



PRIVACY POLICY

NYZR Technologies Inc.

Version 7.0 • August 2026

Document Control

Field	Value
Document type	Public Privacy Policy for the NYR website, mobile application and related Platform functions
Legal entity	NYR Technologies Inc. (referred to as “NYR”, “we”, “us” and “our” in this Policy)
Registered office	375 University Avenue, Suite 3232, Toronto, ON M5G 2J5
Version	7.0
Last updated	August 2026
Current launch scope	Ontario-only private-pay marketplace for enabled Services provided by independent RNs, RPNs, NPs, RMTs and PSWs
Compliance framework	PIPEDA; PHIPA and O. Reg. 329/04 where applicable; and applicable profession-specific privacy and Professional Record requirements
Related notices	Booking-specific notices, location notice, Cookie and Tracking Notice, and other just-in-time notices where applicable
Contact	privacy@nyrapp.com

1. Scope and Application

- (a) This Privacy Policy explains how NYR Technologies Inc. collects, uses, discloses, retains and protects personal information when individuals visit the NYR website, use the NYR mobile application or related Platform functions, request or receive Services, assist another person with a Booking, apply or register to provide Services through NYR, or otherwise interact with NYR. It is NYR’s principal public privacy policy for the website, mobile application and related Platform functions.
- (b) NYR’s current proposed launch model is an Ontario-only, private-pay marketplace that connects Clients and Care Recipients with independent RNs, RPNs, NPs, RMTs and PSWs for Services enabled through the Platform. This Policy is written for that launch model. NYR will review and update this Policy before enabling a materially different Service, jurisdiction, public-funding arrangement, insurer integration, institutional or facility model, or other change that materially affects NYR’s privacy roles or information practices.
- (c) Additional short-form or contextual notices may be provided when personal information is collected or when a particular feature is enabled. These may include notices concerning Booking-specific collections, identity verification, Worker screening or monitoring, location or visit-status information, cookies or analytics, marketing consent, device permissions, or any

recording, transcription or AI-assisted feature. Those notices supplement this Policy and explain the relevant information practice in context.

- (d) This Policy describes NYR’s public information practices. It does not replace the Client Terms, Worker Terms, Independent Worker Agreement, Accepted Booking Disclosure or other agreement governing use of the Platform, and it does not by itself create treatment consent, Representative authority or another consent or lawful authority required for a particular activity.

2. How Privacy Roles Work

NYR’s legal role depends on the particular record, purpose, function, Service and event. Information stored or transmitted through the same Platform or technical environment does not necessarily belong to the same legal category or become available to every person or for every purpose.

- NYR acts independently for its own website, account, matching, marketplace, payment, verification, support, complaint, safety, security, fraud, tax, marketing, legal and compliance records.
- A Worker may be a Health Information Custodian (“HIC”) under the Personal Health Information Protection Act, 2004 (“PHIPA”) for a Professional Record, may act as another HIC’s agent or may occupy another lawful role. The Worker’s role depends on the Worker’s profession, practice relationship, the particular record and purpose, the applicable authority, and who has custody or control. The role of a PSW and the status of a PSW Professional Record are determined under the applicable facts and law.
- For defined Professional Record functions, NYR may act as an agent, electronic service provider, technology provider or other service provider for a Worker, HIC or other responsible record holder. The precise role depends on the applicable authorization, configured function, purpose, custody or control and legal relationship. Hosting, storing, transmitting or administering access to information does not by itself make NYR the HIC or transfer custody or control of a Professional Record to NYR.
- A Booking, Service or incident may generate separate Client- or Care Recipient-supplied information, Worker- or HIC-controlled Professional Records, and NYR administrative, matching, verification, payment, complaint, safety, security, fraud, tax, technical, legal and compliance records. Their source, authorship, custody or control, purpose, legal role and lawful access route must remain distinguishable.

A request may concern information controlled by NYR, a Professional Record controlled by a Worker, HIC or other record holder, or both. NYR may authenticate the requester, verify the asserted authority and purpose, coordinate the routing, and assist within NYR’s role. Routing a request does not determine the requester’s entitlement or the substantive outcome. The responsible Worker, HIC or other record holder remains responsible for decisions within that person’s role, and NYR remains responsible for records and decisions within its own control.

