ShiftPilot

Privacy and Security Overview

How ShiftPilot handles the personal information customers place in the Service, meets its obligations under PHIPA and PIPEDA, and protects Customer Data.

Version	Effective	Classification	
1.0	November 16, 2026	Public	shiftpilot.com/security

Document control

Title	Privacy and Security Overview
Reference	SP-SEC-001
Version	1.0
Effective date	November 16, 2026
Classification	Public
Owner	Privacy Officer, ShiftPilot
Contact	info@shiftpilot.com
Review	Annually, and whenever the Privacy Policy or Terms of Service change
Governing documents	Privacy Policy, last updated November 15, 2026 (shiftpilot.com/privacy) Terms of Service, last updated October 24, 2026 (shiftpilot.com/terms)

Revision history

Version	Date	Description
1.0	November 16, 2026	Initial release.

Contents

1	Purpose and scope	4
2	Information processed	4
3	Personal Health Information Protection Act, 2004 (Ontario)	5
4	Personal Information Protection and Electronic Documents Act	5
5	Security controls	6
6	Business continuity and recovery	8
7	Security incident response	9
8	Retention and disposal	9
9	Assistant and AI processing	9
10	Data location and subprocessors	10
11	Documents available on request	11

1 Purpose and scope

1.1 Purpose

This document describes how ShiftPilot handles the personal information that customer organizations place in the Service, how ShiftPilot meets its obligations under the *Personal Health Information Protection Act, 2004* (Ontario) ("PHIPA") and the *Personal Information Protection and Electronic Documents Act* (Canada) ("PIPEDA"), and the administrative and technical controls that protect Customer Data. It is intended for the privacy, security and procurement staff who assess ShiftPilot on a customer's behalf.

1.2 Scope

This document covers the ShiftPilot service: the web application, the iOS, Android and macOS applications, the scheduling assistant ("Avery"), messaging and hospital-line features, and the infrastructure that supports them.

1.3 Definitions and references

"Service", "Customer Data" and "Security Incident" have the meanings given in the ShiftPilot Privacy Policy. References in the form "PP §5.1" are to sections of the Privacy Policy.

1.4 Precedence

This document summarizes commitments made in the Privacy Policy and the Terms of Service. If this document and either of those documents differ, the published Privacy Policy and Terms of Service govern.

2 Information processed

2.1 Workforce information

ShiftPilot is a staff scheduling service. The personal information it processes relates to the customer's own physicians, staff and administrators, and consists of:

a. identity and contact details: name, email address and mobile number;

b. professional details: credentials, site privileges and roles;

c. scheduling records: availability, leave, shift assignments, shift swaps, and the messages and notifications about them; and

d. operational information about the customer's sites, including aggregate workload figures such as case counts, which contain no patient identifiers (PP §8.3).

2.2 Patient information

The Service does not request patient information, none of its features require it, and it is not designed to store it. Customers agree in the Terms of Service not to enter patient information anywhere in the Service (PP §1.1). Where hospital staff contact a physician through a hospital line that ShiftPilot routes, patient identifiers are removed from transcripts before they are stored, and call and voicemail recordings are deleted after 30 days (PP §1.1, §7, §10).

3 Personal Health Information Protection Act, 2004 (Ontario)

3.1 Role of ShiftPilot

The customer remains accountable for the information it places in the Service and, where applicable, is the health information custodian. ShiftPilot acts as the customer's agent within the meaning of section 17 of PHIPA, and as an information manager, service provider or processor under comparable legislation, including the *Health Information Act* (Alberta), the *Health Information Privacy and Management Act* (Yukon) and the *Health Information Act* (Northwest Territories) (PP §8.1, §8.2).

