Category:	N/A	Date Approved:	October, 2025
Subcategory :	N/A	Issuing Department:	Administration
Section #	N/A	Approved By:	VP, Operations; Privacy Officer
Policy Title:	Privacy & Confidentiality		

POLICY

Primacare Living Solutions Inc. is committed to protecting the privacy and confidentiality of residents, families and employees. This policy outlines how Personal Information (PI) and Personal Health Information (PHI) is collected, used, disclosed, stored and protected and applies to all employees, physicians, volunteers, students, contractors and any other individuals who have access to PI and PHI.

Primacare Living Solutions Inc. will obtain written consent to collect, use, retain or disclose PI or PHI to a third party without written consent from the resident, Substitute Decision Maker (SDM) or employee.

Resident information, with or without the resident's name and including photos or videos, is never to be posted on or referred to on any public forum, including bulletin boards in the home, websites, blogs and social media without expressed and documented consent from the resident/SDM.

New employees, students or volunteers are required to read and sign a letter of Nondisclosure of Confidential Information as a condition of employment or placement, annually and other times as determined by Primacare Living Solutions Inc.. Contractors, vendors, and other groups may be required to sign this letter as well.

Employees whose actions result in an unauthorized collection, use or disclosure of PI OR PHI may be subject to discipline up to and including termination.

Privacy incidents will be reported to the Executive Director (ED) of the home. Incidents may include suspected or actual breaches of privacy laws, internal privacy policies, contractual obligations, etc. The ED will report the incident to the Privacy Officer.

Privacy incidents will be reviewed by the home in collaboration with the Privacy Officer. A record of all privacy incidents will be maintained by the home and reported to the Quality Committee. System level improvements will be identified and implemented as needed.

GUIDELINES

This policy is based on ten internationally recognized privacy principles, which have been adopted as the basis for Canadian privacy statutes and regulations.

Principle 1 - Accountability:

- Primacare Living Solutions Inc. Inc. is responsible for PI or PHI in our possession or control, including information that has been transferred to a third party for processing. The organization will use appropriate means to provide a comparable level of protection while information is being processed by a third party.
- Ensuring compliance to this policy is the responsibility of Senior Management. The organization's Privacy Officer, the Vice President of Operations, has been designated day-to-day responsibility for the organization's privacy policy and processes. The Privacy Officer may be contacted at:

Category:	N/A	Date Approved:	October, 2025
Subcategory :	N/A	Issuing Department:	Administration
Section #	N/A	Approved By:	VP, Operations; Privacy Officer
Policy Title:	Privacy & Confidentiality		

Primacare Living Solutions Inc.
203-200 Ronson Drive, Toronto, ON M9W
5Z9, Attn: Vice President.

- Other individuals within Primacare Living Solutions Inc. may also be assigned to take responsibility for the day-to-day handling and management of resident PI OR PHI.
- Executive Directors and Directors of Care are accountable for ensuring employees receive proper training on this and other privacy - related policies and how to apply these policies in their day-to-day work.

Principle 2 - Identifying Purposes for Collection

- Collect, use, retain or disclose PI or PHI for the following purposes only:
    - To provide safe, high-quality care to the resident and understand their needs and preferences.
    - To establish and maintain responsible business relations with residents;
    - To develop, enhance, market or provide Primacare Living Solutions Inc. services;
    - To manage and develop Primacare Living Solutions Inc. business and operations, including human resources and employment matters;
    - To meet legal and regulatory requirements; and
    - To detect and prevent fraud, and to help safeguard the interests of Primacare Living Solutions Inc.

  All purposes should be limited to those that a reasonable person would consider appropriate in the circumstances.

Principle 3 - Consent for Collection, Use, and Disclosure

- In certain circumstances, PI or PHI may be collected, used, retained or disclosed without the knowledge and consent of the resident. This includes the following:
    - If seeking consent may be impossible or impractical, such as when the resident is seriously ill or mentally incapacitated, or if reasonable efforts have been made to contact the resident/SDM and consent cannot be obtained in a timely way.
    - If disclosure is necessary by law or when we need to disclose information to protect our interests for debt collection or in the context of legal or administrative proceedings.
    - If seeking the consent of the individual might defeat the purpose of collecting the information. This may include the investigation of fraud, a breach of an agreement or a Contravention of a federal or provincial law;
    - for the purpose of a proceeding (e.g. regulatory college proceeding);
    - for the purpose of obtaining payment for health care or related goods and services;
    - for the purposes of risk management, incident analysis or improving the quality of care;
    - If the information is generally considered to be in the public domain;
    - If there is an emergency where the life, health or security of an individual is threatened;
    - If we are involved in a corporate re-organization or we sell or merge all or part of our business
- If the consent of a resident or SDM is needed, it must meet the following legal requirements:
    - The consent must be from the appropriate person (resident/SDM/POA);