3. Privacy Officer and Complaints

- (a) NYJR has designated a Privacy Officer to oversee NYJR's privacy-management program and receive privacy questions, complaints, access or correction requests, consent-withdrawal requests and reports of suspected privacy incidents. Contact the Privacy Officer at privacy@nyjrapp.com.
- (b) NYJR will address a request or complaint within its legal role. Where the matter concerns a Professional Record or decision controlled by a Worker, Health Information Custodian or other responsible record holder, NYJR may authenticate the requester, verify the asserted authority and purpose, and route or coordinate the matter with the responsible person.

4. Information We Collect

A) Website, account and identity information

We may collect your name, contact information, login credentials, address, language and communication preferences, account role, authentication and recovery information, and evidence of acceptance of applicable terms or notices. We collect only the identity attributes reasonably needed for the relevant transaction. At launch, NYJR requires identity verification for each Client Account Holder and Worker and uses Stripe Identity as the standard verification method, including government-issued identification, selfie matching and live capture, subject to any accessible or legally required alternative.

B) Booking and care-recipient information

Clients may optionally provide and maintain general medical information in their profile. This information may be provided during account setup or later, updated by the Client and reused for future Bookings.

Booking-specific forms may collect the requested Service, care address, date and time, information needed for the Worker to evaluate and prepare for the Booking, medications, allergies, relevant conditions, mobility or communication needs, household hazards, accommodation requirements, and other information reasonably necessary for the requested Service or safety.

We identify who supplied the information and whether that person is the Care Recipient, an Account Holder, a person merely assisting with the Booking or a person asserting legal authority. A Client may also provide and maintain general medical information for a saved person who does not hold a NYJR account, where the Client has that person's consent or other lawful authority to provide the information. This information may contain Personal Health Information and may be protected using an optional PIN feature within the NYJR app.

NYJR does not request or intentionally collect Ontario health-card numbers or health-card images for its launch private-pay Services, does not use them for identity verification, does not transmit them to payment providers and does not process OHIP claims. If health-card information is received accidentally, NYJR will restrict access and take appropriate steps to securely delete it unless retention is required or permitted by applicable law, subject to applicable security and evidence-preservation requirements.

C) Representative and authority information

Where someone acts for another person, we may collect the asserted relationship, authority type, scope, verification status, restrictions, effective and expiry dates, and supporting evidence where reasonably necessary. Account ownership, payment, family relationship or assistance with a Booking does not automatically establish authority to access health information or make treatment decisions.

D) Worker, applicant and professional information

For Workers and applicants, we may collect contact and identity information, education, work history, licences, registrations, certifications, insurance information, public-register information, Service eligibility, banking and tax information, availability, Booking and earnings records, complaints, incidents, internal feedback, monitoring records and other onboarding or compliance information.

Where background screening is enabled, we first determine the appropriate legal category and collect the least detailed result reasonably necessary. A police record check, vulnerable sector check, commercial background report, credential-register verification, identity check and vendor-generated fraud signal are not treated as interchangeable. We may retain only confirmation, a limited result category or a completion date rather than the full report where that is sufficient.

E) Professional records and care documentation

Workers may create Professional Records through the Platform in connection with enabled Services and configured workflows, including assessments, care notes, visit summaries, consent records, instructions, incident documentation and follow-up records. These records may be controlled by the Worker or another HIC. Workers do not retain direct in-app access to Professional Records after submission. NYJR collects or hosts only the information required for the configured function and keeps professional entries distinguishable from NYJR administrative notes and system-generated metadata.

F) Payments, payouts and tax information

We and our payment providers may collect payment-method details, billing address, transaction amounts, Platform fees, taxes, refunds, credits, cancellation charges, payout and bank information, tax identifiers and receipt or invoice information. NYJR does not store complete payment-card numbers. NYJR configures payment, payout and tax records to exclude clinical details and other Personal Health Information that is not reasonably necessary for the transaction.

G) Location, device and technical information

We may collect IP address, device and app identifiers, operating-system and browser information, authentication and session events, push-notification tokens, security logs, crash or diagnostic information, permissions and settings, and other technical data needed to operate and secure the website and app. When a Worker has activated the Platform's "Available" status for matching, and during active Bookings, we may process Worker location, arrival, departure or routing information as described in Section 11.

