Information Privacy Policy

Issued: 8/02/2020 Stage: Issued

Objective:

This policy applies to the internal records, client records and unpublished materials of ***focus***.

To provide clear directives about how information that is collected by ***focus*** may be used, and the legal and ethical obligations of staff to protect the private and confidential information of the people we support.

All staff must be aware of their obligations in relation to the privacy of individuals who they come into contact with in the course of their employment.

An Easy Read Version of this document, titled 'Your Information' is also available on request.

Scope:

All ***focus*** employees, clients, and relevant stakeholders.

Policy Statement:

focus recognises that privacy is a human right, protected by Commonwealth, State and Territory privacy laws.

focus complies with the:

- Victorian Information Privacy Act 2000
- Privacy Amendment (Notifiable Data Breaches) Act 2017
- Australian Privacy Principles of March 2014
- Health Records Act 2001; and
- with the privacy principles referred to in those acts.

This policy and procedure aligns our practices to the NDIS Quality and Safeguards framework within the:

- NDIS Practice Standards : Provider Governance and Operational Management - Information Management
- '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 participants and appropriately utilised by relevant workers'.
- NDIS Code of Conduct: Obligations outlined within the element relating to 'Respect the privacy of people with a disability'.

focus is subject to the personal information security obligations under the Privacy Act 1988, and is therefore required to comply with the Privacy Amendment (Notifiable Data Breaches) Act 2017.
focus is committed to protecting the privacy and personal information that it holds about individuals.
focus will act appropriately and in a timely manner in the event of a data breach, to contain the possible resulting harm and notify individuals affected as required.
focus is committed to transparency in its operations and to ensuring it is open to public scrutiny. It must also balance this with upholding the rights of individuals to privacy and of the organisation to confidentiality on sensitive corporate matters.

focus will only collect and store information regarding our employees and service users that is necessary to ensure a safe and effective workplace and/or home environment. The information will be kept secure, will not be accessed by unauthorised personnel and will not be divulged to any third party without the permission of the person concerned.

Information Privacy Policy

focus places an emphasis on high quality ethical relationships with clients and all personnel of ***focus***. The personnel working for the organisation must not create or permit conditions or circumstances in which people's dignity or privacy is denied or treated lightly.

focus will ensure that:

- all individuals enjoy freedom from intrusion and public attention (unless such attention is with prior consent)
- all individuals are treated with honour, respect and worthiness thereby reflecting their culture, community and providing a positive influence for their self-esteem
- written and spoken information is protected from access and use by unauthorised persons.
- use and disclosure of information is only as necessary, in accordance with the relevant legislation (Information Privacy Act 2000, Health Records Act 2001, Disability Act 2006, the Australian Privacy Principles of March 2014)
- reasonable steps are taken to ensure that the information we collect is accurate, complete, up to date and relevant to the services we provide
- personal and health information is securely stored at all times
- we support clients or staff to access their own information held by ***focus*** any time they wish
- we will provide ongoing education to the people we support about their rights and when seeking their consent, use the method of communication they are most likely to understand

focus will only keep information that is essential to the delivery of a quality service and will not sell, rent or disclose information or photographs without the consent of the individual.

focus recognises the increased vulnerability of the people we support to have their personal information, history and details of their daily lives shared inappropriately.

focus staff must understand and respect the right of the people we support to privacy, confidentiality and the right to give informed consent for the sharing of that information.

focus therefore requires staff to understand and be vigilant in protecting and respecting the rights of people with disability to privacy, consideration and confidentiality.

All people of ***focus*** have a responsibility to ensure that information gained (in written, verbal or observed manner) at ***focus*** remains at ***focus*** and is treated with respect, confidentiality and sensitivity and this procedure is adhered to in order to gain or release information on any client, staff member or volunteer.

Personal and sensitive information is collected in a number of ways, including from business cards, direct email, online data entry, verbally, by fax and by mail
Breaches of this policy will result in disciplinary action for staff - including potential dismissal.

