NURSING & HOMEMAKERS INC.
2347 Kennedy Road, Suite 204, Toronto, ON M1T 3T8 • Tel: 416•754•0700 • Fax: 416•754•4014

Privacy, Accuracy and Security of Client/Employee Records and Personal/Health Information

Policy and Procedures

Policy No.	HC 11.3
Approval Committee	Home Care
Approval Date	May 2025
Next Review Date	May 2027

Accountable To: President & CEO

Key Policy Issues:

- Adherence to privacy legislation(s)/principles.
- Accuracy of personal/health information.
- Consent for collection, use, and disclosure of personal/health information.
- Individual access to personal/health information.
- Securely storing, retaining and disposing/destroying client records and personal/health information.

TABLE OF CONTENTS

Created: Sept2016 • RD: May2025 • NRD: May2027

1. POLICY STATEMENT

NHI Nursing & Homemakers Inc., is in compliance with relevant legislations/laws such as the Personal Information Protection and Electronic Document Act ("PIPEDA") and Personal Health Information Protection Act ("PHIPA") regarding collecting, using, disclosing, securely storing, retaining and disposing/destroying client/employee records and personal/health information.

NHI is also a strong supporter of improved privacy standards for the health care industry and of effective government regulation in the area of privacy of personal/health information.

2. PERSONAL INFORMATION PROTECTION AND ELECTRONIC DOCUMENT ACT ("PIPEDA")

Personal Information Protection and Electronic Document Act ("PIPEDA") recognizes two fundamental facts. The first: individuals have a right to privacy concerning their personal information. The second: organizations have a need to collect, use, and disclose personal information for appropriate purposes. The aim of PIPEDA is to achieve a fair balance between these two valid requirements.

Below are 10 principles:

2.1. Accountability

NHI is responsible for protecting its employees' and clients' health and personal information under its control, which includes information that NHI discloses to affiliates, agents and contractors for contract management, administration and other reasonable business purposes.

NHI has appointed a Privacy Officer to oversee compliance with its privacy policies. NHI's management staff is responsible for managing the day-to-day collection and processing of personal and health information required by NHI to conduct its business. NHI uses appropriate contractual agreements or similar means to provide a comparable level of protection with third parties who process NHI's employees' and clients' health and personal information.

NHI has implemented procedures and practices to affect this Principle, including:

- Procedures governing the accuracy, collection, use, disclosure, storage/protection, retention and disposal/destruction of personal/health information.
- Procedures for receiving and responding to inquiries and complaints.
- Education, Training and Communication to staff about NHI's privacy policies and procedures.
- Please refer to the *Accuracy of Personal/Health Information* section for more information/details.

2.2. **Identifying Purpose (Use of Health & Personal Information)**

NHI will identify to clients and employees the reasons for the collection, use and disclosure of their health and personal information. This will be done orally, electronically, in writing or other means at or before the time the information is collected. NHI will identify to clients and employees any new purposes for using or disclosing their health and personal information before such use or collection.

2.3. **Consent**

In most cases, NHI will obtain consent from clients and employees prior to collecting using or disclosing their health and personal information. The form of consent, including whether it's express or implied, oral or written, varies depending on the circumstances and the type of information, including its sensitivity and employees' and clients' reasonable expectations.

The following qualifies as consent:

- Receipt of NHI privacy policies - unless NHI is expressly advised by the employee or client that they do not agree with the terms of NHI's privacy policies, and therefore wishes to opt out of all portions of them.
- Employees' or clients' express written or oral consent obtained through an application process.
- Electronic enrolment forms, survey forms, faxes, electronic mail and telephone conversations with NHI employees or agents.

In exceptional circumstances, where it is permitted or required by law, NHI may collect, use or disclose employee or client personal or health information without consent. NHI reserves the right to disclose such information without consent in the following circumstances:

- A third party that provides administrative services to NHI (these third parties are bound by a contractual commitment to respect NHI's client and employee confidentiality).
- To protect public interest (for example, fraud or money laundering).
- To the courts in the interest of protecting NHI's business.
- To Government agencies, such as the Canada Customs and Revenue Agency, Information and Privacy Commissioners, or Human Rights Commissions, which have the authority to review NHI's files and interview NHI's staff.
- Where NHI is required or authorized to do so by law, for example if a court issues a subpoena.
- For income tax reporting purposes.