H) Communications, complaints, safety and legal records

We collect messages sent through the Platform or to our support channels, call or contact records where applicable, complaints, refund requests, safety reports, suspected fraud, account restrictions, legal demands, regulatory communications and evidence needed to investigate and resolve those matters. We separate allegations from findings and restrict sensitive complaint and safeguarding information to those who need it.

I) Public and third-party sources

We may verify professional status and other limited information through official public registers or other lawful sources. We use that information for purposes reasonably related to professional eligibility, verification, safety, compliance or another reason for which the information was lawfully obtained. We do not use public-register information for unrelated profiling, advertising or sale.

5. Why We Use Information

We use personal information only for identified, appropriate and authorized purposes, including to:

- operate, secure and support the website, app, accounts and authentication processes;
- create, present, accept, manage, complete, cancel and document Bookings;
- match eligible Workers with requested Services without using prohibited discriminatory preferences;
- verify identity, representative authority, professional status, credentials and service eligibility;
- make Booking-specific information available to a Worker considering or accepting the Booking on a minimum-necessary basis;
- support professional documentation, access, correction and lawful continuity functions;
- process payments, payouts, taxes, invoices, receipts, refunds, disputes and chargebacks;
- send Booking, account, safety and other service communications;
- provide accessible service, accommodation and support;
- protect users and Workers, investigate complaints or incidents, prevent fraud and enforce Platform rules;

- comply with legal, regulatory, professional, tax, public-health, child-protection, court and law-enforcement obligations;
- maintain audit evidence, legal holds and records reasonably required for Platform administration and business continuity; and
- improve the Platform using information that NYJR is legally entitled to use for that purpose, subject to the restrictions in Section 12.

6. Consent, Authority and Choices

This Policy is a notice; accepting it is not a substitute for every consent or legal authority required for a particular activity. NYJR separates contractual acceptance, privacy consent, authority to act for another person, consent to treatment, marketing consent and device or software permissions.

- Contractual acceptance of the Client Terms, Worker Terms or another agreement does not itself constitute consent to treatment or prove authority over another person's information.
- Where PIPEDA applies, we obtain meaningful consent when consent is required and identify the important purposes, information and third parties before or at the time of collection.
- Where PHIPA applies, consent or another lawful authority must relate to the specific collection, use or disclosure. A Worker or HIC remains responsible for professional and treatment-consent decisions within that person's role.
- The Worker obtains or verifies, and documents where required, the consent or other authority required for the Service within the Worker's professional or service role. App acceptance or Booking confirmation is not consent to treatment, consent to a personal-assistance Service or another authority required for the Service, and does not replace any consent required by applicable law or professional requirements for a particular treatment or Service. NYJR does not require a separate signed NYJR consent form solely because a Booking is made through the Platform.
- Marketing consent and any consent required for non-essential cookies, tracking, recordings, software installation or future AI functionality are handled separately where applicable.

You may withdraw consent for future processing where the law permits. Withdrawal does not invalidate processing already completed lawfully and may not require deletion of records that must be retained for professional, tax, complaint, safety, legal-hold or other lawful purposes. Some information is necessary to create an account, complete a requested Booking, process payment, maintain security or meet legal obligations; declining that information may prevent the relevant function.

The law may permit or require collection, use or disclosure without consent in limited circumstances, including emergencies, fraud prevention, investigations, legal proceedings, mandatory reporting, public health, child protection and other statutory duties.

7. How We Share Information

We disclose personal information only for identified purposes, with consent or other lawful authority, and on a minimum-necessary basis. Recipients may include:

- the Worker considering or accepting a Booking, where authorized and reasonably necessary for the applicable Booking state;
- the Care Recipient, Account Holder or verified Representative, within the person's established authority;
- payment, hosting, communications, mapping, identity-verification, security and other service providers described below;
- another Worker or HIC where a lawful continuity, referral or other professional-record disclosure process applies;
- professional regulators, public-health authorities, children's aid societies, courts, law enforcement, government bodies or other recipients where disclosure is required or permitted by law;
- insurers or benefit-plan administrators, in relation to Client or Care Recipient information, only if a separately approved workflow and lawful authority permit disclosure; NYJR does not submit claims or guarantee reimbursement;
- with the Worker's consent, provider directories maintained by or associated with insurers or benefit plans may receive the Worker's professional name, designation and licence or registration number for purposes of supporting Client reimbursement;
- a prospective or completed business transaction where permitted by law and subject to appropriate safeguards.