Process Steps:

1 Definitions

Health Information is defined in the *Health Records Act 2001* as information or opinion about:

- the physical, mental or psychological health of an individual; or
- the disability of an individual; or
- an individual's expressed wishes about future provision of health services to him/her; or
- a health service provided or to be provided to an individual that is also personal information; or
- other information collected to provide a health service; or
- other information about an individual collected in connection with donation or intention to donate by the individual his or her body parts, organs or body substances.

Information Privacy Policy

Health Services as defined in the Health Records Act 2001 includes Disability Services.

Personal Information is described by the *Information Privacy Act 2000* as the personal information as recorded in any form about a person whose identity is apparent or can reasonably ascertained from the information, but excludes health information.

Personal Information is defined by details such as:

- addresses
- phone numbers
- details of relatives
- financial information
- information about a person's disability
- medical treatment
- photographs
- wishes a person (or their guardian/authorised representative) may express about the service they would like to receive in the future

Information Privacy refers to the control of the collection, use, disclosure and disposal of information and the individuals right to control how their personal information is handled.

Data Breach A data breach is unauthorised access to, unauthorised disclosure of, or loss of, personal information held by an entity. This breach may be in relation to one record or many records, and may be electronic records or a physical document.

2 When Does Confidentiality and Privacy Exist?

Confidentiality exists when ***focus*** is in possession of personally identifiable information about the health and other personal information regarding an individual.

All confidential personal and health information is to be kept under lock and key or password protected. If removed for any authorised reason, such information will be kept secure until such time it can be returned to its correct storage, and access to such information shall only be through the Chief Executive Officer or other authorised persons.

A breach of confidentially may occur if:

- Written or verbal information is released without the proper consent
- Discussing a client, member, employee, volunteer, student or contractor in front of any other person.

3 What Information does *focus* collect?

- health information
- personal information
- daily notes
- assessments (past and current)
- staff resumes, interview notes, referee comments, performance appraisals, attendance/absenteeism
- incident reports, accident reports (Workcover)
- photographs/videos of people we support in their daily lives, at special events and their achievements
- GPS location data

Information Privacy Policy

4 Client Records

Client records will be confidential to clients and to authorised staff

Information about clients may only be made available to other parties with the consent of the client.
Legal obligations may provide an exemption from a requirement to obtained informed consent from an individual. This may include mandatory reporting matters, and obligations to report incidences of violence, exploitation, neglect and abuse, and sexual misconduct to the NDIS Quality and Safeguards Commission and police.

No information relating to an individual shall be passed onto any other person or organisation without the permission of the individual or their representative, except when required by law, medical emergencies, or in the case of clients, to other persons or organisations as required by the Public Advocate, the Secretary of Human Services, Victorian Office of Senior Practitioner, the NDIS Quality and Safeguards Commissioner, the Minister and the Commonwealth Minister responsible for Medicare; or to a person to whom in the opinion of the Minister it is in the public interest that the disclosure be made.

All client records will be kept securely within our client information management system and updated, archived and destroyed according to the ***focus*** Archiving of Records policy.

5 Personnel Files

A personnel file is held for each staff member and contains:

- contact details and contact details in case of an emergency
- a copy of the employee's contract
- all correspondence relating to job description changes, salary changes, leave entitlements such as long service leave, continuous service leave, unpaid and parental leave

Access to personnel information is limited only to:

- the individual staff member accessing their own file
- the relevant managers responsible for the engagement of that staff member

Refer to the Personnel Files Procedure for more information

6 Why do we Collect This Information?

- to ensure the health, safety and best quality service delivery to our clients
- to ensure a safe and supportive work environment for our staff (recruitment, training and staff management)
- to comply with funding and reporting requirements of the NDIS Quality and Safeguards Commission and the Victorian Senior Practitioner
- to assist in research or statistics relevant to public health or disability service professional advancement
- to assist ***focus*** in management planning, monitoring, evaluation or improvements
- to celebrate the achievements, activities, and development of our clients and to document these for their future reference (memory)
- marketing/promotion of our agency, annual reports

7 Data Breach

Data breach definition - When personal information held by an organisation is disclosed accidentally, lost, or accessed without permission. This can be as a result of human error, or through malicious action by an employee or an external party. Personal Information is information about an identified individual, or an individual who is reasonably identifiable: whether the information or opinion is true or not; and whether the

information or opinion is recorded in a material form or not. Personal information includes a person's health information, tax file number, and information about racial or ethnic origin, sexual orientation or criminal record.

