

Privacy Policy

Last updated 07/31/26

[1. Introduction](#)

[2. Scope of This Policy](#)

[2.1. What Is Covered](#)

[2.2. What Is Not Covered](#)

[2.3. Customer Data](#)

[3. Clinia's Role](#)

[3.1. Clinia's Own Processing](#)

[3.2. Processing on Behalf of Customers](#)

[4. Personal Information We Collect](#)

[4.1. Contact and Identity Information](#)

[4.2. Account and Authentication Information](#)

[4.3. Professional and Business Information](#)

[4.4. Communications and Support Information](#)

[4.5. Technical, Usage, and Log Information](#)

[4.6. Recruitment Information](#)

[4.7. Customer Data](#)

[5. How We collect Personal Information](#)

[5.1. Directly From You](#)

[5.2. Through The Use of Our Website and Services](#)

[5.3. From Clinia Customers and Authorized Users](#)

[5.4. From Service Providers and Business Partners](#)

[5.5. From Public or Third-Party Sources](#)

[5.6. From Legal, Regulatory, or Governmental Sources](#)

[6. How We Use Personal Information](#)

[6.1. To Provide and Operate our Services](#)

[6.2. To Communicate With You](#)

[6.3. To Support Customer Relationships And Administer Our Enterprise](#)

[6.4. To Secure And Protect Our Services](#)

[6.5. To Improve Our Website, Services, And Operations](#)

[6.6. To Support Recruitment And Employment Processes](#)

[6.7. To Comply With Legal And Regulatory Obligations](#)

[6.8. To Protect Rights And Interests](#)

[6.9. For Other Purposes With Consent Or As Permitted By Law](#)

[7. Legal Bases and Consent](#)

[7.1. Legal Bases](#)

[7.2. Consent](#)

[8. Customer Data and Enterprise Services](#)

[9. Health Information and Sensitive Information](#)

- [10. AI-Supported Features and Automated Processing](#)
 - [10.1. Customer-Controlled AI Workflows](#)
 - [10.2. Use of AI at Clinia](#)
 - [10.3. Automated Processing](#)
- [11. How We Disclose Personal Information](#)
 - [11.1. Affiliates](#)
 - [11.2. Service Providers And Subprocessors](#)
 - [11.3. Customer-Directed Disclosures And Integrations](#)
 - [11.4. Professional Advisors](#)
 - [11.5. Legal, Regulatory, Security, And Compliance Purposes](#)
 - [11.6. Business Transactions](#)
 - [11.7. With Consent Or As Otherwise Permitted By Law](#)
- [12. Cross-Border Processing and Data Residency](#)
- [13. Cookies and Similar Technologies](#)
- [14. Retention and Deletion](#)
 - [14.1. Retention](#)
 - [14.2. Deletion](#)
 - [14.3. Customer Data](#)
 - [14.4. Backups](#)
- [15. Security](#)
- [16. Your Privacy Rights and Choices](#)
- [17. Children and Minors](#)
- [18. Changes To This Policy](#)
- [19. Contact Us](#)
- [20. Jurisdiction-Specific Notices](#)
 - [SCHEDULE 1](#)
 - [Canada](#)
 - [SCHEDULE 2](#)
 - [Quebec](#)
 - [SCHEDULE 3](#)
 - [EEA / UK GDPR](#)
 - [SCHEDULE 4](#)
 - [HIPAA](#)
 - [SCHEDULE 5](#)
 - [California](#)
 - [SCHEDULE 6](#)
 - [Other U.S. State Privacy Laws](#)

1. Introduction

Clinia Health Inc. (“**Clinia**,” “**we**,” “**us**,” or “**our**”) provides technology products and services for healthcare and health-related organizations (collectively, the “**Services**”). This Privacy Policy explains how we collect, use, disclose, retain, protect and otherwise process Personal Information in connection with our website, business operations, communications, recruitment activities, and services.

We understand that privacy and data protection are critical for the organizations and individuals who interact with Clinia, given the sensitivity of the Personal Information that we are entrusted with. Our approach is designed to reflect the operational realities of healthcare technology, including enterprise customer relationships, sensitive health information, AI-supported workflows, and deployment models where responsibilities may be shared between Clinia and our customers.

This Privacy Policy is intended to help customers and individuals understand Clinia’s privacy practices. It does not replace any agreement between Clinia and a customer, including any master services agreement, general terms of service, service request, order form, product schedule, data processing addendum, business associate agreement, security terms, applicable privacy, transfer, or healthcare-specific terms, or similar contractual document (collectively, the “**Customer Agreement**”).

Depending on the context, references to “you” in this Privacy Policy might be a reference to you as a customer or our services (a “**Customer**”), as an authorized user of a customer, as a visitor of our Website or as a data subject whose Personal Information is part of Customer Data (as defined below).

2. Scope of This Policy

2.1. What Is Covered

This Privacy Policy applies to Personal Information that Clinia collects or processes when you:

- visit or interact with our website;
- communicate with us, including through email, forms, events, sales processes, support channels, or other business communications;
- use or access Clinia Services as an authorized user of a Clinia customer;
- apply for a role with Clinia;
- otherwise interact with Clinia in a business, technical, professional, or operational context.

