PRIVACY POLICY
SERELORA INC.

Last Updated: January 30, 2026

This Privacy Policy for **Serelora Inc.** ("**Serelora**," "**Company**," "**we**," "**us**," or "**our**"), a Delaware corporation incorporated on January 19, 2026, with its principal place of business at 1111B S Governors Ave #99442, Dover, DE 19904, USA, describes how and why we might access, collect, store, use, and/or share ("**process**") your personal information when you use our services (collectively, the "**Services**").

We maintain the official version of this policy in English and make translations available for your convenience.

OUR COMMITMENTS TO YOU

We do not sell or license your information. Serelora does not sell, rent, trade, or otherwise transfer your personal information or protected health information to third parties for monetary or other valuable consideration.

We do not use your health data for advertising. Your clinical information is never used to target advertisements or shared with ad networks.

Human approval is required for clinical actions. AI-generated suggestions, risk assessments, and care recommendations are informational only. No clinical or administrative action is executed without explicit human authorization.

Every AI output is traceable. All AI-generated content includes provenance metadata linking back to source documents, enabling clinicians to verify the evidence underlying any recommendation.

You control your data. You decide who can access your Patient Knowledge Graph, and you can revoke access at any time. You can export your data in standard formats (FHIR/JSON) and request deletion subject to legal retention requirements.

SCOPE AND APPLICABILITY

This Privacy Policy applies when you:

- Visit our website at https://serelora.com or any website that links to this Privacy Policy
- Use our patient-facing or provider-facing applications, including our care coordination platform, document ingestion features, ambient scribe, Patient Knowledge Graph services, and related clinical workflow tools

• Connect to our Services through EHR/FHIR integrations, claims connectors, or third-party applications

• Use our mobile applications for iOS or Android

• Engage with us in other related ways, including sales, marketing, or support

Questions or concerns? Reading this Privacy Policy will help you understand your privacy rights and choices. If you do not agree with our policies and practices, please do not use our Services. If you have questions or concerns, please contact us at **privacy@serelora.com**.

TABLE OF CONTENTS

1. WHAT INFORMATION DO WE COLLECT?

Personal Information You Disclose to Us

In Short: We collect personal information that you provide to us, including health information when you use our clinical services.

We collect personal information that you voluntarily provide to us when you register on the Services, express an interest in obtaining information about us or our products and Services, when you participate in activities on the Services, or otherwise when you contact us.

Personal Information Provided by You. The personal information that we collect depends on the context of your interactions with us and the Services, the choices you make, and the products and features you use. The personal information we collect may include:

- Names (legal name, preferred name, aliases)
- Date of birth
- Phone numbers
- Email addresses
- Mailing addresses
- Usernames and passwords
- Contact or authentication data
- For healthcare providers: National Provider Identifier (NPI), medical license numbers, specialty designations, and organizational affiliations

Sensitive Information. When necessary, with your consent or as otherwise permitted by applicable law, we process the following categories of sensitive information:

- Health data (including medical records, diagnoses, medications, laboratory results, imaging reports, and clinical notes)
- Insurance and claims information
- Social determinants of health (housing, food security, transportation)
- Race, ethnicity, and demographic information (when relevant for clinical care)
- Account login credentials

Documents and Media. We collect documents you upload to our Services, including medical records, insurance documents, photographs (e.g., medication labels), and audio recordings from ambient scribe sessions (only with explicit consent from all participants).

Payment Data. We may collect data necessary to process your payment if you choose to make purchases. All payment data is handled and stored by PCI-compliant third-party payment processors. We do not store complete payment card numbers.

Information Automatically Collected

In Short: Some information—such as your Internet Protocol (IP) address and/or browser and device characteristics—is collected automatically when you visit our Services.

We automatically collect certain information when you visit, use, or navigate the Services. This information does not reveal your specific identity but may include device and usage information, such as your IP address, browser and device characteristics, operating system, language preferences, referring URLs, device name, country, location, information about how and when you use our Services, and other technical information.

Information Collected from Other Sources

In Short: We may collect information from healthcare providers, EHR systems, and other healthcare-related sources with your authorization.

