Information security

Version: 3
Published: 14 Jan 2025, 7:25 PM
Approved: 14 Jan 2025, Sarah Tilley
Last edited: 9 Oct 2024, 5:18 PM
Next review: 9 Oct 2025

Introduction

Connect Allied Health (CAH) realises the importance of information security to collect, use and retain personal information on a daily basis (with consent from the participant/representative). Under privacy laws, we are required to take reasonable steps to keep all personal information access safe from accidental or deliberate misuse. This policy aims to safeguard our information and our ICT (information and communications technology) resources from those with malicious intent.

Definitions

Term	Definition
adware	Software that automatically displays or downloads advertising material such as banners or pop-ups.
backdoor	A technique to bypass a computer system's security undetected in order to access a computer or its data.
bot (malicious bot)	Self-propagating malware that infects its host and connects back to a central computer. Malicious bots can then be used to spy on user activity, steal passwords, relay spam, open backdoors, or perform attacks on other computers, websites or resources.
data breach	An incident where personal and/or sensitive information has been accidentally or deliberately accessed and/or disclosed in an unauthorised fashion. Some common examples of data breaches include: • personal information accidentally mailed or emailed to the wrong recipients • a locked filing cabinet containing personal files is broken into or left unlocked and accessed by unauthorised persons • a computer or storage device used to store personal information is compromised as a result of a security breach, malware or poor security practices • personal information in printed form or on an insecure storage device is left in a public place • personal information accidentally or deliberately shared on social media.

malware	Software which is specifically designed to disrupt, damage, or gain authorised access to a computer system. Includes viruses, ransomware, spyware, adware and other.
patch	See "update".
phishing	Fraudulent emails purporting to be from reputable companies sent to fool users into revealing personal information such as passwords, bank account details or credit card numbers.
ransomware	A type of malicious software designed to block access to a computer system until a sum of money is paid.
spam	Also known as junk email, spam is unsolicited email usually to containing advertising, malware, or phishing.
update (or patch)	An update to a computer, tablet or smart phone operating system usually to correct security flaws (vulnerabilities) or correct errors.
virus	A type of malicious software that installs without the user knowing. A virus can replicate itself, modify computer programs, corrupt data, open backdoors, or install adware, bots or ransomware.
vulnerability	A flaw in a system that can leave it open to attack.

Applicability

When

- applies to **all** information and communications technology (ICT) used by the organisation including computers, computer networks, internet connections, smart phones and email
- applies when unsolicited phone calls, emails or text messages are received.

Who

- applies to **all** representatives including key management personnel, full time workers, part time workers, casual workers, contractors and the director.

Outcomes

Outcome: Management of each participant's information ensures that it is identifiable, accurately recorded, current and confidential. Each participant's information is easily accessible to the participant and appropriately utilised by relevant workers. To achieve this outcome, the following indicators should be demonstrated:

- Each participant's consent is obtained to collect, use and retain their information or to disclose their information (including assessments) to other parties, including details of the purpose of collection, use and disclosure. Each participant is informed in what circumstances the information could be disclosed, including that the information could be provided without their consent if required or authorised by law.
- Each participant is informed of how their information is stored and used, and when and how each participant can access or correct their information, and withdraw or amend their prior consent.
- An information management system is maintained that is relevant and proportionate to the size and scale of the organisation and records each participant's information in an accurate and timely manner.
- Documents are stored with appropriate use, access, transfer, storage, security, retrieval, retention, destruction and disposal processes relevant and proportionate to the scope and complexity of supports delivered.

Personal information

All personal information, including that of participants and workers, must be:

- Stored securely with reasonable security precautions against misuse or unauthorised access (e.g., electronic information is password protected with authenticator; hard copies stored in locked office under lock and key, CAH laptops for clinical team as appropriate).
- Readily accessible to appropriate staff.
- Retained for the required time (7 years).
- Destroyed securely when no longer required.
- Not shared with any third parties without correct consent.