Examples of data breach include where a secure IT system containing personal information has been hacked, a storage device being lost by an employee, or an employee accidentally releasing personal information to the wrong person.
An eligible notifiable data breach occurs where:

- A reasonable person would conclude that the unauthorised access to or disclosure of the personal information would be likely to result in serious harm to any individuals to whom the information relates; or
- a secure IT system containing personal information has been hacked
- Information is lost (such as leaving a laptop or documents in a public space), unauthorised access to or disclosure of the personal information is likely to occur, and a reasonable person would conclude that this would be likely to result in serious harm to any of the individuals to whom the information relates.

The Chief Executive Officer is responsible for overseeing the assessment, investigation, notification and review of data breaches.

8 Data Breach Response

Identify
When staff have reason to believe there has been a data breach, they should inform their relevant Customer Relationship Leader/Activities Facilitator immediately. They will then work with the relevant Area Manager to complete a preliminary assessment of the breach and take any immediate action to contain the breach if possible.
At this time, details such as when and how the breach was discovered, and by whom, should be recorded. This will be recorded within the Riskman Client Incident reporting system.

Contain
As soon as a breach or suspected breach has been identified, any steps to contain or limit the potential harm should be taken. This may include shutting down a system that has been breached, or recovering any records.

Assess
If the preliminary assessment finds that further investigation and assessment is necessary to understand the nature and extent of the breach, it will be escalated to Executive Management who will implement actions to gather information, assess risks and the likelihood of serious harm from the breach, and therefore whether it is a **notifiable** breach.
If there are reasonable grounds to suspect that there has been a data breach, the Chief Operating Officer and/or CEO will conduct an assessment of the suspected breach. The assessment of a suspected breach must take place within 30 days of it occurring, and should seek to find out the likelihood of serious harm occurring as a result of the suspected breach. If it is assessed to be likely, this has the same notification obligations as a known data breach under the Notifiable Data Breach (NDB) Scheme.

To evaluate whether a known data breach is **notifiable**, the following will be assessed:

1. Has there been unauthorised access, unauthorised disclosure, accidental loss, or theft of personal information that the organisation holds?
For example, the organisation's database is hacked, a portable storage device containing personal information is lost, or the organisation accidentally releases personal information to the wrong person.

2. Is it likely that this may result in serious harm to individual/s whose data has been breached?
This can include but is not limited to psychological, financial, emotional, physical or reputational harm. To be able to accurately assess the likelihood and seriousness of harm, it requires looking at the context of the data and how it may have been breached.
For information about the factors to consider when deciding whether harm is likely and/or serious, refer to section 26WG of the Privacy Amendment (Notifiable Data Breaches) Act 2017

3. Does the likelihood of serious harm remain despite taking available remedial action?
The obligation to notify The Office of the Australian Information Commissioner (OAIC) can be avoided if the organisation takes remedial action in a timely manner to prevent the risk of harm occurring, either by making the harm unlikely to occur, or non-serious.

If the answer to the above three questions is yes, then the breach classifies as an eligible notifiable data breach and organisations are required to notify the OAIC and any affected individuals.
If there are reasonable grounds to suspect that there has been a data breach, the data response team should conduct an assessment of the suspected breach. The assessment of a suspected breach must take place within 30 days of it occurring, and should seek to find out the likelihood of serious harm occurring as a result of the suspected breach. If it is assessed to be likely, this has the same notification obligations as a known data breach under the NDB Scheme.