2.2. What Is Not Covered

This Privacy Policy does not apply to:

- Personal Information handled under a separate Clinia employee or contractor privacy notice;
- websites, applications, services, or integrations operated by third parties; or
- customer-controlled systems, applications, workflows, configurations or environments, except to the extent Clinia processes Personal Information within its own operational scope.

2.3. Customer Data

This Privacy Policy also explains, at a high level, how Clinia handles Personal Information that may be processed through our enterprise services. In many cases, that information is provided to Clinia by, or on behalf of, a Clinia customer. We refer to this type of information as “Customer Data” in our customer agreements.

If your Personal Information is included in Customer Data, the relevant Clinia customer is generally responsible for explaining how that information is used and for responding to privacy requests. You should contact that Customer directly unless this Privacy Policy or applicable law provides otherwise.

Additional information about Customer Data and enterprise services is provided in Section 8.

3. Clinia's Role

Clinia's privacy responsibilities depend on the context in which Personal Information is processed:

3.1. Clinia's Own Processing

For our website, business operations, sales and marketing activities, customer communications, recruitment activities, security operations, and internal administration, Clinia generally acts as the organization responsible for determining how and why Personal Information is processed. Depending on the applicable law, Clinia may be considered a controller, business, organization, or similar role for this processing.

3.2. Processing on Behalf of Customers

For enterprise services, Clinia often processes Personal Information on behalf of a Customer. In that context, the Customer is generally responsible for determining the purpose of the processing, the categories of information submitted to the services, the individuals whose information is processed, the deployment and configuration choices that affect the processing, and the legal basis for using that information. Depending on the applicable law, Clinia may be considered a processor, service provider, business associate, subcontractor, or similar role for this processing. Clinia processes that information in accordance with the applicable Customer Agreement.

4. Personal Information We Collect

The Personal Information Clinia collects depends on how you interact with us and which services are used by our Customer. We collect Personal Information only where reasonably necessary for the purposes described in this Privacy Policy, our Customer Agreements, or as otherwise permitted or required by law. Clinia identifies the purposes for which Personal Information is collected before or at the time of collection, unless otherwise permitted by law.

4.1. Contact and Identity Information

We may collect information such as your name, business email address, phone number, organization, title, role, and other contact details when you communicate with us, request information, attend an event, schedule a meeting, subscribe to updates, or otherwise interact with Clinia.

4.2. Account and Authentication Information

If you access Clinia services, we may collect account-related information such as your name, email address, username, role, organization, authentication status, access permissions, and related account administration information.

4.3. Professional and Business Information

We may collect information about your organization, professional role, qualifications, affiliations, certifications, areas of responsibility, business needs, and interactions with Clinia.

4.4. Communications and Support Information

We may collect information you provide when you contact us, submit a form, participate in a sales or support process, respond to surveys, exchange emails with us, or otherwise communicate with Clinia. This may include message content, support requests, feedback, and related business communications.

4.5. Technical, Usage, and Log Information

When you visit our website or use our services, we may collect technical and operational information such as IP address, device information, browser type, operating system, pages viewed, referring URLs, timestamps, authentication events, access logs, system activity, error information, usage metrics, and security-related logs. This information helps us operate, secure, monitor, support, troubleshoot, and improve our website and services.

4.6. Recruitment Information

If you apply for a role with Clinia, we may collect information such as your name, contact details, resume, employment history, education, qualifications, skills, references, interview notes, communications with us, and other information you choose to provide as part of the recruitment process.

4.7. Customer Data

Clinia's customers and authorized users may submit, upload, transmit, or otherwise make available Personal Information through Clinia's services. This may include information about patients, healthcare providers, customer personnel, end users, or other individuals, depending on how the customer configures and uses the services. This may include Personal Information about you, for example if you are a patient of one of Clinia's Customers or if your information is otherwise submitted through the services by a Clinia Customer or authorized user.

Clinia does not control the categories of Customer Data submitted by customers or authorized users. Customer Data is handled in accordance with the applicable Customer Agreement.

5. How We collect Personal Information

Clinia collects Personal Information in several ways, depending on the nature of your interaction with us. Where we collect Personal Information from third parties about you, we only do so as permitted by law or with your prior authorization.

5.1. Directly From You

We collect Personal Information when you provide it to us directly, including when you complete a form, request a demo, communicate with our team, subscribe to updates, attend an event, submit a support request, participate in a business process, or apply for a role with Clinia.

5.2. Through The Use of Our Website and Services

We collect certain technical, usage, and log information automatically when you visit our website or use Clinia services. This may occur through cookies, similar technologies, application logs, security logs, authentication records, monitoring tools, or other operational systems.

5.3. From Clinia Customers and Authorized Users

We may receive Personal Information from Customers and authorized users when they configure, access, or use Clinia's services, or when they communicate with us in connection with those services. Personal information submitted through the services for a customer's use of the services is generally Customer Data controlled by the Customer. Personal information provided in support, account management, implementation, billing, security, procurement, or similar business communications may be handled by Clinia for the purposes described in this Privacy Policy.

