# Amplify Care
# Privacy Policy

v.4

January 2024

235 The Boardwalk, Suite 301, Kitchener ON, N2N 0B1
**P:** (519) 885-0606 | **E:** info@amplifycare.com

## Document Control

- The electronic version of this document is recognized as the only valid version.

| | |
|---|---|
| **Document Location:** | Amplify Care Organizational Policies and Procedures |
| **Document Contributors:** | External Privacy Consultant; Amplify Care Leadership Team |
| **Document Prime:*** | Sylvia Carney, Manager, Privacy |

*Enquiries relating to this document should be referred to the Document Prime.

## Revision History

| Version No. | Date | Summary of Change | Revised By |
|---|---|---|---|
| [1] | April 21, 2020 | Initial Draft | S. Carney |
| [2] | May 14, 2020 | Incorporate edits from Privacy Advisory Cttee | S. Carney |
| [3] | June 27, 2020 | Incorporate edits from Jane Dargie CS | S. Carney |
| [4] | January 25, 2024 | Revisions from Amplify Care Privacy Office [changes for currency only] | S. Carney |
| [5] | | | |

## Approval History

| Approver | Title | Approved Date |
|---|---|---|
| Ted Alexander | VP, Partnerships and Clinical Innovation | July 30, 2020 |
| | | |

## Purpose of Policy

The Privacy Policy establishes the principles and regulatory obligations which will guide the Amplify Care related to the collection, use, disclosure and retention of personal health information (PHI). This policy applies to all programs and services of the Centre for Family Medicine Care Innovations (CFFM CI)/Amplify Care ("Amplify Care"). Some parts of this policy will apply only in a particular context, contingent on the role which Amplify Care is fulfilling under provincial privacy law.

## Background

As a Corporation, CFFM CI operating as Amplify Care engages in activities to improve the quality of patient care through the effective and innovative use of enabling technologies. Amplify Care is primarily funded by Ontario Health and serves as a delivery partner for various digital initiatives. Amplify Care also supports change management and evaluation initiatives in other provinces.

## Privacy Context of Amplify Care

The *Personal Health Information Protection Act, 2004*[1] (PHIPA) establishes a statutory privacy framework for protecting PHI in Ontario. Responsibilities are assigned under PHIPA to health information custodians ("HICs" like clinics and individual physicians), and to "agents", or those who act on behalf of HICs. The Regulations[2] made under PHIPA, specify further requirements for service providers, where those service providers enable HICs to use electronic means to collect, use, modify, disclose, retain or dispose of PHI ("Service Providers"). The Regulations also specify requirements for "health information network providers" ("HINPs"), which are persons or organizations that enable two or more HICs to use electronic means to disclose PHI to each other.[3]

Under PHIPA, Amplify Care in its development, provision and/or deployment of various digital health programs and services, acts variously as:

- an agent of HIC Participants in certain Amplify Care programs and services
- an Electronic Service Provider to HICs
- a HINP to HIC Participants

According to these roles, Amplify Care is broadly accountable to:

- collect, use, disclose and retain/destroy Personal Health Information (PHI) in accordance with PHIPA
- employ safeguards to protect the PHI entrusted to Amplify Care by Participants in Amplify Care programs and services

Amplify Care also supplies services to non-HIC Participants, and commits to the same privacy accountability for non-HICs as for HIC Participants.

The accountability of CFFM CI in its role as a HINP, is set out in Amplify Care Health Information Network Provider Accountability Statement.

1. ACCOUNTABILITY

*An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles.*

Amplify Care has a Privacy Program in which all employees and contract staff play a part. Amplify Care provides oversight to third-party service providers who are contractually bound to comply with these principles in their support of Amplify Care programs and initiatives.

Key components of this program:

- Annual employee privacy training and awareness which guides personnel in their handling of personal information and personal health information (PI/PHI), and acknowledgement that they understood the training and their responsibilities
- Deployment teams trained to support the Centre's privacy mandate
- privacy training specific to Amplify Care's digital programs and services
- a robust Privacy Guide made available to all HICs participating in eServices eReferral Program
- monitoring and compliance oversight
- security training & awareness program for internal personnel
- privacy impact assessment on all initiatives involving PHI or PI
- developing & maintaining Privacy Policy

Amplify Care commits to periodically reviewing and maturing the Privacy Program and has designated the Manager, Privacy as the privacy contact for the organization. The Privacy Manager is delegated responsibility by the Executive Director, Excellence and Clinical Experience at Amplify Care.

The Privacy Office can be reached at: privacy@amplifycare.com

## 2. PURPOSE OF COLLECTION

*The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.*

Amplify Care does not directly collect PHI unless, in the course of executing its role as agent to a HIC, it is required and authorized to do so Any collection of PHI will be directed by the relevant HIC as that HIC is permitted or required to collect the PHI pursuant to PHIPA s. 17(1).

On the occasions when Amplify Care collects PI, we will obtain consent; explain the purposes for the collection of the PI, at or before the time of collection; and limit the PI to the amount Amplify Care necessary for the identified purposes.

## 3. CONSENT

*The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.*

When the Amplify Care is acting as a HIC's agent, it will be directed by the HIC and comply with any consent requirements in Section 18 of PHIPA. This means that in connection with any of Amplify Care's digital offerings, consent related to PHI will be built into the solution or supporting policies and processes, and individuals will be made aware of the purposes for which PI is being collected, used, disclosed and retained. In accordance with Section 19 of PHIPA, Amplify Care will work with contracted third-party service providers to define any applicable business requirements, such as functionality to record consent as well as to apply consent directives on behalf of the HIC and/or to comply with consent directives previously applied by the HIC.