NYJR does not sell personal information. We do not use Personal Health Information for targeted advertising, place it in ordinary payment metadata or marketing tools, or disclose it to other Workers who are not assigned and authorized for the Booking.

NYJR does not use booking health information or professional records to create advertising audiences, look-alike audiences, behavioural advertising profiles or advertising-conversion events, and does not disclose those records to advertising platforms to target promotions based on health, disability, care needs or use of healthcare services.

8. Service Providers and Cross-Border Processing

NYJR uses service providers to operate the website and app. The table below identifies material providers that may receive personal information or Personal Health Information as part of NYJR's current configuration. We limit each provider's access to the information reasonably required for its service and use safeguards appropriate to the information and service. A provider may also have limited independent obligations or purposes disclosed in its own terms or privacy notice.

Service provider	Purpose and typical information	Primary processing location
Stripe	Payment processing; identity verification; Worker payouts; transaction and tax records. May receive identity data submitted for verification, payment and payout details, transaction data and limited address or jurisdiction data. NYYR configures payment and tax metadata to exclude clinical details and health-card information that are not reasonably necessary for the transaction.	Canada and United States, depending on service
Supabase	Primary Platform database, authentication and storage. May process information stored in the Platform, including Personal Health Information, subject to NYYR's configured access controls.	Canada region for primary hosting; provider support and subprocessors may operate elsewhere
Resend	Transactional email delivery. Receives recipient address and message content. Templates and payloads are designed to minimize sensitive information.	United States
Expo / 650 Industries	Mobile build and push-notification infrastructure. May process app-build data, push tokens and notification payloads; payloads are designed to exclude Personal Health Information.	United States
Apple	iOS app distribution, device push delivery and app-store metrics.	Canada, United States and other provider locations
Google	Android app distribution, device push delivery, app-store metrics and related mobile services.	Canada, United States and other provider locations
Twilio	Phone-number verification by SMS or voice call	United States and other provider locations, depending on service and configuration
Google Maps Platform	Address geocoding, map display and routing. NYYR may send a care address and, where live tracking is used, origin and destination coordinates, including the Worker's current location and the Care Recipient's care location.	United States and other provider locations
OpenStreetMap	Map tiles used in NYYR's administrative live-operations map. May process technical request information associated with delivery of map content, depending on configuration.	Global, through distributed content-delivery and cache infrastructure.

Service provider	Purpose and typical information	Primary processing location
unpkg	Content delivery service used to load the Leaflet mapping library for NYYR's administrative live-operations map. May process technical request information associated with delivery of library assets, depending on configuration.	Global, through content-delivery infrastructure

Some providers process information outside Canada, including in the United States, where information may be subject to the laws and lawful-access regimes of that jurisdiction. Contractual safeguards cannot prevent a foreign authority from exercising valid legal powers. NYYR uses contractual or other appropriate safeguards when engaging service providers and remains accountable for personal information under its control, in accordance with applicable law.

The provider list and configurations may change. NYYR will update this Policy or provide another appropriate notice where a change materially affects the purposes, categories, locations or risks described here.

9. Payments, Identity Verification and Insurance Boundary

- (a) Stripe processes payment cards and other payment information. NYYR receives transaction confirmations and other information needed to administer the Booking, but does not store complete card numbers. Stripe Connect may process Worker identity, bank and payout information. NYYR uses Stripe Identity to verify identity using government-issued identification, selfie matching and live capture. NYYR does not retain the submitted identity document or selfie in its own Platform records and retains only the Stripe Identity verification identifier and verification date, subject to any information required for security, dispute or legal purposes.
- (b) Before identity verification, the user receives a contextual notice describing the provider, information requested, purposes, principal uses and disclosures, whether the information is required, applicable retention or deletion practices and any available accessible or alternative verification method, and any consent required by applicable law is obtained. We do not use health-card information for payment or identity verification. NYYR does not sell, arrange or advise on insurance; obtain insurer portal credentials; adjudicate coverage; submit claims; receive insurer claim decisions or clinical requests; or guarantee reimbursement.