5.4. From Service Providers and Business Partners

We may receive Personal Information from service providers, business partners, event partners, recruitment providers, background check providers, security providers, analytics providers, and similar organizations that support our business operations and that are authorized to make that information available to us.

5.5. From Public or Third-Party Sources

We may collect Personal Information from public sources or third-party sources where permitted by law, such as professional networking platforms, company websites, public registries, business contact databases, or other sources used for business development, recruitment, security, compliance, or verification purposes.

5.6. From Legal, Regulatory, or Governmental Sources

In limited circumstances, we may receive Personal Information from courts, regulators, government agencies, law enforcement, or other legal or regulatory sources where permitted or required by law.

6. How We Use Personal Information

Clinia uses Personal Information only for the purposes described below, depending on the context in which the information is collected and the services involved.

6.1. To Provide and Operate our Services

We use Personal Information to provide, operate, configure, maintain, support, and improve our website and services. This includes account administration, authentication, access management, customer support, troubleshooting, service communications, and technical operations.

6.2. To Communicate With You

We use Personal Information to respond to inquiries, provide information you request, manage our business relationship, send administrative messages, communicate about services, provide support, and share updates relevant to your interaction with Clinia.

6.3. To Support Customer Relationships And Administer Our Enterprise

We use Personal Information to manage customer, partner, vendor, and prospect relationships. This may include sales communications, contract administration, billing support, implementation coordination, account management, and customer success activities.

6.4. To Secure And Protect Our Services

We use Personal Information to ensure the security, confidentiality, integrity, and availability of our website, systems, products, services, and business operations. This includes monitoring for security events, detecting unauthorized access, investigating incidents, preventing fraud, enforcing access controls, maintaining logs, and supporting audit and compliance activities.

6.5. To Improve Our Website, Services, And Operations

We may use Personal Information, technical information, usage data, and aggregated data to understand how our website and services are used, evaluate performance, troubleshoot issues, improve reliability, enhance functionality, and develop operational insights.

Where permitted by the applicable Customer Agreement and applicable law, Clinia may use de-identified, aggregated, anonymized, or non-identifiable technical and operational information to monitor, maintain, improve, and develop the services. This may include service reliability, performance, security, taxonomy mapping, deduplication, ranking, matching, and similar platform-level functionality.

Clinia does not treat Personal Information as anonymized, de-identified, aggregated, or non-identifiable unless the applicable legal and technical requirements are met. Additional information about AI-supported features, automated processing, and related training or improvement limitations is provided in Section 10.

6.6. To Support Recruitment And Employment Processes

We use recruitment information to evaluate applications, communicate with candidates, conduct interviews, assess qualifications, perform reference or background checks where permitted by law, make hiring decisions, and manage recruitment administration.

6.7. To Comply With Legal And Regulatory Obligations

We use Personal Information where necessary to comply with applicable laws, legal processes, regulatory requirements, contractual obligations, audit requirements, and lawful requests from public authorities.

6.8. To Protect Rights And Interests

We may use Personal Information to protect the rights, property, safety, security, and interests of Clinia, our Customers, authorized users, business partners, personnel, and others. This may include enforcing agreements, investigating potential violations, resolving disputes, and establishing, exercising, or defending legal claims.

6.9. For Other Purposes With Consent Or As Permitted By Law

We may use Personal Information for other purposes with your consent or as otherwise permitted or required by applicable law.

7. Legal Bases and Consent

7.1. Legal Bases

Clinia processes Personal Information only where we have a lawful basis to do so under applicable privacy and data protection laws.

Depending on the context and on the applicable jurisdiction, Clinia may process Personal Information based on one or more of the following legal bases:

- your consent;
- the need to perform a contract or take steps before entering into a contract;
- Clinia's legitimate interests, where those interests are not overridden by applicable privacy rights;
- compliance with legal or regulatory obligations;
- protection of vital interests, such as your safety or security;
- purposes otherwise permitted or required by applicable law.

7.2. Consent

Where consent is required, Clinia seeks consent that is appropriate to the nature, context, and sensitivity of the Personal Information involved. It also seeks to obtain consent that is clear, free, informed and given for specific purposes. Consent may be express or implied (in limited circumstances, such as when you voluntarily provide us with Personal Information).

You may withdraw your consent where consent is the legal basis for processing, subject to legal restrictions and reasonable notice. Withdrawing consent may affect Clinia's ability to provide certain communications, services, access, or functionality. Withdrawal of consent does not affect processing that occurred before the withdrawal or processing that is permitted or required by law.

8. Customer Data and Enterprise Services

Clinia provides enterprise services to healthcare and health-related organizations. Customers and authorized users may submit, upload, transmit, configure, or otherwise make available Personal Information through those Services.

Customer Data may include Personal Information about patients, healthcare providers, customer personnel, authorized users, end users, or other individuals, depending on the Customer's configuration and use of the services. Clinia does not determine what Customer Data a Customer chooses to submit to the services or how the Customer uses that information in its own systems, applications, workflows, or environments.