## 4. LIMITING COLLECTION

*The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.*

Amplify Care does not directly collect PHI unless, in the course of executing its role as agent to a HIC, or as a HINP, it is required or permitted to do so. Any collection of PHI will be limited to that which is necessary for the HIC's purposes or for the purpose of providing the service. Third-Party Service Providers will be contractually bound to comply with this principle as they design and implement applicable solutions.

## 5. LIMITING USE, DISCLOSURE AND RETENTION

*Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfillment of those purposes.*

Use, disclosure and retention of PHI by Amplify Care will be limited to the purposes required and permitted for execution of its role in various electronic/digital offerings. When Amplify Care is acting as an agent, use and disclosure of PHI would only be as authorized by the relevant HIC. When acting as a HINP or service provider, Amplify Care does not use nor disclose PHI.

PHI will be securely retained only as required to fulfill the purpose, and in accordance with PHIPA and any applicable agreements addressing retention parameters.

## 6. ACCURACY

*Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.*

Amplify Care will make reasonable efforts to ensure the accuracy of any PHI which is collected, used or disclosed in the fulfilment of its role as an agent of a HIC. When operating in its capacity as a HINP or service provider, the primary obligation relating to accuracy lies with the participating HICs/non-HICs who have custody and control of the PHI.

## 7. SAFEGUARDS

*Personal information shall be protected by safeguards appropriate to the sensitivity of the information.*

Amplify Care abides by the following additional privacy & security guidelines:

### I. ADMINISTRATIVE

1. Amplify Care in its various roles under PHIPA will enter into a written agreement with Participants in the eReferral program or similar eService offerings.

2. Organizational policies and procedures for privacy and security management have been developed, implemented, and are monitored and enforced. A mechanism is in place for reviewing and updating the policies and procedures. Employees, contract staff, students and volunteers are required to comply with these policies as a condition of their employment or applicable relationship with Amplify Care.

3. Service providers are required to comply with Amplify Care's organizational policies and procedures for privacy and security management.

4. Confidentiality and/or non-disclosure agreements (as applicable) are in place for all employees, contract staff, students, volunteers and service providers. These agreements contain appropriate measures for breach of privacy, confidentiality, or security, up to and including dismissal or termination of the contract or agreement, as appropriate.

5. Mandatory and ongoing privacy, confidentiality, and security awareness training is conducted for all employees, contract staff, students and volunteers. Service Providers are required to complete Amplify Care privacy & security awareness training or agree in writing to providing substantially similar content to their personnel.

6. Amplify Care employees and consultants generally have no ability or permission to access personal health information (PHI). If access to PHI is required in the course of providing an Amplify Care service, our employees and consultants are required to adhere to Amplify Care policies and are prohibited from using such information for any purpose other than the provision of the service, or from disclosing such information to any third party.

7. A Privacy/Security Breach protocol with respect to the privacy and security of personal information and/or business confidential Information has been developed and implemented.

## II. TECHNICAL

8. Access control mechanisms, including authorization and authentication measures (such as computer password protection and unique log-on identification) have been implemented to ensure that only authorized personnel can access the Amplify Care environment.

9. Authorized individuals are granted access based on role. Principles of least privilege and need-to-know are employed when provisioning access.

10. Amplify Care maintains audit logs of user activities and system administrator activities. Amplify Care shall audit and monitor such logs.

11. Remote electronic access to the Amplify Care environment is provided via Virtual Private Network.

12. Virus-protection and firewalls have been implemented and are maintained.

13. Multi-factor authentication in place for all users

## III. PHYSICAL

13. The Amplify Care takes reasonable measures to ensure that only authorized individuals have access to physical locations and assets critical to the organization, such as corporate offices, computing equipment and data centres. Environmental controls further address risks to the physical locations and safety of employees, such as fire, water, electrical surges, power outages, corporate espionage, and other dangers.

## 8. OPENNESS

*An organization shall make readily available to individuals, specific information about its policies and practices relating to the management of personal information.*

This Privacy Policy is publicly available on the Amplify Care website: http://ehealthce.ca/

Amplify Care HINP Accountability Statement with Safeguards is available here.

## 9. INDIVIDUAL ACCESS

*Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.*

Any inquiries relating to the existence, use or disclosure of PHI by the Amplify Care or its agents, should be directed to the Privacy Office at Privacy@ehealthce.ca. Challenges to the accuracy and completeness of PI will be reviewed in the context of the role held by Amplify Care. Generally, individual access to, or correction of, PHI will be re-directed to the responsible HIC.

## 10. CHALLENGING COMPLIANCE

*An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization's compliance.*

Amplify Care has a Privacy/Security Breach protocol with respect to the privacy and security of PI. If a complaint pertains to one of our participants or other partners the sender of the complaint may be redirected to the relevant party. A complaint and/or feedback related to Amplify Care's privacy, data protection or information management practices, or Amplify Care's compliance with legislative or regulatory requirements may be submitted to:

Att'n: Privacy Office
Amplify Care

235 The Boardwalk, Suite 301
Kitchener, ON  N2N 0B1

Or by email to: privacy@amplifycare.com
***Please do not include PHI in the email to Amplify Care.***

A complaint may also be made to the Information Privacy Commissioner at:

Information Privacy Commissioner of Ontario
2 Bloor Street East, Suite 1400
Toronto, ON M4W 1A8

REFERENCE DOCUMENTS:

1. Personal Health Information Protection Act (PHIPA, 2004)
2. HINP Accountability Statement
3. Complaint Policy
4. Complaint/Incident Report Form