In order to provide our care coordination services, we may obtain information about you from other sources, including:

- Healthcare providers and clinical staff
- Electronic Health Record (EHR) systems through FHIR APIs and authorized integrations
- Claims aggregators and health information exchanges
- Laboratories and imaging centers
- Health plans and payers
- Identity verification services

Derived and Inferred Information

We create derived information through our Services, including:

- **Patient Knowledge Graph:** A structured representation of your clinical, financial, and social information organized as nodes, edges, and relationships with provenance metadata
- Clinical summaries (including SBAR format), risk scores, and health assessments
- Care recommendations and action suggestions
- De-identified aggregates for analytics and research

2. HOW DO WE PROCESS YOUR INFORMATION?

In Short: We process your information to provide, improve, and administer our Services, communicate with you, for security and fraud prevention, and to comply with law. We may also process your information for other purposes with your consent.

We process your personal information for a variety of reasons, depending on how you interact with our Services:

- **To provide clinical services.** We process your information to build and maintain your Patient Knowledge Graph, generate clinical summaries, create risk assessments, and support care coordination.
- **To facilitate account creation and authentication.** We process your information so you can create and log in to your account.
- **To deliver and facilitate delivery of services.** We process your information to provide document ingestion, ambient scribe transcription, and care workflow support.
- **To respond to user inquiries and offer support.** We process your information to respond to your inquiries and solve any potential issues.
- **To send administrative information.** We process your information to send you details about our products and services, changes to our terms and policies, and other similar information.
- **To protect our Services.** We process your information as part of our efforts to keep our Services safe and secure, including fraud monitoring and prevention.
- **To comply with legal obligations.** We process your information to comply with applicable laws, regulations, court orders, and legal process.
- **For research purposes.** With appropriate authorization or using de-identified data, we may process information for research and product improvement.

3. WHEN AND WITH WHOM DO WE SHARE YOUR PERSONAL INFORMATION?

In Short: We may share information in specific situations described in this section and/or with specific categories of third parties. We do not sell your personal information.

Vendors, Consultants, and Other Third-Party Service Providers. We may share your data with third-party vendors, service providers, contractors, or agents who perform services for us or on our behalf and require access to such information to do that work. We have contracts in place with our third parties, which are designed to help safeguard your personal information. This means that they cannot do anything with your personal information unless we have instructed them to do it. They will also not share your personal information with any organization apart from us. They also commit to protect the data they hold on our behalf and to retain it for the period we instruct.

The categories of third parties we may share personal information with include:

- Cloud computing and hosting services
- AI and machine learning platforms
- Document processing and OCR services
- EHR/FHIR integration providers
- Data analytics services
- Payment processors
- Identity verification services
- Communication service providers (email, SMS)
- Security and monitoring services
- Healthcare providers (with your authorization)

We may also need to share your personal information in the following situations:

- **Clinical Recipients.** We share information with healthcare providers and care teams when you explicitly grant access or when sharing is necessary for treatment, payment, or healthcare operations as permitted by HIPAA.
- **Employers and Plan Sponsors.** With explicit consent or contractual authority, we may share limited or de-identified information with self-funded employer health plan sponsors for plan administration purposes. Individual PHI is shared only with explicit patient authorization.
- **Business Transfers.** We may share or transfer your information in connection with, or during negotiations of, any merger, sale of company assets, financing, or acquisition of all or a portion of our business.
- **Legal Requirements.** We may disclose information when required by law, court order, or government request, or when necessary to protect rights, safety, or property.
- **Research Partners.** With appropriate authorization or using de-identified data in accordance with HIPAA, we may share information with research institutions.

4. DO WE USE ARTIFICIAL INTELLIGENCE?

In Short: Yes. We offer products, features, and tools powered by artificial intelligence. All AI outputs include provenance and require human approval for clinical actions.

As part of our Services, we offer products, features, and tools powered by artificial intelligence, machine learning, and similar technologies (collectively, "AI Products"). These tools are designed to enhance healthcare coordination and provide clinical decision support.

Our AI Products are designed for the following functions:

- Document extraction and Patient Knowledge Graph construction
- Clinical summarization (including SBAR format)
- Risk assessment and predictive health indicators
- Care gap identification and recommendations
- Prior authorization prefill and documentation assistance
- Ambient scribe transcription and note generation

Use of AI Technologies. We may provide AI Products through third-party service providers ("AI Service Providers"). Your input, output, and personal information may be shared with and processed by these AI Service Providers to enable your use of our AI Products. We enter Business Associate Agreements with AI Service Providers that process PHI.