Customers are generally responsible for:

- determining whether and how to use the services for their intended workflows;
- ensuring that Customer Data is collected, used, disclosed, and submitted to Clinia in accordance with applicable law;
- providing required privacy notices to individuals whose data is processed;
- obtaining required consents, authorizations, permissions, or other legal bases;
- managing their own authorized users and end users;
- configuring customer-controlled systems, integrations, and environments; and
- responding to privacy rights requests relating to Customer Data, unless otherwise required by law or agreed in writing.

Clinia uses Customer Data only as needed to provide, secure, support, troubleshoot, monitor, maintain, and improve the applicable services, comply with legal obligations, prevent or address fraud, security incidents, or service integrity issues, and as otherwise permitted by the applicable Customer Agreement or Customer instructions. Clinia does not sell Customer Data.

If your Personal Information has been submitted to Clinia by or on behalf of a Clinia Customer, please contact that Customer first with any request or question about how your Personal Information is used. Where required by applicable law, Clinia will support the Customer in responding to privacy rights requests.

9. Health Information and Sensitive Information

Clinia operates in healthcare and health-related environments where Personal Information may include health information, protected health information, sensitive Personal Information, or other similar categories of information that require additional care under applicable law (collectively, the "**Sensitive Information**").

Clinia handles Sensitive Information within its scope of control in accordance with the applicable Customer Agreement, this Privacy Policy, and applicable law.

Clinia may process Sensitive Information when a Customer configures or uses the services in a way that involves that information. This may include information about patients, care teams, healthcare providers, clinical workflows, health records, documents, search queries, prompts, outputs, or other healthcare-related information, depending on the services used and the Customer's configuration.

Where Sensitive Information is included in Customer Data, the Customer is generally responsible for determining whether the information may be submitted to the services, providing required notices, obtaining required consents or authorizations, and ensuring that the Customer's use of the services complies with applicable healthcare, privacy, professional, and regulatory obligations.

Clinia does not use Sensitive Information for generalized model training or cross-customer improvement unless expressly permitted by the applicable Customer Agreement and applicable law.

If you provide sensitive information to Clinia outside the context of Customer Data, Clinia will use and disclose that information only for the purposes for which it was provided, as described in this Privacy Policy, with your consent where required, or as otherwise permitted or required by applicable law.

10. AI-Supported Features and Automated Processing

10.1. Customer-Controlled AI Workflows

Some Clinia services may include AI-supported features, automated processing, search, retrieval, summarization, conversational functionality, recommendations, ranking, classification, analytics, or other algorithmic functionality.

Where these features are used as part of enterprise services, the Customer is generally responsible for determining whether the features are appropriate for its intended use cases, workflows, users, and regulatory obligations. Customer-controlled AI workflows, prompts, retrieval context, outputs, and related configurations are governed by the applicable Customer Agreement.

Unless expressly permitted by the applicable Customer Agreement and applicable law, Clinia does not use Customer Data, health information, prompts, outputs, clinical content, deployment-specific logs, retrieval results, or Customer-specific evaluation data to train or improve generalized models for use across unrelated Customers.

AI-generated or AI-supported outputs should be reviewed by qualified personnel before being used in clinical, operational, professional, or other decision-making contexts. Clinia does not make patient care decisions or determine treatment.

10.2. Use of AI at Clinia

Clinia may use AI-supported tools and third-party AI services as part of its own internal business operations and workflows, including in connection with our website, communications, sales and marketing, support, security, recruitment, and administrative activities. These tools may have access to Personal Information that is not Customer Data in order to perform their intended functions.

We do not use this Personal Information, or make it available to our AI tools or providers, to train, fine-tune, or otherwise develop generalized AI models, except with your consent or another lawful basis that specifically permits that use.

Where we engage third-party AI providers, we take reasonable steps designed to ensure that they handle Personal Information only as needed to provide services to Clinia, subject to appropriate confidentiality, security, and privacy obligations, and not for their own model training purposes.

10.3. Automated Processing

Where applicable law gives you rights in relation to automated decision-making, profiling, or similar processing, you may contact us using the information in the “Contact Us” section below. If the relevant processing is controlled by a Clinia Customer, we may direct your request to that Customer or support the Customer in responding, as required by applicable law.

11. How We Disclose Personal Information

Clinia discloses Personal Information only where reasonably necessary for the purposes described in this Privacy Policy, as directed by a Customer, as permitted by the applicable Customer Agreement, or as otherwise permitted or required by law.

11.1.Affiliates

We may disclose Personal Information to Clinia affiliates where necessary for business operations, service delivery, customer support, administration, security, compliance, or other purposes described in this Privacy Policy.

11.2.Service Providers And Subprocessors

We may disclose Personal Information to service providers, vendors, subprocessors, contractors, and other partners that support Clinia's business operations and services. These may include providers of cloud infrastructure, hosting, security, monitoring, analytics, customer support, communications, professional services, recruitment, finance, billing, and business operations.

These recipients are authorized to use Personal Information only as needed to provide services to Clinia or as otherwise permitted by law. Where required, they are subject to contractual obligations relating to confidentiality, security, privacy, and appropriate handling of Personal Information.