Privacy Statement

Connect Allied Health is committed to ensuring the privacy of personal information gathered about our participants and their families by responding to the 13 Australian Privacy Principles in the Privacy Act, as amended in 2012, dealing with the collection, use, disclosure and data security of personal information.

Connect Allied Health works on the principle that individuals have the right to be informed and know what personal information is collected about them, the method of collection, why this information is collected, the method of this information storage, who has access to this information and who it may be disclosed to.

The type of personal information that Connect Allied Health collects and holds

Personal information is defined as information – in any format, gathered from any source – which identifies or could be used to identify the individual. This includes, but is not limited to the following:

- Contact details;
- Sensitive information on the health, sex or abilities of the individual; and
- Details about an individual's accessed services.

The personal information that may be gathered includes, but is not limited to the following:

- Name, address, telephone number, email address and any other necessary or required contact information;
- Gender, marital status, guardian details, or any relevant custody details;
- Emergency contact information;
- Details of the individual's school, care facility, family doctor, or any other relevant health professional;
- Details regarding the current and previous medical history of the individual.

How Connect Allied Health collects and holds personal information

Connect Allied Health will only collect information about the individual that is required to provide services or is required for us to meet our duty of care obligations or is required by our contractual obligations or relevant regulatory or legislation requirements. Connect Allied Health will generally only collect personal information about the individual from other sources with an individual's consent, or if required by law.

Connect Allied Health will only collect information in a fair, non-intrusive and lawful way. Where possible, this information will be collected directly from the individual rather than from others.

Data Security

Connect Allied Health takes reasonable steps to protect the personal information it holds as online data from misuse and loss, unauthorised access, disclosure or modification.

Physical Information Storage

Connect Allied Health (CAH) takes reasonable steps to ensure all personal information stored in a physical form (i.e. paper copies) are protected from misuse and loss, unauthorised access, disclosure or modification. CAH will only use paper copies as required.

The purposes for which Connect Allied Health collects, holds, uses and discloses personal information

Connect Allied Health uses or discloses the personal information for individuals for the purpose for which it was collected, or is related to the primary purpose. Personal information is collected primarily for the following purposes:

- Provision of therapy, support and support coordination services;
- Assessment and reporting purposes;
- State, federal and regulatory audits; and
- Training and induction of employees and students.

The exception to this is where personal information is required to be disclosed to external organisations or bodies by law, or as part of Connect Allied Health's obligations as determined by the State Governments Information Sharing Guidelines (see below).

Connect Allied Health do not provide personal or sensitive information to overseas recipients.

How an individual may access personal information about the individual that is held by Connect Allied Health and seek the correction of such information

Individuals have the right to access and seek correction of their personal information held by Connect Allied Health. In order to access or correct information, please contact our head office on 08 8337 8770 or email admin@connectalliedhealth.com.au

How an individual may complain about a breach of the Australia Privacy Principles, that bind Connect Allied Health, and how Connect Allied Health will deal with such a complaint

Individuals are encouraged to follow the Connect Allied Health complaints and feedback procedure if they have a complaint about the way in which their personal information is gathered, held and handled by contacting our office on (08) 8337 8770. If individuals are not satisfied with the handling of their complaint, or feel that the appropriate actions and steps were not made, we encourage individuals to contact the office of the Australian Information Commissioner on 1300 363 992 for further assistance.

Accuracy of Information

Connect Allied Health will take reasonable steps to ensure the accuracy and completeness of the personal information collected, used or disclosed. Wherever possible and reasonable, steps will be taken to ensure information is current and to correct incomplete, inaccurate or outdated personal information.

Information Sharing Guidelines

Connect Allied Health follows the South Australian Government Information Sharing Guidelines for Promoting Safety and Wellbeing. Connect Allied Health will work closely with other agencies to coordinate supports to provide the best quality, multidisciplinary service to the individual and their family. Under the Information Sharing Guidelines, informed consent will be sought and respected from the individual and their family before personal information is shared between organisations, unless the following situations apply:

- It is unsafe or impossible for Connect Allied Health staff to gain consent, and/or consent has been refused and the below situation is true
- Without information being shared, the individual, a member of their family, or a member of the public will be at risk of serious harm, abuse or neglect, or they pose a risk to their own or the public's safety.