Human-in-the-Loop. AI outputs are informational only and do not constitute medical advice, diagnosis, or treatment recommendations. All AI suggestions, risk scores, and action drafts must be reviewed and approved by authorized clinicians or administrators before any clinical or administrative action is taken. We do not submit high-stakes forms or execute clinical decisions without human authorization.

5. HOW DO WE HANDLE PROTECTED HEALTH INFORMATION (PHI)?

In Short: When we handle PHI, we comply with HIPAA Privacy, Security, and Breach Notification Rules. We enter Business Associate Agreements with vendors that process PHI and maintain comprehensive safeguards.

HIPAA Compliance. When Serelora acts as a Business Associate or handles Protected Health Information, we comply with the Health Insurance Portability and Accountability Act (HIPAA) Privacy, Security, and Breach Notification Rules.

Business Associate Agreements. We enter Business Associate Agreements (BAAs) with all vendors that create, receive, maintain, or transmit PHI on our behalf. BAAs establish permitted uses and disclosures and require appropriate safeguards.

Access Controls. Access to PHI is role-based and limited to authorized personnel. All access to PHI is logged with user identification, timestamp, and purpose. Multi-factor authentication is required for provider and administrative access.

Minimum Necessary Standard. We limit PHI access, use, and disclosure to the minimum necessary to accomplish the intended purpose.

Your Rights Under HIPAA. As applicable, you have the right to:

- Access and obtain copies of your PHI
- Request amendments to your PHI
- Receive an accounting of disclosures of your PHI
- Request restrictions on certain uses and disclosures
- Receive confidential communications
- File complaints with us or with the HHS Office for Civil Rights

6. HOW DO OUR MOBILE APPLICATIONS INTERACT WITH YOUR INFORMATION?

In Short: Our mobile applications interact with your information in limited, specific ways. Temporary files are regularly deleted and we use app-private storage that cannot be accessed by other apps.

Our mobile applications for patients and providers connect to servers and systems to provide secure, mobile access to health information and care coordination features. These are the limited ways our mobile applications interact with your information:

- **Profile Photos.** When you add a profile photo, you may select an existing photo or take a new photo. A temporary copy is stored in app-private storage on your device. Temporary files are regularly deleted and are also deleted if you uninstall our mobile app.
- **Health and Fitness Data.** When you connect our mobile apps to Apple Health, Google Fit, or Health Connect, your data is securely transmitted and saved in your record. We do not store health and fitness data within our mobile apps beyond what is necessary for transmission.
- **Document Viewing.** When you view documents using our mobile apps, temporary copies are stored in app-private storage to make files viewable. Temporary copies are deleted when you close your session.
- **Photos and Videos in Messages.** When you include a photo or video in a message, temporary copies are stored in app-private storage. These temporary files are regularly deleted and are also deleted if you uninstall our mobile apps.
- **Telehealth Appointments.** When you join a telehealth appointment, our mobile apps will ask for permission to access your device's video and audio functionality. Our mobile apps do not record or store video or audio data from these visits unless ambient scribe is separately enabled with consent.
- **Automatic Appointment Arrival.** If enabled, our mobile apps temporarily store identifiers and times for upcoming appointments to detect your arrival. If you disable this feature, the identifiers are deleted.
- **Location Services.** You may choose to allow our mobile apps to interact with your device's location data for features like finding nearby providers or location-based check-in. Our mobile apps do not store or use your location data beyond these specific features.
- **Phone Calls.** If you choose to call a phone number displayed within the app, we will ask for permission to access your device's phone. Our mobile apps do not store your call history or data about the call.

App-Private Storage. Our mobile apps store data on your mobile device in app-private storage that cannot be accessed by other apps. Files you download or save from our mobile apps may be placed in locations accessible to other apps, such as your files app, only with your explicit permission.

Temporary File Deletion. Any temporary files created during the interactions described above are regularly deleted, and are also deleted if you uninstall our mobile apps.

7. WHAT ARE OUR AI TRANSPARENCY AND EXPLAINABILITY PRACTICES?

In Short: We are committed to transparent, explainable AI. Every AI output includes provenance metadata linking to source documents so clinicians can verify evidence.

Provenance. Every extracted fact, Patient Knowledge Graph update, and model output includes provenance metadata identifying the source document, page/section, timestamp, and extractor version. This enables clinicians to verify evidence underlying any AI-generated content.

Source Attribution. AI summaries include citations that link back to original source documents. Every SBAR or model output includes a "source and evidence" panel linking to original documents.