Category:	N/A	Date Approved:	October, 2025
Subcategory :	N/A	Issuing Department:	Administration
Section #	N/A	Approved By:	VP, Operations; Privacy Officer
Policy Title:	Privacy & Confidentiality		

  - The consent must be knowledgeable. This means that the individual must know the purposes of the collection, use, or disclosure as described in this policy;
  - The consent must not be obtained through deception or coercion;
  - The individual must be given the option to withdraw consent, but the withdrawal will only be on a going- forward basis.

- If an individual has expressly withheld or withdrawn consent to use or disclose their PI OR PHI, staff are not permitted to use (i.e., view, modify, etc.) the information for the purpose of providing or assisting in the provision of care, unless:
  - the staff member has obtained express consent from the individual; or
  - it is an emergency and express consent cannot be obtained in a timely manner.

- Reasonable effort should be made to collect all PI or PHI about a resident directly from the resident except as otherwise consented to by the resident (e.g., through a SDM), or as permitted or required by law. Indirect collection is not permitted except in limited circumstances: where the information to be collected is necessary for providing resident care and it is not reasonably possible to collect directly from the resident in an accurate or timely fashion, The information will be collected from another person or entity permitted to disclose the information.

Principle 4 - Limiting Collection

- Primacare Living Solutions Inc. will only collect PI or PHI by fair and lawful means, and will:
  - limit its collection of PI or PHI to that which is necessary for a lawful purpose identified by the organization
  - not collect more PI or PHI than is reasonably necessary for the purpose; and
  - not collect PI or PHI if non-identifying information will serve the purpose.

Principle 5 - Limiting Use, Disclosure, and Retention

- PI OR PHI will not be used or disclosed for purposes other than those for which it was collected, except with the express consent of the individual or as permitted or required by law.

- De-identification of PI or PHI involves modifying the information to remove identifying features or details. De-identified information may be used for non-care purposes, such as quality improvement initiatives. Steps should be taken to mitigate risks associated with the potential re-identification of PI or PHI. Any attempt to re-identify PI or PHI is prohibited.

- The PI OR PHI that the organization collects may be transferred to subsidiary and affiliated companies; our insurers and bankers; medical and insurance carriers; and other companies engaged in contractual activities on our behalf for the purposes for which the personal information is to be used.

- Employees are accountable for ensuring sensitive information is only used and disclosed for authorized purposes and to authorized individuals. Employees may not use (i.e., access, view, handle) PI OR PHI unless they have a legitimate clinical or business “need to know” directly related to their role and responsibilities in the home. If in doubt, employees should ask their supervisor for further guidance..

- The organization may retain certain personal information of resident when they cease to live in the Home.

Principle 6 - Accuracy

- Employees will take reasonable steps to ensure PI or PHI in our control is as accurate, complete, and up to date as necessary for the purposes for which it is to be used or disclosed

Principle 7 - Safeguards

- Primacare Living Solutions Inc. will take steps that are reasonable in the circumstances to ensure that PI or PHI is protected against theft, loss and unauthorized use or disclosure. These safeguards will be reasonable in the circumstances and commensurate to the level of risk. Primacare Living Solutions Inc. uses the following categories of safeguards to protect information:
  - physical safeguards (e.g., locking filing cabinets and rooms);
  - administrative safeguards (e.g., policies, contracts, privacy training, etc.); and
  - technical safeguards (e.g., multifactor authentication, encryption, audits, etc.).
- The organization will protect PI OR PHI regardless of the format in which it is held.
- All employees, students, and volunteers will complete mandatory privacy training during orientation and annually thereafter as a condition of employment. Upon successful completion of the training, employees must complete a Letter of Nondisclosure of Confidential Information (attestation).
- The Privacy Officer advises on the procurement, configuration and implementation of digital solutions (or new features for existing applications like Point Click Care) when the solutions are intended to include employee information, personal information and/or personal health information. The organization supports this by:
  - Providing and rating mandatory privacy criteria for RFPs;
  - Assessing vendors/solutions during procurement;
  - Supporting communications with external consultants; and
  - Working with teams to mitigate privacy risks before going live.
- The disposal or destruction of PI or PHI should be done with care to prevent unauthorized parties from gaining access to the information.