Transfer of Personal Information to Third Parties

Written consent from the individual is needed prior to the release of information to any third parties. Requests can be made via email to admin@connectalliedhealth.com.au

Exceptions to this may apply when applying the Information Sharing Guidelines and the transfer of information is to facilitate service provision where there is a risk of harm to the individual, their family or the public.

When transferring information, reasonable steps will be taken to maintain the security and privacy of the personal information that is being transferred.

Privacy Policy

Connect Allied Health does not collect or track personal information from its site visitors. Generic information from server logs may be used to track the number of hits to the site, and to find out what types of browser software are used by visitors. This information will be used only in aggregate form, and used solely for improving web site design. Information provided via the enquiry form is used solely to assist with fulfilling the user's needs and is not sold to any 3rd parties or used in advertising or promotions.

General information security precautions

- access to all personal information is strictly based on a need-to-know basis
- when sending group emails, use the 'BCC' field rather than the 'To' field so email recipients cannot see other recipients' email addresses
- always password lock computers when unattended (shortcut to password lock a Windows computer is "Windows key + L")
- operating system updates must be installed promptly after they become available
- active anti-virus software must be installed and kept up-to-date on all computers
- internet modem routers must have security (i.e. firewall) enabled
- internet modem routers and network security cameras must have a strong admin password
- WiFi networks must have strong passwords to gain access
- only download or install software from trusted sources
- work from One Drive; avoid downloads from One Drive
- access to CAH computers and laptops
- mail servers should be configured to use encryption
- computers should be configured so admin rights are restricted to key management personnel (i.e. so workers can't install software)
- when an employee leaves, their access to the organisation's computer network and email systems is removed promptly and allocated laptop returned
- workers must not download information onto work computers
- Unified Threat Management (UTM)

    - UTM consists of a device that filters all data traffic coming in and out of the network
- Multi Factor Authentication for Microsoft 365; use of authenticators to access CRM
- auditing of Microsoft 365 activity has been turned on
- staff who have left the organisation have been stopped from accessing Microsoft 365 upon their departure from the organisation
- access to data folders is restricted

Passwords

- all computers which store or access personal information require unique and strong passwords to gain access
- passwords must not be shared or reused between computers, users, or different applications (e.g., password for Facebook should be different to the password for Google mail which should be different to the computer login password)
- passwords should not be left written on paper left lying around
- passwords should be regularly changed i.e. every three months
- always use strong passwords with a minimum of 8 characters or password phrases which include a combination of:
    - lower case letters (abcdefghijklmnopqrstuvwxyz)
    - upper case letters (ABCDEFGHIJKLMNOPQRSTUVWXYZ)
    - numbers (1234567890)
    - symbols (!@#$%^&*()-=_+,.<>/?’”[]{}|\`~:;"')
- do not use easy-to-guess passwords such as “123456”, “password” or “qwerty” etc

Avoiding scams and ransomware

- do not pay the ransom if your computer is infected with ransomware
- be aware of current scams targeting individuals and businesses by following government sites such as SCAMWATCH
- be suspicious of any unsolicited emails or text messages purporting to be from government agencies, banks, delivery services or other similar organisations—check the sender’s email address for clues (scammers will try to fool you with a very similar email sender’s address) and delete any suspicious emails or look up the organisation’s main phone number and call if unsure
- be suspicious of unsolicited phone callers purporting to be from Telstra, Microsoft, the Australian Tax Office and do not provide any information, instead end the call—if unsure, look up their main number and call it to confirm
- do not allow remote access to any computer or network resource by a third party unless it is arranged with a known and trusted IT services provider.

Portable devices

- smart phones and mobile computers must not be left unattended in public
- smart phones and mobile computers must not be left in vehicles (locked or unlocked)
- smart phones and mobile computers must not be stored in checked-in baggage when flying
- portable storage devices (e.g., USB drives, USB flash drives) should be vetted and checked for viruses prior to their use
- portable storage devices require password protection if they are used to store any personal information (such as employee or participant information).