11.3.Customer-Directed Disclosures And Integrations

Where Clinia provides enterprise services, Customers may configure the services to connect with Customer systems, Customer applications, identity providers, data sources, analytics tools, AI or model providers, or other third-party services. Personal information may be disclosed through those integrations based on the Customer's configuration, instructions, and use of the services.

Clinia is not responsible for privacy practices of third-party services selected, configured, or controlled by the Customer.

11.4.Professional Advisors

We may disclose Personal Information to lawyers, auditors, accountants, insurers, consultants, and other professional advisors where reasonably necessary for legal, audit, insurance, financial, governance, compliance, or business purposes.

11.5.Legal, Regulatory, Security, And Compliance Purposes

We may disclose Personal Information where we believe disclosure is necessary or appropriate to comply with applicable law, legal process, regulatory requirements, governmental requests, audit obligations, or contractual commitments.

We may also disclose Personal Information to protect the rights, safety, security, property, or interests of Clinia, our customers, authorized users, personnel, business partners, or others. This may include detecting, preventing, or responding to fraud, security incidents, service integrity issues, unauthorized access, or misuse of our website or services.

11.6.Business Transactions

We may disclose Personal Information in connection with a proposed or completed business transaction, such as a merger, acquisition, financing, reorganization, sale of assets, due diligence process, or similar corporate transaction. Where required by law, we will take appropriate steps to protect Personal Information in connection with the transaction.

11.7.With Consent Or As Otherwise Permitted By Law

We may disclose Personal Information with consent or as otherwise permitted or required by applicable law.

12. Cross-Border Processing and Data Residency

Clinia is based in Canada and may process Personal Information in Canada, the United States, the European Economic Area, the United Kingdom, or other jurisdictions where Clinia, its affiliates, service providers, subprocessors, or partners operate.

When Personal Information is processed outside the jurisdiction where it was collected or where you reside, it may be subject to the laws of that other jurisdiction. Clinia takes reasonable steps designed to protect Personal Information in accordance with this Privacy Policy, applicable Customer Agreement, and applicable privacy and data protection laws.

Where required by applicable law, Clinia uses appropriate safeguards for cross-border processing and transfers. These safeguards may include contractual protections, data processing addenda, standard contractual clauses, transfer impact assessments, adequacy decisions, privacy impact assessments, vendor due diligence, technical and organizational safeguards, or other measures recognized by applicable law.

For Clinia-managed services, data residency, hosting locations, subprocessors, and transfer safeguards may be described in the applicable Customer Agreement or other customer-facing material.

For Customer-managed deployments, the Customer may control the deployment environment, cloud account, infrastructure configuration, network boundary, deployment region, data residency, access management, monitoring, logging, and related operational settings. In those deployments, patient data, clinical records, operational data, and other Customer Data may remain within the Customer-controlled environment unless the Customer configures the services otherwise.

Where Clinia requires access to Personal Information in a Customer-managed deployment for support, troubleshooting, security, or operational purposes, access is handled in accordance with the applicable Customer Agreement, product schedule, support process, customer authorization, and applicable law.

13. Cookies and Similar Technologies

Clinia uses cookies and similar technologies on our website and, where applicable, in our services.

Cookies are small text files placed on your device when you visit a website or use an online service. Similar technologies may include pixels, local storage, software development kits, tags, and related tools.

We may use cookies and similar technologies to:

- enable website and service functionality;
- remember preferences, such as language or region;
- support authentication and secure access;
- understand how our website and services are used;
- measure performance and improve user experience;
- support security, fraud prevention, and service integrity;
- manage communications, analytics, or marketing activities, where permitted by law.

Some cookies are necessary for our website or services to function. Others are optional and may depend on your preferences, browser settings, or consent choices.

Where our website uses a cookie preference tool, you can use that tool to manage available cookie choices. You may also be able to manage cookies through your browser settings. If you disable or block certain cookies, some website or service features may not function properly.

Cookies and similar technologies used within Clinia products or enterprise services may be limited to those required for authentication, security, session management, service operation, or similar necessary purposes, unless otherwise described in the applicable product documentation or customer agreement.

14. Retention and Deletion

14.1. Retention

Clinia retains Personal Information only for as long as reasonably necessary for the purposes described in this Privacy Policy, unless a longer retention period is required or permitted by law.

The period for which we retain Personal Information depends on the nature of the information, the purpose for which it was collected, the services involved, applicable legal or regulatory requirements, contractual obligations, security needs, audit requirements, dispute resolution needs, and legitimate business purposes.

14.2. Deletion

When Personal Information is no longer required, Clinia will delete, anonymize, or otherwise handle it in accordance with applicable law, our retention practices, and applicable contractual obligations.

14.3. Customer Data

Customer Data processed through enterprise services is retained and deleted in accordance with the applicable Customer Agreement, Customer instructions and applicable law. In Customer-managed deployments, retention and deletion may be controlled by the Customer within the Customer's own environment.

14.4. Backups

Backups, logs, audit records, and security records may be retained for limited periods where necessary for security, continuity, compliance, audit, legal, or operational purposes. Where deletion from backups is not immediately practicable, Personal Information will be protected from further processing except as required or permitted by law.