NHI's clients and employees may withdraw their consent for any other identified purposes at any time subject to legal and/or contractual restrictions with reasonable notice. However, withdrawing consent may affect NHI's ability to work with the client or

Created: Sept2016 • RD: May2025 • NRD: May2027

employee. NHI's Privacy Officer should be contacted to discuss the implications of withdrawing consent.

Unless NHI hears otherwise from clients and employees, consent has been granted at the time this and other privacy policies have been distributed to them.

See section *Consent for Collection, Use and Disclosure of Personal/Health Information* for more information/details.

2.4. **Limiting Collection (Collecting Information)**

NHI collects information by means that are required by law. NHI limits the collection of health and personal information from clients and employees, which is necessary to fulfill the identified purposes.

Health and personal information are collected:

- Primarily from the client or employee, through applications or other forms completed through telephone, email or in-person interviews.
- From government entities.

2.5. **Limiting Use, Disclosure and Retention**

NHI does not use or disclose health and personal information for purposes other than those for which it is collected, except with consent or as required or permitted by law. NHI retains information only as long as necessary for the fulfillment of identified purposes or to comply with the law.

- NHI will not sell client or employee personal or health information.
- NHI will disclose information only with consent.
- Access to client or employee personal or health information is given only to those who need the information in order to fulfill its identified purposes.

NHI retains personal and health information for:

- Only as long as necessary or relevant for the identified purposes.
- As required by law.

2.6. **Accuracy**

The extent to which NHI keeps personal and health information as accurate, complete and up-to-date will depend upon the use of the information and whether it is necessary for the identified purposes, taking into account the interests of the employees/clients and minimizing the possibility of using incorrect or inappropriate information about clients or employees – that may be used to make a decision about them.

Please refer to section on *Accuracy of Personal/Health Information* for more information/details.

2.7. **Safeguards**

NHI takes all reasonable measures to ensure client and employee health and personal information is kept safe from loss, unauthorized access, notification and disclosure.

- Please refer to *Securely Storing* section for more information/details.

NHI protects personal and health information disclosed to:

- NHI's affiliates, by ensuring that such affiliates have privacy policies regarding the use and disclosure of personal and health information; and
- NHI's agents and contractors, by contractual agreement stipulating the confidentiality of personal and health information and the purposes for which they may use and/or disclose this information.

NHI ensures its employees are aware of the importance of maintaining the security and confidentiality of client and employee personal and health information.

NHI disposes of and destroys this information with care, in order to prevent unauthorized parties accessing the information.

- Please refer to *Securely disposing/destroying* section for more information/details.

2.8. **Openness Regarding Privacy Policies and Practice**

NHI makes its privacy policies and practice available to clients and employees thorough written materials and its website.

2.9. **Access to Personal and Health Information**

Employees and clients may have access to any personal and health information that NHI collects about them, what it is used for, and to whom it is disclosed, except where the law requires or does not permit access.

Please refer to *Individual Access to Personal/Health Information* for more information/details.

2.10. **Challenging Compliance**

Employees and clients who wish to challenge NHI's compliance with its privacy policies may address their issues to NHI's Privacy Officer at the following address:

NHI Nursing & Homemakers Inc.
2347 Kennedy Road, Suite 204
Toronto, Ontario M1T 3T8

3. ACCURACY OF PERSONAL/HEALTH INFORMATION

The extent to which NHI keeps personal and health information as accurate, complete and up-to-date will depend upon the use of the information and whether it is necessary for the

identified purposes, taking into account the interests of the employees/clients and minimizing the possibility of using incorrect or inappropriate information about clients or employees – that may be used to make a decision about them.

Whenever possible, NHI corrects information given to an outside organization.

Since NHI uses personal and health information to provide services to clients, it is important that the information be accurate and up-to-date. Clients and employees who become aware of any changes to their personal or health information should contact NHI's Privacy Officer to update the information

The client record is updated when there is a change in health status, the care plan, the client's medications, or when the client is transitioned to another level of care or service.