Social media

- only those authorised to do so should represent the organisation on social media
- personal information and confidential company information must not be posted or shared on social media
- when an employee leaves, their access to the organisation's social media must be promptly removed.

Printed material

- personal information in printed format must be stored securely when not being used
- personal information in printed format must not be left lying around
- when no longer required, printed material that contains personal information must be shredded or removed by a secure document destruction service.

Incidents

- a data breach or breach of privacy and confidentiality is an incident, follow the Manage incident process to manage and resolve the incident
- incidents where individuals are at serious risk of harm as a result of the breach must be advised of the breach and assisted with ways to reduce their risk of harm from the breach
- incidents where individuals are at serious risk of harm as a result of the breach are reportable to the Office of the Australian Information Commissioner
- report incident to the NDIS Commission as appropriate, in specified time frame (refer to Incident Management Policy) .

IT Security Summary

- Access to Office computers
    - Each user has a unique user ID and password that they are allowed to access
    - Each user has been setup on the computers that they are allowed to access.
- Applications
    - Applications are cloud based and access is controlled via user ID and password.
    - Backup and recovery of data held in cloud applications is handled by the application vendor.
- Office 365
    - Office 365 is used for email and file (documents, spread sheets etc) management.
    - Access to Office 365 is via unique user ID and password
    - Password conventions are managed within Office 365
    - Administration access to Office 365 is restricted to the IT Support
    - Access to Office 365 is either via;
        - browser – requires the user to login or
        - Outlook (desktop app) and File Explorer – access via login to computer
    - Restrictions to Data held in Office 365 Team Site
        - Certain folders within the Office 365 Team Site are restricted to specific staff members.
        - Control of the access is managed by IT Support
    - Backup:

        - Office 365 (Emails, Calendars, Contacts, One Drive and team Site) are backed up from the Office 365 cloud to a separate cloud (held within Australia).
        - Backup provider is Datto, product is Backupify SaaS Protection
        - The backup is automated, runs three times per day, keeps backup snapshots for 1 year
        - Access to the recovery operations are restricted to the Backup Admin – currently IT Support
        - All data transportation is encrypted
    - Remote Access
        - Remote access to Office 365 is via unique user ID and password
    - Anti-Virus
        - Windows machines: Windows Defender
        - MAC: XProtect
    - Remote Access for IT Support
        - Aero Admin is used with access via unique machine ID and password
        - All data transmissions between the remote computer and host computer are encrypted
    - Patch Management
        - Windows machines – via Windows 10 automatic patch management
        - MAC – user notified and manually controlled updates.
    - Computer Backups
        - Computers are not backed up – all sensitive data is to be kept either within cloud applications or Office 365
        - Staff are not permitted to download sensitive data to a computer; staff must use Splose and One Drive

Backupify/Datto SaaS Protection

At every step along our data-replication process, Backupify/Datto SaaS Protection uses 256-bit encryption. In particular:

- All authenticated user interaction with the Backupify/Datto SaaS Protection application
- Logging in
- Configuring services
- Altering settings
- Accessing archived data

Backupify/Datto SaaS Protection encrypts your duplicate archives. For every new account created (each email address), our system automatically generates a unique AES 256-bit encryption key for that user. All data written for the user is encrypted with that key prior to storage. Data remains encrypted both in-transit and at-rest.

Private keys

Upon retrieval (e.g. when a user views/downloads Archives through the Backupify/Datto SaaS Protection Web interface), the key is used to decrypt the stored data. All users' AES keys are stored on the Backupify/Datto SaaS Protection production system and the central list of keys is encrypted with Backupify/Datto SaaS Protection's master RSA-2048 private key.

Internal controls

Backupify/Datto SaaS Protection grants access to stored data internally using the "principle of least privilege" through appropriate roles and only on a "need to know" basis and manages its systems in line with security industry best practices,

including the ISO 27000 series and NIST Security Publications.

Legislation

The Privacy Act 1988 (Privacy Act)

The National Disability Insurance Scheme Act 2013 (NDIS Act)