Explainability. Where applicable, we surface SHAP-style or citation-based attributions explaining contributing factors for AI-generated assessments. Clinicians can expand to view source documents.

Audit Trail. We maintain comprehensive audit trails showing who accessed what information and for what purpose. Patients can view a history of access events.

8. HOW LONG DO WE KEEP YOUR INFORMATION?

In Short: We keep your information for as long as necessary to fulfill the purposes outlined in this Privacy Policy unless otherwise required by law. Medical records may be subject to longer retention requirements.

We will only keep your personal information for as long as it is necessary for the purposes set out in this Privacy Policy, unless a longer retention period is required or permitted by law (such as tax, accounting, medical record retention, or other legal requirements).

Retention periods vary by data category:

- **Patient Knowledge Graph and Clinical Records:** Retention may be governed by provider or employer contracts and applicable medical record retention laws, which may require retention for 7 or more years.
- **Account Information:** Retained while your account is active and for a reasonable period thereafter.
- **Audit Logs:** Retained for a minimum of 6 years as required by HIPAA.
- **Technical Logs:** Retained for security and troubleshooting purposes, typically 90 days to 1 year.
- **De-identified Data:** May be retained indefinitely for analytics and research.

When we have no ongoing legitimate business need to process your personal information, we will either delete or anonymize such information, or, if this is not possible, we will securely store your personal information and isolate it from any further processing until deletion is possible.

9. HOW DO WE KEEP YOUR INFORMATION SAFE?

In Short: We maintain administrative, technical, and physical safeguards designed to comply with HIPAA and industry best practices. However, no system is 100% secure.

We have implemented appropriate and reasonable technical, administrative, and physical security measures designed to protect the security of any personal information we process.

Technical Safeguards:

- Encryption in transit (TLS 1.2+) and at rest (AES-256)
- Role-based access control with least privilege principles
- Multi-factor authentication for provider and administrative accounts
- Comprehensive audit logging of access to PHI
- Firewalls, intrusion detection, and network segmentation
- Regular penetration testing and security assessments

Administrative Safeguards:

- Security and privacy training for all employees
- Background checks for employees with access to PHI
- Documented security policies and procedures
- Incident response plans with defined escalation procedures
- Vendor due diligence and ongoing monitoring

Physical Safeguards:

- SOC 2 Type II certified data centers with physical access controls
- Workstation security policies
- Secure disposal of hardware and storage media

Safeguards Built Into Our Mobile Apps:

- Multi-factor authentication by default
- App-private storage that cannot be accessed by other apps
- In-app notifications and permission requests to help you make informed decisions
- Screenshot functionality disabled by default on Android devices
- HTTPS for all secure communication with servers

Steps You Can Take to Protect Your Information:

- Do not share the username and password you use with our Services
- Change your password immediately if you believe any unauthorized access has occurred
- Use the security tools on devices you use with our Services
- Do not root or jailbreak devices you use with our mobile apps—doing so can create security risks by removing your devices' built-in security measures and exposing sensitive information

However, despite our safeguards and efforts to secure your information, no electronic transmission over the Internet or information storage technology can be guaranteed to be 100% secure, so we cannot promise or guarantee that hackers, cybercriminals, or other unauthorized third parties will not be able to defeat our security. We maintain incident response plans and will notify affected users and regulators in accordance with applicable laws, including HIPAA breach notification requirements.

10. DO WE COLLECT INFORMATION FROM MINORS?

In Short: We do not knowingly collect data from or market to children under 13 years of age without parental consent.

We do not knowingly collect, solicit data from, or market to children under 13 years of age, nor do we knowingly sell such personal information. By using the Services, you represent that you are at least 13 or that you are the parent or guardian of such a minor and consent to such minor dependent's use of the Services.

For minors aged 13-18, parental or guardian controls and provider policies apply in accordance with applicable law.

If we learn that personal information from users less than 13 years of age has been collected without parental consent, we will deactivate the account and take reasonable measures to promptly delete such data from our records. If you become aware of any data we may have collected from children under age 13, please contact us at privacy@serelora.com.

11. WHAT ARE YOUR PRIVACY RIGHTS?

In Short: Depending on your location, you may have rights to access, correct, delete, or port your personal information. You may also withdraw consent at any time.

Withdrawing your consent. If we are relying on your consent to process your personal information, you have the right to withdraw your consent at any time. You can withdraw your consent by contacting us at privacy@serelora.com.

