Confidentiality and Privacy Policy

Aim:
To ensure the privacy (both visual and auditory) of Residents, Staff and Visitors is maintained in accordance with the requirements of the Privacy Act 2020 and the Health Information Privacy Code 2020. Nazareth House Privacy Officer (the Facility Manager) will ensure the rights of Residents, their family/whanau and staff are maintained in relation to privacy issues.

Procedure:

The Privacy Officer is the Facility Manager:

The Privacy Officer will have participated in education relating to the requirements of the Health Information Privacy Code and/or Privacy Act. This may be sourced through the Privacy Commission. (*See reference website at the end of this document).*

Responsibilities:

1. To ensure storage arrangements for all information (paper based and electronically held) complies with the Health Information Privacy Code.

2. To ensure that the documented process for collection, storage, disclosure and disposal of information is complied with.

3. To review the documented processes for collection, storage, disclosure and disposal of information annually to ensure they comply with the Health Information Privacy Code 2020.

4. To monitor the use of assessment and information gathering documents to ensure they facilitate a streamlined process in the collection of information.

5. To facilitate the training of all staff in the management of health information in accordance with the Health Information Privacy Code 2020.

6. To respond appropriately to requests for health information from other health organisations.

7. To respond to Resident's or their identified representative's requests for access to a Resident's individual health information.

8. To ensure that the Resident's written permission (or representative where appropriate) is gained for disclosure or collection of information as appropriate.

9. To authorise another staff member to assume the role of Privacy Officer in their absence. This will normally be the Registered Nurse.

General Principles of implementing Privacy Legislation:

1. All information relating to Residents, resident family/whanau, staff and operational matters must be treated with the strictest of confidence.

2. All new staff will sign a Privacy and Confidentiality declaration at the commencement of employment.

3. In the event of a request for information pertaining to a Resident or staff member, the individual making the request must **NOT** be given direct information over the phone. They should be informed that if they will give their telephone number, the appropriate person will return their call.

4. Information relating to staff and Residents or their visitors, will not be discussed with other Residents or their visitors unless permission (provided in writing) has been granted to share that information.

5. The Registered Nurse, Unit Manager or Facility Manager have the authority to discuss any information requested in accordance with the requirements of the above noted legislation.

6. The Resident's medical files remain the property of Nazareth House and the visiting Doctor or Nurse Practitioner and must not be removed from the premises at any time. When Residents are required to visit their Doctor or Nurse Practitioner at a medical practice, the Resident's files may be taken with the Resident for the purposes of updating and must be returned to Nazareth House immediately after the completion of the appointment.

7. As part of compulsory audit requirements, Auditors and Audit monitoring agency personnel may have access to Resident files as part of determining compliance to legislative requirements. This information is solely viewed for the purpose of Audit and will not be shared with third parties without the permission or the Resident or their representative.

8. Staff will be afforded the same rights to privacy and confidentiality in relation to issues pertaining to them.

9. Storage of old records and deceased Residents will be in accordance with statutory requirements (10 years from date of last entry). These records can be held in a different form from the original records, if preferred. This means documents may be scanned, converted into digital files, and stored, while the hard copy originals are securely disposed of.

10. As long as information from original source documents gets stored securely in digital systems (e.g. cloud based and backed up), the paper version of these documents can be disposed of securely.

11. Residents or their legal agents may formally request in writing to view copies of a Resident's medical file. Release of these is in accordance with the provision of the Privacy Act 2020 and the Health Information Privacy Code 2020.

12. The Facility Manager is responsible for authorising such requests and must be present while the file is viewed.

13. Ensure appropriate authorisation as per Section 45 of the Privacy Act for uplifting or being supplied information to a person other than the Resident.

14. Individuals will be informed of the basis for withholding any information and their right to have your decision reviewed by the Privacy Commissioner. You do not have to provide the individual with the information at the same time as you make a decision (although this will generally be the case). There will be no undue delay in providing authorised information. Generally, unless the request for information has been transferred to another agency eg; GP, the individual seeking information will be notified of the decision to supply or not, within 20 working days of receiving the request.

Resident Physical Privacy:

Procedure:

1. Residents will be assisted to make private telephone calls with the hand-held phone. Avoidable background noise will be minimised so as not to interfere with communication.

2. Residents will be provided with a private area appropriate for conducting private conversations with visitors and during the making of telephone calls.

3. Staff will ensure they provide cares in a manner that promotes discretion, dignity and privacy, and provide care away from the view of others.