15. Security

Clinia maintains reasonable administrative, technical, and organizational safeguards designed to protect Personal Information against unauthorized access, use, disclosure, alteration, loss, or destruction. These safeguards are designed to be appropriate to the nature and sensitivity of the information, the purposes of processing, and the risks involved.

Safeguards may include access controls, authentication controls, role-based permissions, encryption, logging, monitoring, vulnerability management, secure development practices, incident response procedures, personnel training, confidentiality obligations, vendor oversight, and business continuity practices.

Security responsibilities depend on the services, deployment model, Customer configuration, and operational scope. For Clinia-managed environments, Clinia is responsible for safeguards within its operational control. For Customer-managed deployments, the Customer is responsible for infrastructure-level controls within the Customer environment, including cloud account governance, network configuration, identity and access management, monitoring, backups, deployment region, and related infrastructure security controls.

Clinia does not require unrestricted access to Customer Data to provide the services. Where support access to Customer Data, Customer environments, logs, prompts, outputs, health information, or other Sensitive Information is required, access is limited to the approved purpose, authorized personnel, applicable support process, and customer authorization where required.

Clinia maintains security and privacy governance practices that are reviewed and improved over time. These practices are supported by operational monitoring, vulnerability management, incident response, change management, risk management, and independent assurance activities, where applicable.

No security measure can guarantee complete security. Customers and authorized users also play an important role in protecting Personal Information, including by managing credentials, access permissions, Customer-controlled environments, integrations, and user activity.

16. Your Privacy Rights and Choices

Depending on where you are located and how your Personal Information is processed, you may have certain rights in relation to your Personal Information. The availability to you of such rights depends on the privacy legislation applicable to you. Note that after exercising certain of these rights, we may no longer be able to provide certain of our services to you.

These rights may include the right to:

- request access to your Personal Information;
- request correction of inaccurate or incomplete Personal Information;
- request deletion of Personal Information;
- withdraw consent, where processing is based on consent;
- object to or restrict certain processing;
- request information about how Personal Information is collected, used, disclosed, or transferred;
- request portability of Personal Information, where applicable;
- make a complaint to Clinia or to a privacy or data protection authority.

To submit a privacy request to Clinia, please contact us using the information in the “Contact Us” section below. We may need to verify your identity before responding to your request.

Where your request relates to Customer Data processed by Clinia on behalf of a Customer, we may direct you to the relevant Customer. The Customer is generally responsible for responding to privacy requests relating to Customer Data, unless applicable law or a written agreement requires otherwise. Where required, Clinia will support the Customer in responding to your request.

Clinia will respond to privacy requests within the time required by applicable law. In some cases, we may refuse a request or limit our response where permitted by law, including where the request affects the rights of others, relates to information we are required or permitted to retain, would compromise security or confidentiality, or relates to information controlled by a Clinia Customer.

17. Children and Minors

Clinia’s website and business services are not directed to children, and Clinia does not knowingly collect Personal Information directly from children for any purpose.

Because Clinia provides services for healthcare and health-related organizations, Customer Data may include Personal Information about minors where a Customer submits or configures the services to process that information. In those cases, the Customer is generally responsible for determining whether the information may be processed, providing required notices, obtaining required consents or authorizations, and complying with applicable laws relating to minors’ information.

If you believe that a child has provided Personal Information directly to Clinia without appropriate consent, please contact us using the information in the “Contact Us” section below.

18. Changes To This Policy

Clinia may update this Privacy Policy from time to time to reflect changes in our services, business operations, legal requirements, privacy practices, or other operational needs.

When we update this Privacy Policy, we will revise the “Last updated” date above. Where required by law or where changes are material, we may provide additional notice, such as by posting a notice on our website, sending a communication, or using another appropriate method. Where a change involves a new or different processing activity that requires consent under applicable law, Clinia will seek consent through an appropriate mechanism.

The updated Privacy Policy will apply from the date it is posted or from another date stated in the updated version.

19. Contact Us

If you have questions about this Privacy Policy or Clinia's privacy practices, or if you wish to submit a privacy request, you may contact us at:

Clinia Health Inc.
Attention: Privacy Officer / Data Protection Officer
221 de la Commune Street West, Suite 210
Montréal, Québec, Canada, H2Y 2C9
Email: legal@clinia.com

If your request relates to Personal Information processed by Clinia on behalf of a customer, please identify the relevant customer where possible. This helps us route the request appropriately. We may refer you to that Customer.

You may also have the right to contact a privacy or data protection authority in your jurisdiction. For Québec matters, this may include the Commission d'accès à l'information du Québec. For Canadian federal private-sector privacy matters, this may include the Office of the Privacy Commissioner of Canada. For EEA or UK matters, this may include your local supervisory authority.

20. Jurisdiction-Specific Notices

The attached notice schedules (the "**Notices**") provide additional information for individuals located in certain jurisdictions or whose Personal Information is subject to specific privacy or data protection laws. These Notices supplement the rest of this Privacy Policy; in case of inconsistency, these Notices prevail only as concerns data subjects to which they apply.