Account Information. If you would at any time like to review or change the information in your account or terminate your account, you can:

- Contact us using the contact information provided
- Log in to your account settings and update your information
- Export your Patient Knowledge Graph in FHIR/JSON format

Upon your request to terminate your account, we will deactivate or delete your account and information from our active databases. However, we may retain some information to prevent fraud, troubleshoot problems, assist with investigations, enforce our legal terms, and/or comply with applicable legal requirements.

Data Portability. You may request a machine-readable export of your Patient Knowledge Graph and source documents in FHIR/JSON format through your account settings or by contacting privacy@serelora.com.

Your Healthcare Organizations. To use certain features of our Services, you may have an account with a healthcare organization. Because of this, your use of our Services is also subject to each of your healthcare organizations' privacy policies. Please contact your healthcare organizations if you have any questions about their privacy policies, how they store and retain your health information, and how you can make requests to them about their disclosure, correction, or deletion of your health information.

12. DO UNITED STATES RESIDENTS HAVE SPECIFIC PRIVACY RIGHTS?

In Short: If you are a resident of certain U.S. states, you may have additional rights regarding your personal information, including the right to access, correct, delete, and port your data.

State Privacy Laws. If you are a resident of California, Colorado, Connecticut, Delaware, Florida, Indiana, Iowa, Kentucky, Maryland, Minnesota, Montana, Nebraska, New Hampshire, New Jersey, Oregon, Rhode Island, Tennessee, Texas, Utah, Virginia, or other states with applicable privacy laws, you may have additional rights.

Your Rights. These rights include:

- Right to know whether or not we are processing your personal data

- Right to access your personal data
- Right to correct inaccuracies in your personal data
- Right to request the deletion of your personal data
- Right to obtain a copy of the personal data you previously shared with us
- Right to non-discrimination for exercising your rights
- Right to opt out of targeted advertising, sale of personal data, or profiling

Sale of Personal Information. We have not sold or shared any personal information to third parties for a business or commercial purpose in the preceding twelve (12) months. We do not sell personal information.

How to Exercise Your Rights. To exercise these rights, you can contact us by emailing privacy@serelora.com, using your account settings, or by referring to the contact details at the bottom of this document.

Appeals. Under certain US state data protection laws, if we decline to take action regarding your request, you may appeal our decision by emailing us at privacy@serelora.com. We will inform you in writing of any action taken or not taken in response to the appeal. If your appeal is denied, you may submit a complaint to your state attorney general.

California "Shine The Light" Law. California Civil Code Section 1798.83 permits California residents to request information about disclosures to third parties for direct marketing purposes. We do not disclose personal information to third parties for direct marketing purposes.

13. CONTROLS FOR DO-NOT-TRACK FEATURES

In Short: We do not currently respond to DNT browser signals as no uniform standard has been finalized.

Most web browsers and some mobile operating systems and mobile applications include a Do-Not-Track ("DNT") feature or setting you can activate to signal your privacy preference not to have data about your online browsing activities monitored and collected. At this stage, no uniform technology standard for recognizing and implementing DNT signals has been finalized. As such, we do not currently respond to DNT browser signals or any other mechanism that automatically communicates your choice not to be tracked online. If a standard for online tracking is adopted that we must follow in the future, we will inform you about that practice in a revised version of this Privacy Policy.

14. DO WE MAKE UPDATES TO THIS POLICY?

In Short: Yes, we will update this policy as necessary to stay compliant with relevant laws.

We may update this Privacy Policy from time to time. The updated version will be indicated by an updated "Last updated" date at the top of this Privacy Policy. If we make material changes to this Privacy Policy, we may notify you either by prominently posting a notice of such changes or by directly sending you a notification. We encourage you to review this Privacy Policy frequently to be informed of how we are protecting your information.

15. HOW CAN YOU CONTACT US ABOUT THIS POLICY?

If you have questions or comments about this policy, you may contact our Privacy Office:

Serelora Inc.

Privacy Office

1111B S Governors Ave #99442

Dover, DE 19904

United States

Email: privacy@serelora.com

For HIPAA-related complaints, you may also file a complaint with the U.S. Department of Health and Human Services, Office for Civil Rights.

GDPR and UK GDPR Privacy Questions. If you need to contact us regarding GDPR or UK GDPR matters, please email privacy@serelora.com. If you are a Data Subject as defined by GDPR, you should also reach out to your healthcare organization for requests related to your personal data accessed through our Services.

* * *