Take remedial action
Remedial action can be taken at any point throughout the data breach response process the sooner the better. However, it may be that the full extent and nature of the breach, and therefore the actions that could be taken, are not known until after assessing and investigating the breach.
Examples of remedial action include remotely deleting sensitive information from a laptop which has been lost, or emailing affected individuals with advice to change their password details for an online account for which login information may have been hacked.
The data breach response should document the process of any remedial action, making sure to document rationale and reasoning as to why a certain conclusion has been made.
If, after the remedial action has been taken, the risk of harm is reduced so that it is unlikely to occur, or non-serious, then there is no requirement to notify.
Even if there is no requirement, however, the data response team should consider whether to contact affected individuals with advice for further protecting their information as a customer service measure.

9 Data Breach Notification

Notify
Once a breach has been assessed as notifiable, ***focus*** must, as soon as practicable:

- prepare a statement that includes details of the breach and recommendations of the steps individuals should take; and
- give a copy of the statement to the Office of the Australian Information Commissioner (OAIC).

The Chief Operating Officer is responsible for notifying and liaising with the OAIC for data breaches which have been assessed as eligible for the purposes of the Notifiable Data Breaches Scheme, using the OAIC's Notifiable Data Breach form.
If the OAIC has reasonable grounds to believe that there has been an eligible breach, they can direct ***focus*** to provide notice of the breach.
Relevant individuals and bodies should be notified as soon as practicable. Notification must include the following information as a minimum:

- The organisation's name and contact details
- Description of the data breach
- Type of information involved in the breach
- Advice and recommendations for individuals to take in response

The way notification occurs will depend on the context and nature of the breach, and the relationship of the individuals affected to the organisation. It should occur as soon as practicable after completing the notification statement for the OAIC.

10 GPS Location Services

As technology changes and improves, ***focus*** may require the use of software or apps which contain GPS location services.

Installation and usage of any apps with this feature on your personal device, or a ***focus*** device, is considered express consent for this information to be collected.

The use of this feature has the potential to:

- identify your geographical location
- monitor adherence to roster to manage the risks associated with non-compliance to the ***focus*** Code of Conduct and Workplace Health & Safety (WHS) requirements.

Information collected from this data will not be used for the following purposes:

- as the sole and primary means of disciplinary action
- to target or victimise employees
- as a form of real time employee performance monitoring

This means that surveillance information can be used for disciplinary purposes only to substantiate allegations stemming from other sources.
Only the Executive Management Team has access to any GPS location information.

11 Client Information Management - Authorisation for SupportAbility

focus uses SupportAbility for the collection, storage and retrieval of our client information.

All clients have provided permission for their information to be stored on SupportAbility within intake and service agreement processes.

SupportAbility is a client information management system, which manages all aspects of client data to meet the needs of clients and requirements of ***focus***. It is a goal driven, evidence based tool that supports documentation, recording, collation and management of all client data to ease access and reporting in all areas of the organisation.

All support staff and managers in contact with the people that ***focus*** supports must have access to SupportAbility in order to access relevant information, establish client goals, enter file notes, manage funding, enter medical notes, create journals and assessments and to access reports to illustrate progress.

SupportAbility is an internet based application that can be accessed and updated in real time from any location using a laptop or tablet device with internet connectivity.

Information housed in SupportAbility is considered of the highest sensitivity and of paramount confidentiality. Staff with access to SupportAbility are to be aware that they are to only access information that is specific to the client/s they are working with.

Information Privacy Policy

12 Use and Disclosure

focus will only use or disclose information for the primary purpose for which it was collected or a directly related secondary purpose.

We will only disclose information when we are under a legal obligation to do so, including where there is a lawful duty of care.

13 Security, Retention and Disposal

focus staff will:

- Safeguard the information that is collected and store it against misuse, loss, unauthorised access and modification
- Only destroy information in accordance with the Information Privacy Act 2000, the Health Records Act 2001 and the Disability Act 2006 and the Australian Privacy Principles of March 2014
- Ensure filing cabinets are locked when not in use
- Shred sensitive information prior to recycling or destruction.