10. Communications, Cookies and Tracking Technologies

- (a) We send account, Booking, safety, payment and other transactional communications through the app, email, SMS or another enabled channel. A message is classified by its actual content. If it contains a promotion, referral incentive, discount, upsell or other commercial content, we apply Canada's Anti-Spam Legislation requirements, including express consent, implied consent,

or a statutory exclusion or exemption, as applicable, and required sender identification and unsubscribe controls.

- (b) Marketing communications are sent only where permitted. Marketing consent and unsubscribe status are handled separately from privacy consent and agreement acceptance.
- (c) The website may use strictly necessary cookies or similar technologies for security, sessions, preferences and accessibility. The mobile application may use device identifiers, push tokens, app permissions, crash or diagnostic tools, mobile SDKs and other technical services required to operate and secure the app. Non-essential analytics, advertising pixels, session replay, cross-context tracking, mobile analytics SDKs or comparable tracking will not be enabled without an appropriate notice and consent mechanism where required. Additional details, including material cookies, SDKs, permissions and tracking technologies, will be provided in NYJR's Cookie and Tracking Notice or another contextual notice.

11. Location and Worker Monitoring

- (a) Where enabled, Worker location may be collected when the Worker activates the Platform's "Available" status to support matching with Bookings within the applicable service radius. For an accepted Booking, Worker location may also be collected after the Worker starts the relevant travel, arrival or Service status so that the Booking can be coordinated and appropriate visit progress can be provided. NYJR does not collect continuous Worker location outside an Available-status matching, Booking or safety-related workflow.
- (b) A Worker's precise location is not shown to Clients. Clients may be shown ETA and distance. For an accepted Booking, route and location information may be available to authorized NYJR personnel for safety, security, Booking administration, complaints, disputes and compliance purposes.
- (c) The live location stream ends when the relevant matching, Booking or safety-related state ends. Limited arrival, departure, routing or location-event history may be retained where reasonably necessary for safety, complaints, disputes, fraud prevention, payment, security, compliance or legal purposes. NYJR may retain location records for up to two years where reasonably necessary for those purposes, with access restricted accordingly.
- (d) Location, routing and visit-status information shown to Clients or sent in notifications is limited to what is reasonably necessary for Booking coordination and safety and does not include clinical details, protected-ground information or unnecessary household or safety notes.
- (e) NYJR may process Booking activity, communications metadata, response times, internal feedback, location events and fraud or security signals for legitimate and proportionate Platform-operation, safety, eligibility, complaint, dispute-resolution and compliance purposes. Monitoring is not used to infer protected characteristics or to make a final material adverse Worker decision concerning Platform eligibility, suspension, deactivation or professional fault solely through automated processing.

12. Analytics and Artificial Intelligence

- (a) NYZR may use aggregate information or de-identified information for security, performance, service quality and product improvement only where NYZR is legally entitled to use the source information for that purpose. De-identified information is subject to safeguards designed to prevent reasonably foreseeable re-identification, and aggregate reporting must not reveal information about an identifiable individual or a small group in a way that could reasonably identify a person.
- (b) At launch, NYZR does not use Personal Health Information, whether controlled by NYZR, a Worker or another HIC, to train general-purpose or independent NYZR artificial-intelligence or machine-learning models. We do not place Personal Health Information in advertising, ordinary analytics, public ratings, payment metadata or routine support tools.
- (c) Where available, NYZR offers on-device voice dictation to help users complete certain fields. The feature is designed to process speech locally on the user's device rather than send spoken clinical responses to an online speech-recognition service, and is unavailable on devices that do not support local recognition.
- (d) Other than the on-device voice dictation described above, any future ambient recording, transcription, AI-assisted documentation, model training, automated clinical functionality or materially new secondary use requires appropriate review, authority, consent, notice and safeguards before activation.
- (e) At launch, NYZR does not make a final material adverse Worker decision concerning Platform eligibility, suspension, deactivation or professional fault, or an undisclosed final material adverse Client decision, solely through automated processing. Where automated systems assist a consequential decision, NYZR will provide an appropriate correction or human-review route. This does not prevent proportionate low-discretion technical blocks or the immediate imposition of urgent temporary restrictions, which are reviewed promptly.