Where more than one privacy law applies to the same processing activity, Clinia will handle Personal Information in accordance with the most stringent applicable requirement.

SCHEDULE 1
Canada

Where the Personal Information Protection and Electronic Documents Act (“**PIPEDA**”) applies, Clinia collects, uses, and discloses Personal Information for purposes that a reasonable person would consider appropriate in the circumstances.

Clinia identifies the purposes for which Personal Information is collected before or at the time of collection, unless otherwise permitted by law. Clinia limits the collection, use, disclosure, and retention of Personal Information to what is reasonably necessary for those purposes or as otherwise permitted or required by law.

Clinia takes reasonable steps to keep Personal Information as accurate, complete, and up to date as necessary for the purposes for which it is used, taking into account the context, sensitivity, and source of the information.

Where consent is required, Clinia seeks meaningful consent appropriate to the nature, context, and sensitivity of the Personal Information involved. Consent may be express or implied, depending on the circumstances and applicable law.

Individuals may request access to Personal Information held by Clinia and may request correction of inaccurate or incomplete Personal Information. Clinia will respond to requests in accordance with applicable law.

Clinia maintains safeguards designed to protect Personal Information against unauthorized access, use, disclosure, alteration, loss, or destruction, taking into account the sensitivity of the information and the purposes for which it is processed.

Where Clinia processes Customer Data on behalf of a customer, the customer is generally responsible for determining the purposes of processing, providing required notices, obtaining required consents or other legal bases, and responding to individual rights requests, unless applicable law or a written agreement provides otherwise.

SCHEDULE 2

Quebec

Where Québec privacy law applies, including the *Act respecting the protection of Personal Information in the private sector*, Clinia handles Personal Information in accordance with applicable Québec privacy requirements.

Clinia maintains privacy governance practices intended to support appropriate handling of Personal Information, including accountability for privacy practices, safeguards, incident response, vendor oversight, and processes for responding to privacy requests.

Where Personal Information is transferred or made accessible outside Québec, Clinia will take steps required by applicable law, which may include assessing relevant privacy factors and using contractual or other safeguards designed to protect the information.

Where Clinia uses technology that includes functions allowing individuals to be identified, located, or profiled, Clinia will provide information required by applicable law and, where required, activate such functions only in accordance with applicable consent or notice requirements.

Where Clinia uses Personal Information to make a decision based exclusively on automated processing and that decision affects an individual, Clinia will provide information required by applicable law, including information about the use of automated processing and the individual's related rights.

If a confidentiality incident involving Personal Information occurs, Clinia will assess and respond to the incident in accordance with applicable law. Where required, Clinia will notify the *Commission d'accès à l'information*, affected individuals, or other required parties, and will maintain required records of confidentiality incidents.

Individuals may request access to or correction of their Personal Information and may exercise other rights available under Québec privacy law, subject to applicable limits. Where required by law, this may include a right to data portability.

Clinia will not treat information as anonymized unless the applicable legal standard for anonymization is met.

The person in charge of the protection of Personal Information is indicated in the section "Contact Us" of this Privacy Policy.

SCHEDULE 3 **EEA / UK GDPR**

Where the EU General Data Protection Regulation, the UK General Data Protection Regulation, or related European data protection laws apply (collectively, the “**GDPR**”), Clinia processes personal data in accordance with applicable GDPR requirements.

Depending on the context, Clinia may act as a controller or as a processor. Clinia generally acts as a controller for personal data processed in connection with our website, business operations, sales and marketing activities, customer communications, recruitment activities, security operations, and internal administration. Clinia generally acts as a processor where we process Customer Data on behalf of a Customer through enterprise services.

Where Clinia acts as a controller, the legal bases for processing may include consent, performance of a contract, compliance with legal obligations, legitimate interests, protection of vital interests, or other legal bases recognized by applicable law. Clinia relies on legitimate interests only where those interests are not overridden by applicable rights and interests of data subjects.

Where Clinia acts as a processor, Clinia processes personal data in accordance with the Customer’s documented instructions, the applicable Customer Agreement, and other applicable privacy or transfer terms.

Subject to applicable conditions and limitations, individuals may have the right to request access, correction, deletion, restriction, objection, portability, withdrawal of consent, and information about automated decision-making or profiling. Individuals may also have the right to lodge a complaint with a competent supervisory authority.

Where personal data is transferred outside the EEA, the United Kingdom, or Switzerland, Clinia uses transfer mechanisms and safeguards required by applicable law. These may include adequacy decisions, standard contractual clauses, the UK international data transfer addendum, transfer impact assessments, contractual safeguards, technical and organizational measures, or other recognized transfer mechanisms.

Where Clinia uses de-identified, aggregated, anonymized, or non-identifiable information for service improvement, analytics, or operational purposes, Clinia will assess whether the information remains personal data under applicable European data protection laws. Information that is pseudonymized or otherwise linkable to an identified or identifiable individual will continue to be handled as personal data.

SCHEDULE 4 **HIPAA**

Where the *Health Insurance Portability and Accountability Act* and its implementing regulations (“**HIPAA**”) apply, Clinia may process protected health information (“**PHI**”) as a Business Associate or subcontractor on behalf of a covered entity or another business associate.