Principle 8 - Openness about Information Policies and Practices

- Primacare Living Solutions Inc. will make specific information about its information management policies and practices readily available to individuals. The organization does this through a written statement made available to the public on our website.

Principle 9 - Individual Access

- Upon request, a resident or SDM will be informed of the existence, use and disclosure of their PI OR PHI in the

custody/control of Primacare Living Solutions Inc. and will be given access to it. The home will respond to such requests within 30 days and at minimal cost to the individual. The information will be provided in a clear and readable format. For more information See Release of Resident Information Access to Health Care Records.

- The home will take reasonable steps to ensure that processes are in place to review system controls and/or logs to detect and deter unauthorized use or access to resident PI or PHI. The Executive Director may monitor use of any of the home's digital technologies and will conduct regular audits of Point Click Care. These audits include proactive audits (e.g., random residents) and reactive audits (e.g. following a privacy incident or complaint.
- In certain situations, the home may not be able to provide access to any or all of the PI or PHI it holds about an individual. Access to information may be denied where an exception applies under FIPPA or PHIPA. Exceptions are limited and specific and may include information that is prohibitively costly to provide, information that contains references to other individuals, information that cannot be disclosed for legal, security, or commercial proprietary reasons, and information that is subject to solicitor-client or litigation purposes. The reasons for denying access will be provided to the individual upon request.

Principle 10 - Challenging Compliance

- An individual will be able to challenge the organization's compliance to the above principles with its Privacy Officer. The Privacy Officer, or delegate, will investigate all complaints related to compliance. If a complaint is found to be justified, the organization will respond appropriately. Complaints may also be made directly to the Office of the IPC.
- An individual can challenge the accuracy and completeness of their PI or PHI and have it amended as appropriate. Amendments will generally not involve deletions or alterations of the original record but would take the form of addendums to the record. Where appropriate, the amended information will be shared with third parties who have access to the information.
- If an individual believes their PI or PHI on record is incorrect, they can request a correction. If the home disputes the correction, the individual will have an opportunity to provide the home with a statement of disagreement that will be attached to the record. Authorized employees must read and disclose this statement when accessing or sharing the related information.

PROCEDURE FOR MANAGING PRIVACY BREACHES

STEP 1 – Notify Employee and Other Custodians

- Notify employee involved in the breach including the Privacy Officer, Director of Care or delegate, and Executive Director
- Depending on the nature or seriousness of the privacy breach, the Executive Director will send an email Alert to Senior Management
- Engage social worker to support residents & families as needed
- If the breach involves PI or PHI on an electronic system shared between multiple custodians, notify all affected

custodians.

STEP 2 – Identify the Scope of the Breach and Take Steps to Contain It

- Identify the scope of the breach including individuals or organizations who may have been involved with or responsible for the breach and the nature and amount of PI or PHI affected
- Retrieve any copies of PI or PHI that have been disclosed
- Ensure no copies of the PI or PHI have been made or retained by anyone not authorized to receive the information. Record the person's contact information in case follow-up is needed.
- Determine whether the breach would allow unauthorized access to any additional PI or PHI. Take appropriate steps such as changing passwords within electronic systems and/or temporarily shutting down the system entirely.
- In the case of unauthorized access considering suspending the individual's access rights.

STEP 3 – Notify the Individuals Affected by the Breach, The Information and Privacy Commissioner and/or Regulatory Colleges

Direct Notification of Affected Individual(s):

- Notify individuals affected by the breach at the first reasonable opportunity
- There are many factors to consider when determining the method of notification, for e.g. the sensitivity of the PI or PHI. If unsure, consult with the Privacy Officer
- When notifying the affected individual(s), provide the following information:
    - Where appropriate, the name of the individual responsible for the breach
    - The date of the breach
    - A description of the nature and scope of the breach
    - A description of the PI or PHI that was subject to the breach
    - Measures implemented to contain the breach
    - The name and contact details of the Executive Director who can address any inquiries.
    - Notice to the individual letting them know they are entitled to make a complaint to the Information and Privacy Commissioner.
    - If financial information or information from government-issues documents (e.g. health care numbers) are involved, include the following statement in the notice:

      "As a precautionary measure, we strongly suggest that you contact your bank, credit card company and related government offices to advise them that you may have been affected by this breach. We recommend you monitor and verify all of your bank accounts, credit cards, and any other transactional statements for any suspicious activity. If you suspect misuse of your personal information, you can obtain a copy of your credit report from a credit reporting bureau to verify the legitimacy of the transactions listed.