13. Retention and Deletion

NYZR retains personal information only for as long as reasonably necessary for the purposes for which it was collected, to satisfy applicable professional, tax, payment, complaint, safety, security, legal and regulatory requirements, and to preserve information subject to a legal hold.

Record category	Retention approach
Accounts and non-medical profile information	Retained while the account is active and for a period after closure where reasonably needed for security, disputes, legal obligations or account administration. Information no longer required is deleted or anonymized in accordance with NYZR's retention practices.

Record category	Retention approach
Booking intake and questionnaires	If incorporated into or relied upon as part of a Professional Record, retention follows the requirements applicable to the responsible Worker, HIC, profession and record. Cancelled, unaccepted, abandoned or incomplete intake may follow a shorter purpose-based period, subject to safety, fraud, complaint, payment and legal-hold requirements.
Professional records	Retained according to the responsible Worker or HIC, profession, record type, Service date, age of the Care Recipient and applicable legal requirements. Where NYYR hosts or supports a Professional Record, NYYR acts within its applicable role and does not replace the responsible record holder's obligations.
Worker credentials and status verification	Retained while reasonably needed to verify current eligibility and for a period after deactivation where required to document historical Service-date status, complaints, incidents, transactions or legal obligations.
Background-screening information	NYYR seeks to retain only the level of detail reasonably necessary for the applicable screening purpose. Information is deleted when no longer required, subject to lawful retention needs and legal holds.
Payment, payout, tax and receipt records	Retained for applicable tax, accounting, payment-dispute, chargeback and legal periods. Clinical details are excluded unless reasonably necessary and lawfully permitted.
Complaints, incidents, legal and regulatory records	Retained for the period reasonably required to investigate, respond, protect safety, satisfy legal or professional obligations and preserve relevant evidence. Legal holds override ordinary deletion.
Location and monitoring records	Live tracking ends with the relevant matching, Booking or safety-related state. Limited location or monitoring information may be retained where reasonably necessary for safety, complaints, disputes, fraud prevention, payment, security, compliance or legal purposes.
Security and breach records	Retained for applicable security, investigation, notification, legal and regulatory purposes, including any minimum period required by law.
Backups, replicas and vendor copies	Information may remain temporarily in secure backups, replicas or service-provider systems until ordinary deletion or expiry processes are completed. Account closure or a deletion request may not result in immediate deletion from every backup or system copy.

At the end of the applicable retention period, information is deleted, destroyed, de-identified or anonymized, subject to lawful retention requirements, technical limitations, secure backup expiry and legal holds. An account-closure or deletion request does not require deletion of a Professional Record or other information that a HIC, NYYR or another responsible record holder must retain for professional, tax, payment, complaint, safety, fraud, security, legal or regulatory purposes. Where required, corrections to Professional Records preserve the original entry and appropriate correction history.

14. Security

- (a) NYJR uses administrative, technical and physical safeguards appropriate to the sensitivity, amount, format and use of the information. Safeguards are reviewed as the Platform, service providers, threats and legal requirements change.
- (b) These safeguards may include access controls, authentication measures, encryption, logging, secure development and configuration practices, service-provider safeguards, confidentiality obligations, training, incident-response procedures, backups and continuity measures.
- (c) No system is completely secure. Users should protect their credentials, use available security features and contact us promptly at privacy@nyjrapp.com if they suspect unauthorized access.

15. Privacy and Security Incidents

- (a) NYJR investigates suspected unauthorized access, use, disclosure, loss, theft or other compromise and determines the affected information, legal role, responsible HIC or organization, risk, required containment and notification route.
- (b) Where NYJR acts as an agent or technology or service provider in relation to records for which a Worker or HIC is responsible, NYJR notifies and supports the responsible Worker or HIC in accordance with applicable law and agreement so that the responsible person can assess and carry out any PHIPA duties that attach to that person's custody or control of the record. Where NYJR has custody or control of the affected information, acts independently for the affected Platform record or purpose, or is otherwise directly responsible under PIPEDA, PHIPA or another law, NYJR assesses and completes its own reporting, individual-notification and breach-record obligations.
- (c) Incident notices are provided through an appropriate channel and include the information required by law. NYJR maintains incident records as required by applicable law.