14 When is Private Information Shared?

- when consent has been given to ***focus*** sharing certain information with certain individuals or another organisation (ie. another service provider)
- when ***focus*** is under a legal obligation to do so, such as a court or tribunal
- where the release of information is required to meet a duty or perform a function under the NDIS Quality and Safeguards Commission and/or Victorian Senior Practitioner. For example: mandatory reporting requirements.
- where it is necessary for the treatment or care of a person and the person is unable to consent, and may otherwise suffer detriment
- to the Public Advocate

15 Gaining Consent to Share Information.

Support plans and service agreements - consent of the participant or of a delegated support person is obtained within the annual support review in regards to collecting private information. This consent (and any restrictions and/or additional preferences) is recorded within the person's information on Supportability for referral.
In some cases, the people ***focus*** support may not demonstrate capacity to give consent and/or they are legally unable to make a decision such as this. In such instances, a guardian would have been appointed or the

individual may have selected an authorised representative (usually a family member) to make these decisions. This information will be in the individuals' personal information and recorded on the SupportAbility system. When gaining the person's consent, the individual must be given the following information to be considered "informed consent".

- why the information is being collected
- that the information will be protected by ***focus***
- how ***focus*** will use the information
- who else ***focus*** may need to share this information with
- ***focus*** will always try to get their consent prior to releasing information
- how they can access their own information if they wish
- what consequences may eventuate if they don't give us consent to collect/share this information
- If a person is unable to do this consent must be obtained in writing from a family member or guardian.

16 Ability to Give Consent.

In order for ***focus*** to accept an individual's consent, we need to believe that it is "informed consent", which means that we believe the individual has understood our communication to them.

This highlights the need for Customer Relationship Leaders and Activities Facilitators to use the form of communication that the individual is most likely to understand - signing, gestures, physical prompts, visual/pictorial aids in order to gain the understanding of the individual. This also requires Customer Relationship Leaders and Activities Facilitators to include some training on Rights, Privacy, and Confidentiality in the People's meetings that each location has with their clients on an ongoing basis. Easy Read versions of all of these policies have been developed and are available at all services for referral. The Information Privacy policy is also presented within the Service Agreement process to enhance capacity, ensuring they are given information regarding their information rights in a format that reflects their communication abilities.

17 Inability to Give Consent.

In some cases, the people we support may not be able to give consent.

If a person is believed to have died, gone missing or been involved in a serious accident, and information is needed to identify/locate the person or a relative, the following steps should be taken:

- check that the disclosure of information would not go against the individuals' wishes
- disclose only information that would help identify the person or locate a relative who would need to identify the person
- follow procedures for "Incident Reporting" and "Missing Person" or "Death of a Person"
- in the above-mentioned circumstances, the Chief Executive Officer (CEO) would be involved and would authorise this release of information

18 Use of Photographic and Video Material.

focus will:

- Only use photographs of clients for promotional purposes with the documented permission of the person and/or their guardian or representative.
- Only take videos of a person with the prior consent of the managers, and only then for specific purposes.
- Ensure consent to use photographic material is acknowledged within the person's service agreement and recorded in their client information.

No photographic or video material is to be kept on private cameras or mobile phones. When a mobile phone or privately owned camera is used the image is to be down loaded immediately onto the ***focus*** system and the original deleted.

Any staff member who retains photographic images will be disciplined.

Where ever possible a ***focus*** device should be used to take photographic images.

19 What if someone feels their privacy has been breached?

If at any time, a client or staff member has concerns about the way that their personal or health information has been managed, please feel free to contact the Chief Operating Officer or the Chief Executive Officer directly.

If after this discussion, they are not satisfied with the way the inquiry/complaint is handled, please follow the ***focus*** Complaints procedure (lodge an official document to be investigated).

If this still does not satisfy expectations, the person can contact the NDIS Quality and Safeguards Commission on 1800 035 544 or the Privacy Commissioner on (03) 8619 8719.

If this form of conciliation fails, the complainant may take the complaint to the Victorian Civil and Administrative Tribunal (VCAT).