      - *Equifax at 1-800-465-7166 or www.equifax.ca*
      - *TransUnion at 1-800-663-9980 or www.transunion.ca*

      If you are concerned that you may be a victim of fraud, you may request these bureaus place a fraud alert on your credit files instructing creditors to contact you before opening any new accounts.

Category:	N/A	Date Approved:	October, 2025
Subcategory :	N/A	Issuing Department:	Administration
Section #	N/A	Approved By:	VP, Operations; Privacy Officer
Policy Title:	Privacy & Confidentiality		

If your health card number has been affected by the breach, you should report your lost or stolen health card number:

- *ServiceOntario INFOline at 1-866-532-3161 or 1-800-387-5559*

If you suspect misuse of your health card number, you can report suspected cases of fraud by calling:

- *Ministry of Long Term Care at 1-888-781-5556 or email at reportohipfraud@moh.gov.on.ca*

You may also wish to review this publication from the Information and Privacy Commissioner of Ontario, Identity Theft: A Crime of Opportunity."

Indirect Notification of Affected Individual(s):

- There are exceptional circumstances where you may consider providing indirect notification to affected individuals. If the organization is considering indirect notification, the Privacy Officer should consult with the Information and Privacy Commissioner. Indirect notice to individuals may be considered where one or more of these exceptional circumstances apply:
  - The breach affects a significantly larger number of individuals making notifying the affected individuals directly impractical.
  - The risk of harm to affected individuals has reasonably been determined to be low.
  - You are unable to determine the identities of affected parties despite taking reasonable steps to do so.
  - There are questions regarding reliability/accuracy of contact information.
    Note: outdated contact information for a portion of the affected parties doesn't mean that the affected parties should be notified indirectly. A hybrid approach to notification involving both direct and indirect methods may be appropriate.
  - Direct notification would be reasonably likely to be harmful or detrimental to the affected individuals.

Notification of the IPC

- Custodians are required to report certain privacy breaches to the IPC. At Primacare Living Solutions Inc., this reporting is completed by the Privacy Officer as described in Reporting a Privacy Breach to the IPC

Notification of Regulatory Colleges

- Notification of the healthcare practitioner's regulatory college is required within 30 days of the breach if any of the following apply:
  - The practitioner was an employee or agent of Primacare Living Solutions Inc. and was terminated, suspended or disciplined as a result of the breach;
  - The practitioner's privileges or affiliation are revoked, suspended or restricted as a result of the breach;
  - The practitioner resigns and the custodian has reason to believe the resignation is related to the investigation or any actions carried out as a result of an alleged breach;
  - The practitioner relinquishes or voluntarily restricts their privileges or affiliation with Primacare Living Solutions Inc. and the custodian has reasonable grounds to believe it is related to the investigation or any actions carried out as a result of an alleged breach.

Category:	N/A	Date Approved:	October, 2025
Subcategory :	N/A	Issuing Department:	Administration
Section #	N/A	Approved By:	VP, Operations; Privacy Officer
Policy Title:	Privacy & Confidentiality		

STEP 4 – Investigate and Remediate

- Conduct an internal investigation to:
  - Ensure the immediate requirements of containment and notification have been met
  - Review the circumstances surrounding the breach
  - Review the adequacy of existing processes, policies and procedures related to protecting PI or PHI
- The chart below provides guidelines regarding the appropriate response to a privacy breach.

Type of Breach	Definition	Appropriate Response
Level I Breach (Inadvertence, Negligence)	Unintentional violations of privacy policies or legislation that may be caused by lack of knowledge or training, environmental factors, carelessness, or other human error, and include: • Accidentally accessing High or Moderately Sensitive information including PI or PHI that is not required to carry out work-related duties. • Inadvertently disclosing PI or PHI to the wrong person. • Using improper channels to obtain access to PI or PHI that you are otherwise authorized to access. • Leaving your computer unattended while you are logged into a system that includes High or Moderately Sensitive information, including PI or PHI. • Discussing High or Moderately Sensitive information, including PI or PHI, or leaving such information unattended, in a public area. • Second incident of any Level I breach, depending on severity (does not have to be the same breach).	1. a) Verbal and / or written reminder of obligations or letter of expectations (to be recorded by supervisor); and/or b) First written warning in staff member's personnel file. 2. Education on privacy policies and law. 3. Possible report to applicable Regulatory College. 4. Possible report to the Information and Privacy Commissioner.
Level II Breach (Intentional, "Knew or Ought to Have Known", Repeated Level 1 offence)	Intentional breaches and/or violation of known policies and legislation relating to access, use, and disclosure of PI or PHI. These include situations where the employee ought to have known that their actions would violate policies or legislation. Examples include: • Repeated violations or third incident of any Level I breach, depending on severity (does not have to be the same breach); • Accessing ConnectingOntario for a non-care purpose; • Intentionally accessing or using High or Moderately Sensitive information, including PI or PHI, for a purpose that is out of scope of their Primacare Living Solutions Inc. job	1. a. Final written warning in staff member's personnel file; and/or b. Suspension of employment 2. Education on privacy policies and law. 3. Report to applicable Regulatory College. 4. Report to the Information