In those circumstances, Clinia handles PHI in accordance with the applicable business associate agreement, HIPAA-specific terms, Customer Agreement, customer instructions and applicable law.

Clinia does not use or disclose PHI except as permitted by the applicable business associate agreement or HIPAA-specific terms, as instructed by the Customer, or as otherwise permitted or required by law.

Where information is derived from PHI, Clinia will treat that information in accordance with the applicable business associate agreement, HIPAA-specific terms, Customer instructions, and applicable law. Clinia will not treat PHI-derived information as de-identified unless the applicable HIPAA de-identification standard has been met or the information is otherwise outside the scope of HIPAA.

The Customer is generally responsible for determining whether HIPAA applies to its use of the services, providing any required HIPAA Notice of Privacy Practices, obtaining required authorizations where applicable, and responding to individual requests relating to PHI.

This Privacy Policy is not a HIPAA Notice of Privacy Practices for any healthcare provider, health plan, healthcare clearinghouse, or other covered entity. Individuals with questions about PHI processed by Clinia on behalf of a Customer should contact the relevant customer directly, unless applicable law or the Customer’s instructions provide otherwise.

SCHEDULE 5

California

Where the *California Consumer Privacy Act*, as amended by the *California Privacy Rights Act*, and its implementing regulations (collectively, the “**CCPA**”) apply, this section provides additional information for California residents.

Depending on the context, Clinia may act as a “business” or as a “service provider” under the CCPA. Clinia generally acts as a business for Personal Information processed in connection with our website, business operations, sales and marketing activities, customer communications, recruitment activities, security operations, and internal administration. Clinia generally acts as a service provider where we process Customer Data on behalf of a customer through enterprise services.

Clinia may collect the categories of Personal Information described in this Privacy Policy, including identifiers, contact information, professional or employment-related information, internet or electronic network activity information, commercial or business relationship information, communications information, recruitment information, and sensitive Personal Information where applicable.

Clinia uses these categories of Personal Information for the purposes described in this Privacy Policy, including to provide and operate services, communicate with individuals, manage customer and business relationships, secure and protect services, improve our website and operations, support recruitment, comply with legal obligations, and protect rights and interests.

Clinia may disclose Personal Information to the categories of recipients described in this Privacy Policy, including affiliates, service providers, subprocessors, customer-directed integrations, professional advisors, legal or regulatory recipients, and parties involved in business transactions.

Clinia does not sell Personal Information. Clinia does not share Personal Information for cross-context behavioral advertising except where permitted by applicable law and described in this Privacy Policy.

Where Clinia processes Customer Data on behalf of a Customer, Clinia does not sell Customer Data or share Customer Data for cross-context behavioral advertising, except where expressly permitted by the applicable Customer Agreement, Customer instructions, and applicable law.

Clinia does not knowingly sell or share Personal Information of individuals under 16 years of age.

Where Clinia uses de-identified or aggregated information, Clinia will maintain and use that information in accordance with applicable CCPA requirements, including requirements intended to prevent re-identification where applicable.

Subject to applicable conditions and limitations, California residents may have the right to:

- know what Personal Information Clinia collects, uses, discloses, sells, or shares;
- request access to Personal Information;
- request deletion of Personal Information;
- request correction of inaccurate Personal Information;
- opt out of the sale or sharing of Personal Information;
- limit the use and disclosure of sensitive Personal Information, where applicable;
- not be discriminated against for exercising CCPA rights.

To exercise these rights, please contact us using the information in the “Contact Us” section below. We may need to verify your identity before responding to your request.

SCHEDULE 6
Other U.S. State Privacy Laws

Residents of certain U.S. states may have additional privacy rights under applicable state privacy laws. Depending on the state and the context of processing, these rights may include the right to request access, correction, deletion, portability, information about processing, opt out of certain targeted advertising, opt out of certain sales of personal data, opt out of certain profiling or automated decision-making, and appeal a decision regarding a privacy request.

Clinia will honor applicable U.S. state privacy rights where required by law.

Clinia does not sell Personal Information. Clinia does not use Personal Information for targeted advertising or cross-context behavioral advertising unless described in this Privacy Policy and permitted by applicable law, including any required consent or opt-out rights.

Where Clinia processes Customer Data on behalf of a Customer, Clinia generally acts as a processor, service provider, or similar role under applicable U.S. state privacy laws. In that role, Clinia does not sell Customer Data or use Customer Data for targeted advertising or cross-context behavioral advertising, except where expressly permitted by the applicable Customer Agreement, Customer instructions, and applicable law. The Customer is generally responsible for determining the purposes and means of processing, providing required notices, obtaining required consents or authorizations, and responding to privacy rights requests, unless applicable law or a written agreement provides otherwise.

Where Clinia uses de-identified, aggregated, or non-identifiable information for service improvement, analytics, or operational purposes, Clinia will do so in accordance with applicable U.S. state privacy law requirements. Clinia will not treat information as de-identified or outside the scope of applicable privacy laws unless the applicable legal standard is met.