4. Residents who may have altered inhibitions must be supported to maintain their dignity and not encroach on the rights of others relating to sexual boundaries and privacy. (*see Policy on Intimacy and Sexuality in Older Persons for further information).*

Physical Security of Information:

- Implement a clear desk policy where there is the potential for paperwork to be observed (including outside standard office times) by unauthorised persons. Lock information away.

- Prevent unauthorised access – secure electronic system, through use of passwords.

- Non-disclosure of passwords or key-pad codes to unauthorised personnel.

- Turn computer screens and whiteboards away from public areas. Where this is not possible, ensure doors are closed or screens on windows, to prevent viewing of whiteboard information.

- Place computers and printers where they cannot be accessed by unauthorised personnel.

- Ensure ‘staff only’ signs are displayed on doors which have restricted access, as a means to ensure safety or privacy.

- Ensure staff personnel files are locked away and only accessed by those with appropriate management approved authorisation.

Electronic Records Privacy:

- As the use of electronic records increases through implementation of 'telehealth', which includes access to electronic records off-site eg; by Doctors / Nurse Practitioner, on-call Registered Nurse; staff are reminded that they should not be accessing electronic records outside of work hours unless necessary to ensure the care needs of residents are met. Staff are reminded through their 'Employee Handbook / Code of Conduct - House Rules' of their responsibility in relation to privacy of information.

- Ensure appropriate firewalls are in-place.

- Install and update antivirus software.

- Update passwords regularly. Notify software providers eg; HCSL, 1Chart, when personnel leave to ensure access codes previously authorised are deactivated.

- Restrict staff access to information - only allow access to information that staff need to do their particular role. *See 'User Permission' in 'Clinical Documentation and Report Writing Policy'.*

- Storage of and access to computer backups and company owned mobile devices.

- Digital photos are not to be taken on personal cameras / phones or other electronic devices owned by a staff member or visitor. Where a personal phone has to be used due to no other available option; any photographs or information uploaded must be transmitted onto a facility device at the earliest possible time and then the images and information deleted from the personal staff members phone / device. All photos are to be loaded onto Nazareth House approved devices only. A register of approved devices is held by the Privacy Officer.

Transmission of Information:

Transmission of information includes the following measures:

- Clinical information will not be transmitted to private email or other privately owned mobile devices

- When using a facsimile to transmit information, make a telephone call prior to transmission to ensure that the information is uplifted immediately by the intended person who is authorised to receive the information being sent.

- Where reference must be made in electronic transmission of clinical information to another healthcare provider, do not include the name of the Resident; instead use NHI and Resident initials only.

Disposal of Information:

When information is no longer needed (after 10 years from the date of the last entry), it must be disposed of in an appropriate manner. Disposal of information could involve things like:

- using a shredder (only non-clinical information) with permission of the Facility Manager.

- if using an outside Contractor, making the secure destruction of documents a condition of the contract E.g.; secure document destruction service.

Information Access Breaches may include:

- lost records and equipment - lost or stolen laptops, USBs (memory sticks) or paper records
- incorrect e-waste disposal - incorrect computer hardware disposal and return caused by computer hard disk drives or portable storage devices such as USBs, being thrown away, recycled or returned to leasing companies, or serviced incorrectly, without the contents first being erased
- employee browsing - accessing or disclosing personal information without authorisation
- document theft - taken from recycling or rubbish bins
- information given to the wrong person - information sent to the wrong physical or email address
- information transmitted in emails for purposes other than that which the email address was supplied
- fraudsters - releasing personal information to a person pretending to be someone else

Breach notifications:

To determine risk and need for privacy breach notifications, click on the following link: https://privacy.org.nz/responsibilities/privacy-breaches/notify-us/evaluate

If a breach of privacy has been identified, the Office of the Privacy Commissioner and affected individuals will be notified as soon as possible. It is an offence under the Privacy Act 2020 to fail to notify of such a breach which may pose 'serious harm'. To submit a notification click on the following link: https://www.privacy.org.nz/responsibilities/privacy-breaches/notify-us/

Governance Sharing of Clinical Information:

It is acknowledged that the Residents' appointed / elected Medical Practitioner is the medical professional responsible for determining the day to day care of the Resident.

It is further acknowledged that the 'Provider' under section 22F (4) of the Health Act 1956 may from time to time have access to information pertaining to a Resident's health status.

Such information sharing will only occur:

1. At the instigation of the Facility Manager;
2. Where it is in the best interest of the Resident and relates to the provision of care services to that Resident;
3. The disclosure of the information may occur when it is required for a risk management assessment;
4. The purpose and limitation of the disclosure is expressed by the Facility Manager at the time of making the disclosure.