	description.	and Privacy Commissioner.
Level III Breach (Personal gain, Malice, Serious repeated offence)	Intentional violations of policies or legislation for personal gain or to cause patient or organizational harm and include: • Second incident of any Level II breach, depending on severity (does not have to be the same breach); • Intentional and unauthorized use or disclosure of High or Moderately Sensitive information, including PI or PHI. • Collecting PI or PHI under false pretenses; • Accessing, using and/or disclosing High or Moderately Sensitive information, including PI or PHI, for commercial advantage, personal gain or malicious harm; • Failure to cooperate with the Privacy Officer in any investigation or proceeding; • Failure to comply with a Privacy Officer resolution or recommendation.	1. Termination of employment 2. Report to applicable Regulatory College. 3. Report to the Information and Privacy Commissioner.

- Maintain a log of all privacy breaches in the home. For each privacy breach record:
  - The name of the employee or agent that caused the breach (if applicable) for e.g. in the case of unauthorized access to PI or PHI.
  - The nature, type, scope and cause of the breach
  - The number of individuals affected by the breach
  - A description of the PHI that was subject to the breach
  - A summary of the steps taken to respond to the breach
- The Privacy Officer is required to report privacy breach statistics to the IPC as required by PHIPA. See Annual Reporting of Privacy Breach Statistics to the Commissioner for further details.

DEFINITIONS

Custodian: means a person or organization who has custody or control of personal health information as a result of or in connection with performing the person's or organization's powers, duties or work.

Deidentification: in relation to the personal health information of an individual, means to remove any information that identifies the individual or for which it is reasonably foreseeable in the circumstances that it could be utilized, either alone or with other information, to identify the individual.

Personal Information is any information about an identifiable individual that is recorded in any form and includes race, ethnic origin, colour, age, marital status, family status, religion, education, medical history, criminal record, employment history, financial status, address, telephone number, and any numerical identification, such as Social Insurance Number, Health Card Number. It is also deemed personal information to identify a Resident as living in the facility to anyone not employed by PRIMACARE LIVING SOLUTIONS. The term does not include information that does not identify particular

individuals, like aggregate statistics or anonymous employee data.

Personal Health Information means identifying information about an individual in oral or recorded form, if the information,

- relates to the physical or mental health of the individual, including information that consists of the health history of the individual's family,
- relates to the providing of health care to the individual, including the identification of a person as a provider of health care to the individual,
- is a plan that sets out the home and community care services for the individual to be provided by a health service provider or Ontario Health Team pursuant to funding under section 21 of the *Connecting Care Act, 2019*,
- relates to payments or eligibility for health care, or eligibility for coverage for health care, in respect of the individual,
- relates to the donation by the individual of any body part or bodily substance of the individual or is derived from the testing or examination of any such body part or bodily substance,
- is the individual's health number, or
- identifies an individual's substitute decision-maker is the individual's digital health identifier or other identifying information related to the creation of the digital health identifier.

RELATED DOCUMENTS

Release of Resident Information-Access to Health Care Records

REFERENCES

Fixing Long Term Care Act (FLTCA) 2021,
Ontario Regulations 246/22.
Personal Health Information Protection Act, 2004 (PHIPA)
Freedom of Information and Protection of Privacy Act, 1990 (FIPPA).
The Personal Information Protection and Electronic Documents Act (PIPEDA) - Office of the Privacy Commissioner of Canada
Reporting of Privacy Breach Statistics to the Commissioner
Reporting a Privacy Breach to the IPC
The privacy breach management toolkit - Canada.ca
Responding to a Health Privacy Breach: Guidelines for the Health Sector | Information and Privacy Commissioner of Ontario