4. CONSENT FOR COLLECTION, USE AND DISCLOSURE OF PERSONAL/HEALTH INFORMATION

NHI does not automatically gather personal information. Personal information is obtained if you voluntarily supply it to NHI via e-mail, completing our on-line forms or other means.

In the course of conducting our business, we at NHI may collect, use or disclose information as necessary (to fulfill the purpose for which it was collected) about individuals. That information may be considered personal information; such as an individual's home address, home telephone number or e-mail address. Information is not disclosed to anyone in the organization, except to staff required to perform their assigned tasks.

Personal information is generally collected at the time of hire. Sometimes personal information is collected during the course of employment for specific purposes, for example, administering benefits and policies, performance evaluations, disciplinary measures, and so on. By providing us with personal information, individuals' consent to the information's collection, use and disclosure is implied. Consent is also implied to NHI's use and disclosure of personal information for purposes that are reasonable and obvious and/or necessary in working with NHI

We safeguard personal information in a manner that is appropriate to the sensitivity of the information and as per privacy legislations. Personal information does not include information that cannot be associated with a specific individual, such as information that is aggregated or made anonymous.

There are some circumstances where the collection, use and disclosure of personal/health information is required or permitted by law. These circumstances include personal information necessary to:

- Investigate a breach of law or contravention of legal agreement.

- Provide aid in an emergency situation in which the life/safety/health of an individual is at risk.
- Comply with a court order or a subpoena.
- Provide information which is publicly available or subject to legal privilege.
- Collect an outstanding debt.

Consent is required for the collection of personal information, and the *subsequent use or disclosure of this information*. Where possible and practicable, NHI shall seek consent for the use or disclosure of personal information at the time of collection.

Individuals may withdraw their consent to NHI's collection, use and disclosure of their personal information; however, they should be aware that such withdrawal might impact negatively on NHI's ability to provide them with employment-related services.

Please refer *to Personal Information Protection and Electronic Document Act ("PIPEDIA")* section for more details/information.

5. INDIVIDUAL ACCESS TO PERSONAL/HEALTH INFORMATION

Employees and clients may have access to any personal and health information that NHI collects about them, what it is used for, and to whom it is disclosed, except where the law requires or does not permit access.

Upon request, an individual shall be informed of the existence, use, and disclosure of their personal/health information, and will be given access to that information.

NHI will do its best to respond to requests within a reasonable timeframe and with an explanation if requests are not to be met.

An individual will be able to challenge the accuracy and completeness of the information, and have it amended as appropriate.

Under certain circumstances or as permitted/required by law, NHI may not provide employees or clients to aspects of their personal or health information as maintained by NHI. These circumstances may include:

- The information is protected by solicitor-client privilege.
- Disclosing the information would threaten the life or security of another individual.
- The information was collected for purposes related to the detection of fraud.
- The information was generated during the course of a formal dispute resolution process.
- The information would likely reveal personal or health information about another individual.

In order to access personal information or to make inquiries, or complaints, individuals should make a written request to NHI's Privacy Officer at the following address:

NHI Nursing & Homemakers Inc.
2347 Kennedy Road, Suite 204
Toronto, Ontario M1T 3T8

Please note requests will be responded to promptly, and any issues addressed fairly.

6. SECURELY STORING, RETAINING AND DISPOSING/DESTROYING CLIENT RECORDS AND PERSONAL/HEALTH INFORMATION

NHI will ensure that any personal/health information is stored, retained, transferred and disposed of in a *secure* manner, and as per relevant laws/legislations. Security safeguards will protect the personal/health information against loss or theft, as well as unauthorized access, disclosure, copying, use or modification, this will be enforced by the CEO/President of NHI. Personal/health information regardless of the format in which it is held will be protected. NHI will only collect personal information that is necessary and legally required to fulfill the purpose for e.g., Human Resources collecting personal information during hiring.

As a general rule, all personal information is stored under the control of Human Resources and Management at NHI's offices. Managers and Supervisors may also have some personal information belonging to their direct reports.