3.2 Obligations

Requirement	ShiftPilot practice	Reference
Agent acts only for the custodian (s. 17)	Collects, uses and discloses information only to provide the Service and on the customer's instructions. ShiftPilot does not sell personal information, use it for advertising or use it to train machine-learning models.	PP §8.2
Safeguards (s. 12(1))	Encryption in transit and at rest, role-based access enforced on the server, audit logging, continuous monitoring and daily backups held outside the database provider. See section 5.	PP §5, §6
Notice of theft, loss or unauthorized use or disclosure (s. 12(2), s. 17(3))	Notice to the customer's designated contact without undue delay and within 72 hours of confirming a Security Incident, with the information the customer needs to notify affected individuals and the Information and Privacy Commissioner of Ontario. See section 7.	PP §5.5
Retention and secure disposal (s. 13)	Retained for the term of the subscription; after termination, kept for 90 days for export and deleted from production systems within a further 30 days. Backup copies expire after 90 days. See section 8.	PP §6.4, §7
Written agreement	ShiftPilot will execute an agent agreement, information manager agreement or data processing agreement on request.	PP §8.2
Storage outside Canada	Production data is stored in the United States. ShiftPilot provides the information a customer needs to determine whether this is permitted under the legislation that applies to it. See section 10.	PP §16

4 Personal Information Protection and Electronic Documents Act

ShiftPilot processes personal information as a service provider to the customer and follows the ten fair information principles set out in Schedule 1 to PIPEDA.

Principle	ShiftPilot practice	Reference
1. Accountability	A designated individual is accountable for compliance and can be reached at info@shiftpilot.com. Subprocessors are bound by written terms no less protective than the Privacy Policy.	PP §8.4, §10

Principle	ShiftPilot practice	Reference
2. Identifying purposes	The Privacy Policy states what is collected and why. Information is used to operate the customer's scheduling and related notifications.	PP §2, §3
3. Consent	Members are told what is collected. Members can stop text and WhatsApp messages by replying STOP and set their own notification preferences; administrators can turn off any channel or type of message. In the mobile app, assistant conversations are sent to the AI provider only after the member has expressly allowed it, and that permission can be withdrawn at any time.	PP §9, §13
4. Limiting collection	Only the information scheduling requires. No patient information.	PP §1.1, §8.3
5. Limiting use, disclosure and retention	Used only to provide the Service, disclosed only to the subprocessors listed in section 10, and retained as described in section 8.	PP §4, §7
6. Accuracy	Members and administrators maintain profiles, contact details and availability in the Service. Every change is recorded.	PP §5.3
7. Safeguards	See section 5.	PP §5
8. Openness	The Privacy Policy, Terms of Service and subprocessor list are public and dated. New subprocessors are announced at least 30 days in advance.	PP §10, §17
9. Individual access	Members can view their own information in the Service, request a copy or a correction, and delete their account.	PP §11
10. Challenging compliance	Individuals may challenge compliance with the accountable individual and, if not satisfied, complain to the Office of the Privacy Commissioner of Canada or to their provincial or territorial commissioner.	PP §8.4
Breach of security safeguards (s. 10.1)	Notice to the customer within 72 hours of confirming a Security Incident, with the information the customer needs to assess real risk of significant harm, report to the Commissioner and notify individuals.	PP §5.5

5 Security controls

5.1 Control summary

The table below sets out ShiftPilot's controls against the five Trust Services Criteria published by the American Institute of Certified Public Accountants (AICPA). Sections 5.2 to 5.8 describe them in more detail.

Criterion	Controls
Security	Encryption in transit (TLS 1.2 or higher) and at rest (AES-256). Passwords stored only as salted bcrypt hashes. Role-based access enforced on the server for every request, with each organization's data isolated from every other organization. Production access limited to named personnel and protected by multi-factor authentication.

