometric verification or biometric identification; or (d) a biometric template that relates to the individual.

Version Control

Version	Date	Comments
V0.1	October 2022	Data Strategy and Governance, Cyber Hub ACTHD
V 0.2	November 2022	DSG, includes Five Safes and Data Disclosure Policy
V0.3	March 2023	Legal Policy review
V1.0	June 2023	Final revision