Some personal information may also be transferred to the care of a NHI client in order to place a NHI employee on a temporary or contract work assignment. The client is made aware of NHI's commitment to the confidentiality of personal information, and is requested to respect this commitment and all applicable privacy laws.

Personal information may also be transferred to contractors, such as trainers and external payroll processors, to assist NHI in carrying out operational activities. In such cases, NHI takes the steps necessary to ensure that contractors comply with applicable privacy legislation.

Each department will routinely review and update its policies to safeguard personal and health information, specific to its circumstances. The methods of protection will include the below measures.

Please note in regards to disclosing health information for secondary use, this is not applicable at NHI.

6.1. Securely Storing

a) Restricted access to office.

b) Levels of access is granted to authorized personnel only to maintain security.

c) Security cameras in file cabinet areas.

d) Alarm system.

e) Lock and key for filing cabinets (practiced daily).

f) Following documents (hard copy) are kept in a secure locked filing cabinet and only accessible to authorized personnel:
- Client contracts signed by Senior Management.
- Memorandum of Understanding signed by the client and Senior Management team.
- Consent forms: Signed by client, patients, family members or Power of Attorney ("POA").
- Clients'/Patients' financial information.
- Clients'/Patient's chart.
- Employee files.

g) Only team members who are actively involved in a client's care have access to the client's record.

6.2. **Securely Retaining**

a) As per the Government of Canada, generally speaking any records/supporting documents such as an organization's tax documents, should be retained for a period of six (6) years.

b) If an individual/client requests for ***access*** to a record - protocol and the Personal Health Information Protection Act ("PHIPA"), will be adhered to; information will be retained *for as long as necessary* until matters pertaining to the request are completed.

c) As per the Employment Standards Act ("ESA"), *Employee Personal Information* (name, address, date of birth; if the employee is a student and under the age of 18, and start date of employment) - must be kept for three (3) years after the employee has stopped working for the employer/organization. The minimum requirement for *Employee Records* is three (3) years after the date to which the record relates.

d) Patient/Client Records entail medical record, notes, charts and other material. Medical Records and notes, and charts and other material regarding patient/client care are all part of a patients'/clients' *Records of Personal Health Information*:
- Under the Public Hospitals Act, for an adult in-patient (18 years and older) the minimum retention period is ten (10) years after discharge/death.
- Under the Public Hospitals Act, for an adult out-patient (18 years and older), the minimum retention period is ten (10) years after last visit/death.
- The retention period for records such as disinfection logs, education and training material varies.

e) If in the case of a pending legal proceeding/valid purpose, retain records for longer than ten (10) years.

f) NHI retains personal and health information for:
- Only as long as necessary or relevant for the identified purposes.
- As required by law.

6.3. **Organizational (e.g., confidentiality agreements and limited access for staff)**

a) NHI will ensure that all employees are aware of the importance of maintaining the confidentiality of personal/health information.

b) All NHI employees sign a Confidentiality Agreement.

c) Employees are aware of Personal Information Protection and Electronic Document Act ("PIPEDA") and Personal Health Information Protection Act ("PHIPA"), and any other relevant laws/legislations.

6.4. **Securely disposing/destroying**

NHI adheres to the Personal Information Protection and Electronic Document Act ("PIPEDA") and Personal Health Information Protection Act ("PHIPA") regarding the disposal/destruction of information/records.

Care will be utilized when disposing or destroying personal/health information and records, to prevent unauthorized parties from gaining access to the information. NHI adheres to the PHIPA principle of disposing information/records in a "secure manner."

Principle 5 of PIPEDA states that: *"Personal information that is no longer required to fulfil the identified purposes should be destroyed, erased, or made anonymous. Organizations shall develop guidelines and implement procedures to govern the destruction of personal information."*

PIPEDA also mentions that care needs to be employed when disposing or destroying personal information, in order to prevent unauthorized parties from gaining access to the personal information.

NHI employees will be provided with Education and Training on their roles and responsibilities in protecting any personal information and adhering to legal requirements.

NHI will ensure that any personal/health information is properly disposed of with care.

6.4.1. <u>Electronic</u>

- NHI has in place authorized personnel to destroy any electronic data.