Criterion	Controls
Availability	Every database write replicated across multiple availability zones. A full backup taken every 24 hours to a system separate from the database provider, verified automatically and retained for 90 days. Recovery point objective of 24 hours and recovery time objective of four hours for a full restoration. Immutable deployments that can be rolled back.
Processing integrity	Every schedule publication, import, generation and edit creates a version an administrator can restore. Every change to a shift is recorded with the person who made it, the time, and the state before and after.
Confidentiality	Customer Data used only to provide the Service. Every subprocessor bound by written confidentiality terms. Backups subject to the same encryption and access controls as production data.
Privacy	Sections 3, 4, 8 and 9 of this document, and the published Privacy Policy.

5.2 Infrastructure

The Service is hosted on Vercel, Inc. and Convex, Inc., the latter operating on Amazon Web Services. Each provider maintains a current SOC 2 Type II report and is bound by contractual confidentiality and security obligations to ShiftPilot. On request, ShiftPilot will obtain those reports for a customer under the providers' confidentiality terms (PP §5.4).

5.3 Encryption

Data in transit between devices and the Service, and between the Service and its infrastructure providers, is encrypted with TLS 1.2 or higher. Customer Data at rest, including database records, file storage, search indexes and backup copies, is encrypted with 256-bit AES. Account passwords are never stored in plain text; they are hashed with an adaptive, salted one-way algorithm (bcrypt) (PP §5.1).

5.4 Access control

Access within the Service is governed by role-based permissions assigned by the customer's administrators. Members see their own information and the information their organization chooses to share with them; administrative functions are restricted to designated administrators; hospital site logins see only the sites to which they are assigned. Every request to the backend is authenticated and scoped to the requesting user's organization (PP §5.2).

Access by ShiftPilot personnel to production systems is limited to named individuals who need it to operate and support the Service, is protected by multi-factor authentication at the infrastructure-provider level, and is used only as needed to provide the Service, resolve an incident or meet a legal obligation (PP §5.2).

5.5 Audit logging

Changes to schedules, assignments, user roles and organization settings are recorded in an audit log that identifies the person, the time and the change, and that log is available to the customer's administrators in the Service. Each change to a shift also records its source (the schedule board, the assistant, the mobile app or a spreadsheet sync) and the shift before and after. Every email, text and WhatsApp message the Service sends is logged with its delivery outcome (PP §5.3).

5.6 Monitoring

Application errors and security-relevant events are monitored continuously and reviewed by ShiftPilot's engineering team. On the web, session replays used for error diagnosis mask all on-screen text; the mobile app records no replay (PP §5.3, §10).

5.7 Change management

All application code is held in version control with full history. Automated tests covering organization isolation and access checks run before release. Every production deployment is immutable and can be rolled back to any earlier deployment (PP §6.1).

5.8 Integrations

Inbound phone and text webhooks are accepted only with a valid signature from the carrier. Google and Microsoft calendar and spreadsheet integrations operate only where the customer or user has connected them, and only with the permissions approved when they are connected (PP §10).

6 Business continuity and recovery

Layer	Practice
Replication	Every write to the production database is replicated across multiple availability zones before it is acknowledged. A single hardware or zone failure does not cause data loss.
Daily backups	A complete export of every production table is taken every 24 hours and stored, encrypted at rest, in a system separate from both the production database and the database provider. Each export is verified automatically and retained for 90 days.
Schedule version history	Every publication, import, generation or manual edit of a schedule creates a point-in-time version, retained for the life of the account and restorable by an administrator without engineering involvement.
Recovery objectives	Full restoration from a daily backup: recovery point objective of 24 hours and recovery time objective of four hours from the decision to restore. Restoration of a schedule from version history: minutes, with no loss beyond the change being reversed.
Testing	A daily backup is restored into a non-production environment at least once every six months, and the outcome is recorded.
Customer export	Administrators can export schedules in spreadsheet form at any time and can request a complete machine-readable export of their organization's data.

Reference: PP §6.1 to §6.5.

