**Confidentiality & PHIPA Compliance Agreement**

Prepared For: [Enter your client name here]

Completed By: [enter your team name here]

**www.yourwebsite.com**

**Email: you@yourwebsite.com**

**Phone: your\_phone\_number**

**Add Your Company Logo/Name here**

**Add stock/company or document related Image here,**

*Once you add image, click on it got to “Picture format” and than from “Arrange” tab go to the “sent to back” and click sent to back option. Also make sure the wrap the image “behind text” is also checked. And manually position image.*

**Updated:**

**April 27, 2025**

**Table of Contents**

[Disclaimer 2](#_Toc194784608)

[How to Use This Document 2](#_Toc194784609)

[Introduction 3](#_Toc194784610)

[Purpose & Scope 3](#_Toc194784611)

[Confidentiality Obligations 3](#_Toc194784612)

[Protected Health Information (PHI) & PHIPA Compliance 3](#_Toc194784613)

[Authorized Access & Data Security 4](#_Toc194784614)

[Reporting & Breach Notification Procedures 4](#_Toc194784615)

[Non-Disclosure & Legal Consequences 4](#_Toc194784616)

[Acknowledgment & Agreement 5](#_Toc194784617)

[Final Notes 5](#_Toc194784618)

# Disclaimer

This **Confidentiality & PHIPA Compliance Agreement** is a **legal framework** for healthcare organizations to ensure compliance with **PHIPA (Personal Health Information Protection Act), and Ontario’s health data protection laws**. This document does **not** constitute legal advice and should be reviewed by an HR or legal expert before implementation.

Employers must ensure compliance with **Ontario’s Ministry of Health, OHSA, ESA, PHIPA, and industry-specific privacy regulations**.

# How to Use This Document

This document is a **binding confidentiality agreement** for healthcare employees, contractors, and vendors who handle patient information. Employers should:

* **Customize provisions** based on the clinic’s operations and legal requirements.
* **Ensure strict compliance** with **PHIPA, and other privacy regulations**.
* **Require all employees** to sign this agreement before accessing any patient data.
* **Educate employees** on their legal obligations related to patient confidentiality.
* **Regularly update** policies based on **changes in privacy and healthcare laws**.

# Introduction

At **[Healthcare Facility Name]**, maintaining the confidentiality of **Protected Health Information (PHI)** is of the highest priority. Employees, contractors, and third-party service providers must strictly adhere to **PHIPA, and internal data security policies**.

This **Confidentiality & PHIPA Compliance Agreement** ensures that all personnel understand their legal obligations to protect patient information, avoid unauthorized disclosures, and maintain compliance with healthcare industry standards.

# Purpose & Scope

This agreement applies to **all employees, contractors, vendors, and individuals** who have access to sensitive healthcare data at **[Healthcare Facility Name]**. The purpose of this document is to:

* Establish confidentiality expectations for handling patient information.
* Ensure compliance with federal and provincial health data privacy laws.
* Protect electronic and physical patient records from unauthorized access.
* Define legal consequences for confidentiality breaches.

# Confidentiality Obligations

Employees and authorized personnel must:

* Maintain strict confidentiality of patient records, conversations, and treatment details.
* Only access medical records necessary for job duties.
* Use secure systems and encrypted communication channels when handling patient data.
* Avoid discussing **PHI** in public areas, social media, or unauthorized locations.
* Comply with all internal security policies related to patient data protection.

# Protected Health Information (PHI) & Compliance

PHI includes but is not limited to:

* Patient names, addresses, and contact details
* Medical histories, diagnoses, and treatment plans
* Billing information and insurance details
* Any electronic or written health records

Under HIPAA and PHIPA:

* Employees must not share or disclose PHI unless authorized.
* Electronic PHI must be password-protected and encrypted.
* Paper-based PHI should be stored securely and disposed of properly.
* Employees must complete mandatory PHIPA compliance training.

# Authorized Access & Data Security

* Only authorized personnel may access electronic health records **(EHRs)** and patient data.
* Access must be limited to job-related functions.
* Employees must use secure passwords and multi-factor authentication **(MFA)**.
* Any printed PHI documents must be shredded after use.
* No PHI should be stored on personal devices.
* Unauthorized access or disclosure will result in disciplinary action, including termination.

# Reporting & Breach Notification Procedures

In case of a suspected **data breach, unauthorized access, or accidental disclosure**, employees must: Immediately report the incident to the designated Privacy Officer or Compliance Team.

* Provide a full written report of the breach details.
* Cooperate with internal investigations and regulatory reporting requirements.
* Follow necessary remediation steps as directed by compliance officers.
* Understand that failure to report breaches can result in legal penalties.

# Non-Disclosure & Legal Consequences

* Any **unauthorized disclosure** of PHI will be considered a serious violation of privacy laws.
* Legal consequences may include:
* **I**mmediate termination of employment.
* Legal prosecution under PHIPA laws.
* Financial penalties and fines imposed by regulatory bodies.
* Revocation of professional licenses for healthcare practitioners.
* Employees will remain bound by this confidentiality agreement even after leaving employment.

# Acknowledgment & Agreement

I, **[Employee Name]**, acknowledge that I have read, understood, and agree to comply with the **Confidentiality & PHIPA Compliance Agreement** of [Healthcare Facility Name]. I understand that protecting **patient privacy and PHI confidentiality** is a legal and ethical obligation. I also understand that **violations may result in termination, legal action, and financial penalties**.

**Employee Signature:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Date:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Privacy Officer/HR Representative Signature:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Date:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

# Final Notes

This agreement ensures that healthcare employees and contractors comply with data security and patient confidentiality laws. Employers should regularly review and update this document to align with changing regulatory requirements and best practices.

**Please delete the last page once you are done.**

****



**Contact Us:**

**Email:** [contact@prosupporthr.ca](mailto:contact@prosupporthr.ca)

**Phone:** 289-628-1484

**Website:** <https://prosupporthr.ca>

**Copyright © 2025 Prosupport HR Partners**

All rights reserved. Unauthorized reproduction or distribution of this template is prohibited