16. Access, Correction, Account Closure and Other Requests

- (a) You may request access to, or correction of, personal information that NYJR controls, subject to identity verification, legal exceptions and the rights of other individuals. A request may concern NYJR-controlled information, a Worker- or HIC-controlled Professional Record, or both, and a mixed request may require coordinated responses. Where the request concerns a Professional Record controlled by a Worker or HIC, NYJR may route the request to that person and support the response within its role rather than decide it independently. Routing does not determine whether the request will be granted or refused.
- (b) A correction request may be addressed through an amendment, notation, linked statement or another legally appropriate method. Professional opinions or observations are not necessarily

replaced merely because they are disputed, and the original entry and correction history may need to be preserved.

- (c) You may request account closure and deletion of information that NYJR is not required or permitted to retain. Closure does not automatically delete Professional Records, transaction records, legal holds, complaint evidence, security logs or backups that remain subject to applicable retention requirements.
- (d) You may withdraw consent for future processing or change optional communication and marketing choices where applicable. Other rights may apply depending on the information and law involved. We normally respond to a formal access or correction request within 30 days or within any extension or different period permitted or required by law.
- (e) To make a request, email privacy@nyjrapp.com. We may ask for information reasonably necessary to authenticate you and confirm your authority. We do not require more identification than is proportionate to the request.

17. Care Recipients Under 18, Capacity and Representatives

- (a) NYJR accounts are intended for adults. An adult may assist a child or another person with a Booking, but assistance, parenthood, family relationship or payment does not automatically establish authority for every privacy or treatment decision.
- (b) Capacity is specific to the information, treatment or decision and is not determined by age alone. A capable Care Recipient, including a capable minor, may make the relevant decision, subject to applicable law. If the person is incapable for that decision, the applicable substitute decision-maker may act within the scope and priority established by law. A person booking for someone else must certify that they have authorization or legal authority to do so. NYJR generally does not require documentary proof at the time of Booking, but will require appropriate evidence where a Power of Attorney for Personal Care or court-appointed guardian is relied upon, and may request other information reasonably necessary to confirm asserted authority. Capacity and consent decisions relating to a Service remain the responsibility of the Worker within the Worker's professional or service role.
- (c) Authority held during a person's lifetime may end or change upon death. A former attorney, payer, Account Holder or family member does not automatically have authority to access a deceased person's information, and NYJR may require evidence of estate or other lawful authority.
- (d) Retention of Professional Records depends on the responsible profession, HIC, record type and applicable legal requirements. Professional Records associated with completed Bookings are generally retained for at least ten years after the applicable last visit, end of the care relationship or other required retention trigger and, where applicable for a minor, until at least ten years after the Care Recipient reaches or would have reached age 18. The general medical profile

associated with a Client account may be retained while there is Booking activity and for up to ten years after the last Booking activity, subject to earlier deletion or de-identification where the information is no longer reasonably necessary. Information from the profile that is incorporated into a Professional Record is retained as part of that Professional Record in accordance with the retention period applicable to that record.

18. Accessibility

NYR provides or arranges accessible ways to create or recover an account, receive information, communicate with support and make privacy requests where reasonably required. We do not treat inability to complete a digital step because of disability as abandonment, refusal or non-cooperation without offering a suitable alternative. To request an accessible format or communication support, contact support@nyrapp.com.

19. Changes to This Policy

We may update this Policy to reflect changes in our services, technology, vendors, legal roles or requirements. The current version and effective date will be posted on the website and made available through the app.

We will provide appropriate advance or contextual notice of a material change. We will obtain any consent or other authority required by applicable law before activating a materially new collection, use or disclosure.

20. Contact

For privacy questions, access or correction requests, consent-withdrawal requests, account-closure requests or complaints:

Privacy Officer: privacy@nyrapp.com

General support: info@nyrapp.com

NYR Technologies Inc.
375 University Avenue, Suite 3232, Toronto, ON, M5G 2J5, Canada.

Privacy regulators:

Office of the Privacy Commissioner of Canada — www.priv.gc.ca
Information and Privacy Commissioner of Ontario — www.ipc.on.ca