Informed Consent (authorisation) will be obtained from the individual Resident or their advocate / EPA / Whanau prior to the disclosing of such information. The disclosure of that information will be such as is necessary for the management of the provision of appropriate care services.

Where consent is not able to be obtained related to competence; no Resident identifiers will be disclosed and the information will be shared to the limit necessary to ensure no deterioration in the health of the individual Resident and for the purposes of clinical risk management.

Resident clinical information will not be shared with Governance where the Resident has expressly declined or vetoed the sharing of their information with Governance.

Key Principles of the Privacy Act:

The 12 principles have, in very general terms, the following effect:

Principle	Summary
Principle 1 - purpose for collection	Only collect information when you need it for a lawful purpose connected with your agency.
Principle 2 - source of information	Obtain the information directly from the person concerned if possible.
Principle 3 - what to tell an individual	Tell the person what you are doing.
Principle 4 - manner of collection	Do not use unfair or unreasonably intrusive means of collecting the information.
Principle 5 - storage and security	Take care of the information once you have obtained it.
Principle 6 - access	The person can ask to see the information.
Principle 7 - correction	The person can ask you to correct the information.
Principle 8 - accuracy	Make sure that the information is accurate before you use (process) it.
Principle 9 - retention	Dispose of the information once you have finished with it.
Principle 10 - use	Only use the information for the purpose for which it was obtained.
Principle 11 - disclosure	Only disclose the information if this was the reason for which you obtained it.
Principle 12 - unique identifiers	Only use unique identifiers in place of person's name where necessary.

Table 1 - A general summary of the Privacy Act principles

<u>Refusal to Supply Requested Information:</u>

There must be no disclosure of personal information, unless it is believed on reasonable grounds that:

- disclosure is one of the purposes, or a directly-related purpose, for which the information was obtained. (This exception is the most important, and links to principle 3 requiring the individual to be told of any anticipated disclosures.) (section 11(a),
- disclosure is to the individual or authorised by the individual (section 11(c) and (d)
- the individual is not identified (section 11(h) and (i)
- disclosure is necessary to avoid prejudice to the maintenance of the law or the conduct of proceedings before a Court or Tribunal (section 11(e),(i) and (iv)

- disclosure is necessary to prevent or lessen a serious threat to public health or safety or the life or health of the individual concerned (section 11(f).

See: http://www.legislation.govt.nz/bill/government/2018/0034/latest/LMS23392.html

References and Related Documents:

https://elearning.privacy.org.nz/login/index.php - Access to online education on Privacy Act.

Nursing Council competencies – Competency 2.3
http://www.nursingcouncil.org.nz/Nurses/Scopes-of-practice/Registered-nurse

Privacy (Information Sharing) Amendment Bill 2012; Health Information Privacy Code 2020 (Rule 11 in particular); Privacy Act 2020; Health Act 1956.

The Council has set out principles and standards to guide professional behaviour in the Code of Conduct for nurses (2012). These principles and standards can be applied to social and electronic media.

HCSL System User Permission Restrictions:

Create and deactivate Users is completed on site by the Facility Manager or Unit Manager.

Access Code Formula:

When setting up User and Password Codes they should be:

Password structure must include no less than 8 characters which include a capital letter, lower case letters, at least one number and a character such as @ or # or & or ! within the password. Passwords must be stored securely.
When staff cease their employment, the employer is to ensure passwords are deactivated.

Passwords must only be accessible to those staff authorised to access the computer files and only those files that were intended for viewing / updating by that person. This is the responsibility of management to maintain these processes.

For HCSL aged care software system support contact gill@agedcarecompliance.com or support@agedcarecompliance.com or http://agedcarecompliance.com/contact/

See OR 6A HCSL User Permissions document

See: Nursing Council (NZ) Social Media Guidelines 2012. http://nursingcouncil.org.nz/News/New-guidelines-for-nurses-on-social-media

http://privacy.org.nz/assets/Files/Codes-of-Practice-materials/HIPC-1994-incl.-amendments-revised-commentary.pdf

https://www.privacy.org.nz/ The Privacy Commission

https://www.telehealth.org.nz/tech/security/ - regarding external access to electronic systems

Related Documents: OR 6A HCSL User Permissions; CS 14A Clinical Documentation and Report Writing Policy; OR 12 Informed Consent Policy; OR 12A Informed Consent Form; SAE 21 Security Policy; (SAE21A Surveillance Camera information); SD 3 Communication Policy; E 4 Admission Agreement.

HDSCS: 1.1.1, 1.1.2, 1.1.3

https://privacy.org.nz/privacy-act-2020/campaign/ (including access to e-learning modules) - https://elearning.privacy.org.nz/