7 Security incident response

If ShiftPilot becomes aware of unauthorized access to, or loss, theft or unauthorized use or disclosure of, Customer Data in its custody or control, ShiftPilot will:

a. notify the customer's designated contact without undue delay, and in any event within 72 hours of confirming the Security Incident;
b. provide the information the customer reasonably requires to meet its own obligations to notify affected individuals and the Information and Privacy Commissioner of Ontario or other applicable regulator; and
c. take reasonable steps to contain, investigate and remediate the Security Incident.

A shorter notification period required by law or by a written agreement with the customer takes precedence (PP §5.5).

8 Retention and disposal

Information	Retention
Accounts and profiles	For the term of the customer's subscription.
Schedules, availability, version history and audit logs	For the term of the subscription, as the customer's operational record.
Notification and message logs	For the term of the subscription, to support delivery verification.
Hospital-line recordings	Deleted after 30 days. Redacted transcripts follow the message logs.
After termination	Retained for 90 days so the customer can export it, then deleted from production systems within a further 30 days. A customer may request earlier deletion in writing.
Backup copies	Expire 90 days after they are taken, after which deleted data is unrecoverable.

Reference: PP §6.4, §7.

9 Assistant and AI processing

The Service includes a scheduling assistant, Avery, reached through the web application, the mobile app, SMS and WhatsApp. When a user writes to the assistant, the message and the scheduling information needed to answer it are sent to OpenAI, directly or through the Vercel AI gateway (PP §9). The following terms apply:

a. OpenAI does not use content sent through its API to train its models, and deletes conversation state and safety logs after no more than 30 days;

b. ShiftPilot does not use assistant conversations to train AI models;
c. a change the assistant proposes to a schedule, availability record or setting takes effect only after the user expressly confirms it;
d. in the mobile app, the assistant runs only after the user has allowed their conversations to be sent to the AI provider, and the user can withdraw that permission at any time;
e. the customer can turn the assistant off for its organization, for a channel or for individual users; and
f. the assistant has no access to patient information and gives no medical advice.

10 Data location and subprocessors

Production data is stored in data centres in the United States. Each subprocessor is bound by written terms that require it to protect the information to a standard no less protective than the Privacy Policy, and to use it only to provide its service to ShiftPilot. Customers receive at least 30 days' notice before a new subprocessor is engaged (PP §10, §16).

Subprocessor	Purpose
Vercel, Inc.	Application hosting, file storage, AI gateway, isolated sandboxes for the assistant's calculations
Convex, Inc. (on Amazon Web Services)	Primary database, file storage, scheduled functions
Railway Corporation	Schedule generation; the assistant's voice gateway
Upstash, Inc.	Short-lived caching
GitHub, Inc.	Source code; encrypted storage of daily backups
Twilio Inc.	SMS and WhatsApp delivery; hospital phone lines where enabled
Resend, Inc.	Email delivery
650 Industries, Inc. (Expo)	Mobile push notifications and app updates
OpenAI, L.L.C.	Assistant language model, document search and voice; call transcription where enabled
Anthropic, PBC	Review of assistant conversations to find and correct errors
Google LLC; Microsoft Corporation	Spreadsheet, drive and calendar integrations, only where connected
Functional Software, Inc. (Sentry)	Application error monitoring
PostHog, Inc.	Usage statistics; no session recording
Telnyx LLC	Hospital fax lines, where enabled
Mango Technologies, Inc. (ClickUp)	Support requests and product feedback

11 Documents available on request

a. An executed PHIPA agent agreement, information manager agreement or data processing agreement.
b. The SOC 2 Type II reports of ShiftPilot's hosting providers, obtained under their confidentiality terms.
c. A complete machine-readable export of the customer's data.
d. The information a customer needs to assess storage of its data outside Canada.

Requests and questions about this document: **info@shiftpilot.com**.

ShiftPilot · Privacy and Security Overview · SP-SEC-001 · Version 1.0 · Effective November 16, 2026. This document summarizes the ShiftPilot Privacy Policy and Terms of Service, which govern if they differ. The current version is published at shiftpilot.com/security.