- Electronic copies entail any information that is stored on an electronic device/media for e.g., computer hard drive, printer/photocopier hard drive, memory disks, USB flash drives, mobile phones or any magnetic tapes.
- Any electronic records will be fully deleted, therefore; the information cannot be recovered or mis-utilized.
- NHI will destroy any copies and backup files.
- All personal information on electronic devices such as computers or photocopiers will be permanently deleted prior to disposing/destroying them.

  It is good practice to destroy sensitive information utilizing the following methods:
  - There are variety of methods to destroy electronic media for e.g., disintegration, incineration, pulverizing, shredding and even melting.
  - Media can also be cleared by overwriting. Software and hardware products can be utilized to overwrite the media and replace with non-sensitive data.
  - Degaussing is another method, wherein magnetic media is exposed to a magnetic field, therefore; making the data unrecoverable.

6.4.2. Hardcopy

- Hardcopy entails any physical data for e.g., paper print outs/paper files, printer ribbons, notes, memos, messages, any correspondence or reports.
- NHI will securely shred any paper files in order to prevent any privacy breaches.
- NHI has in place authorized personnel to destroy any personal paper files.
- NHI will ensure that personal information cannot be retrieved/reconstructed.
- Unacceptable methods are recycling personal information records or leaving personal information documents for garbage pick-up.

Procedures pertaining to the storing, retaining and destroying of personal/health information will be reviewed on an on-going basis and updated accordingly, and as per any updates to applicable laws/legislations.

7. REFERENCES

1. St Joseph's Home Care (SJHC). Privacy & Personal Information Policy. http://www.stjosephshomecare.ca/privacy-policy

2. Government of Ontario (Ontario.ca). e-Laws. Personal Health Information Protection Act, 2004, S.O. 2004, c. 3, Sched. A. https://www.ontario.ca/laws/statute/04p03

3. Office of the Privacy Commissioner of Canada. Personal Information Retention and Disposal: Principles and Best Practices. https://www.priv.gc.ca/en/privacy-topics/business-privacy/breaches-and-safeguards/safeguarding-personal-information/gd_rd_201406/

4. Government of Canada (Canada.ca). Justice Laws Website. Personal Information Protection and Electronic Documents Act (S.C. 2000, c. 5). Personal Information Protection and Electronic Documents Act

5. Government of Canada (Canada.ca). Taxes - Income Tax. Keeping Records https://www.canada.ca/en/revenue-agency/services/tax/businesses/topics/keeping-records/where-keep-your-records-long-request-permission-destroy-them-early.html#kp_yr_rcrds

6. Privacy Transparency Empowerment. Part X of the CYFSA: Retention, Transfer and Disposal of Personal Information. Part X of the CYFSA: Retention, Transfer and Disposal of Personal Information | Information and Privacy Commissioner of Ontario

7. Government of Ontario (Ontario.ca). Freedom of Information and Protection of Privacy Manual. Chapter 7: Privacy Fundamentals. Chapter 7: Privacy Fundamentals | Freedom of Information and Protection of Privacy Manual | ontario.ca

8. Government of Ontario (Ontario.ca). e-Laws. Freedom of Information and Protection of Privacy Act, R.S.O. 1990, c. F.31. Freedom of Information and Protection of Privacy Act, R.S.O. 1990, c. F.31 | ontario.ca

9. Government of Ontario (Ontario.ca). e-Laws. Personal Health Information Protection Act, 2004, S.O. 2004, c. 3, Sched. A. Personal Health Information Protection Act, 2004, S.O. 2004, c. 3, Sched. A | ontario.ca

10. College of Occupational Therapists of Ontario. Standard for Record Keeping, 2023. Standard for Record Keeping, 2023 — The College of Occupational Therapists of Ontario

11. Government of Ontario (Ontario.ca). e-Laws. Your Guide to The Employment Standards Act. Record Keeping. Record keeping | Your guide to the Employment Standards Act | ontario.ca

12. Ontario Hospital Association (OHA). Records Retention Toolkit: A Guide to the Maintenance and Disposal of Hospital Records. Records Retention Toolkit, September 2022.pdf