

VICLINIC, INC. PRIVACY POLICY NOTICE

Updated: May 19, 2023

We respect your privacy. This section of this Agreement describes our privacy practices regarding personal and medical Information we collect from individuals, including when you visit our offices, websites administered or operated by us, and/or our mobile applications (collectively, the “Sites”).

If you do not agree with all of the terms of this Agreement (including this Privacy Policy Notice “Notice”), you should not use, browse, or otherwise access any of the Sites. By browsing or using any of the Sites, you signify your agreement to this Agreement (including this Privacy Policy).

Definition of Personal and Health Information

For the purposes of this Agreement, “Personal Information” means any information that (i) identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular individual or household; (ii) your past, present, or future physical or mental health or condition, (iii) the provision of health care to you, or (iv) your past, present, or future payment for the provision of health care.

Personal Information does not include publicly-available information from governmental sources. Information that is provided in the aggregate or that is de-identified is not Personal Information.

We are required by law to maintain the privacy of your Personal Information and to provide you with notice of our legal duties and privacy practices with respect to your Personal Information. To the extent required by law, when using or disclosing your Personal Information or when requesting your Personal Information from another covered entity, we will make reasonable efforts not to use, disclose, or request more than the minimum necessary set of your Personal Information or, if needed by us, no more than the minimum amount of Personal Information necessary to accomplish the intended purpose of the use, disclosure, or request, taking into consideration practical and technological limitations.

This Notice of Privacy Practices applies to all of the records of your care generated by Viclinic. When we use or disclose your Personal Information, we are required to abide by the terms of this Notice (or other Notice in effect at the time of the use or disclosure).

Personal Information We May Collect About You – Sources and Categories of Information

Sources of Collection

This section describes the sources from which we may have collected Personal Information about you, and which we may continue to collect. These sources include, but are not limited to: When you visit the Sites or interact with us in other ways, such as when you request information about our Service or information we provide to the public; visit the Sites; or transmit information through the portal we maintain on behalf of our users. For example, when you pay fees, request documents and certificates, submit other inquiries, call, or otherwise engage with us.

Categories of Personal Information Collected

This section describes the categories of Personal Information we may collect about you. Included are categories that describe employee as well as client data. These categories include, but are not limited to:

- Personal identifiers such as name, physical addresses, email addresses, and other contact information, emergency contacts, driver's license number, passport number, marital status, parents' information, account number/username, password, and IP addresses.
- Unique device and online identifiers, such as device IDs, browsing history, and other similar identifiers.
- Protected class information, such as gender, age, disability status, citizenship, medical condition, physical or mental disability information collected in the employment context (not from job applicants). Educational and professional background information, such as work histories, employer information, and educational history that would be found on a resume.
- Audio or visual information, such as passport pictures, or recordings of your calls to us.
- Internet or other electronic network activity, such as information regarding your browsing history, visits to and interaction with our Sites, and information about visits to our social media accounts.

How We Use Personal Information We Collect

This section describes the reasons we may have collected and used Personal Information and why we may continue to collect and use it. These reasons include, but are not limited to:

Providing Services

We use your Personal Information to provide a full range of services, including without limitation: contacting you and responding to your requests and inquiries; facilitating the Service; processing payments; responding to requests for documentation; providing marketing; providing customer service; distributing newsletters and similar materials; improving the Sites; and compliance with applicable laws, regulations, or codes of practice.

Security and Fraud Prevention and Detection

We use information for security purposes such as fraud prevention and detection. We may use Personal Information to enforce our rights, for fraud prevention, or to protect our company, affiliates, our customers, the Sites, or a third-party website or platform.

Compliance with Laws and to Protect Ourselves

We use your Personal Information to support auditing, legal, and compliance purposes including responding to court orders or subpoenas. We may also share your Personal Information if a government agency or investigatory body requests. We may also use your Personal Information when we are investigating potential fraud or other areas of concern or if we believe in good faith that disclosure is legally required or otherwise necessary to protect our rights and property, or the rights, property, or safety

Marketing and Recruiting

We use Personal Information to inform you about Viclinic, Inc. and the services we offer. We may also use your Personal Information to send you information about career opportunities.

Employment and Human Relations Functions

We use Personal Information in connection with our hiring, employment, and job training activities.

Communications

We use Personal Information to communicate with you about your account or our relationship with you. We may contact you about your use of our Sites. We may contact you about your account or feedback. We might also contact you about this Agreement.

To Avert a Serious Threat to Health or Safety

Viclinic may use and disclose your Personal Information when necessary to prevent a serious threat to your health and safety, or to the health and safety of the public or another person. Any disclosure would only be to someone able to help prevent the threat or to the extent necessary to comply with state and federal laws to prevent or control disease, injury, or disability regarding public health.

Debug and Identify Errors

We use your Personal Information to debug and identify and repair errors that impair existing intended functionality.

Statistical Analysis and Research

We may use your Personal Information for statistical analysis and research purposes including analyzing performance.

Other

We may use your Personal Information as otherwise described or permitted by law, for any other purpose as described in this Agreement, or as we may notify you.

In addition, we may use your Personal Information in the aggregate and in a de-identified manner to create case studies, and/or to determine residents' demographics and preferences. By doing so, we are better able to deliver to you relevant information that you may find to be helpful and informative.

OTHER PERMITTED AND REQUIRED USES AND DISCLOSURES OF PERSONAL INFORMATION THAT MAY BE MADE WITHOUT YOUR AUTHORIZATION OR OPPORTUNITY TO AGREE OR OBJECT

Required by law

We may use or disclose your personal information to the extent that the use or disclosure is required by federal, state, or local laws or regulations. The use or disclosure will be made in compliance with the law

or regulation and will be limited to the relevant requirements of the law or regulation. You will be notified, if required by law or regulation, of any such uses or disclosures.

Health oversight activities

We may disclose your personal information to a health oversight agency for activities authorized by law. These oversight activities include, for example, audits, investigations, inspections, and licensure. These activities are necessary for the government to monitor the health care system, government programs, and compliance with civil rights laws.

Victims of abuse, neglect, or domestic violence

We may disclose your personal information to a public health authority that is authorized by law to receive reports of child or elder abuse or neglect. In addition, we may disclose your personal information if we believe that you have been a victim of abuse, neglect, or domestic violence to the governmental entity or agency authorized to receive such information. In this case, the disclosure will be made consistent with the requirements of applicable federal and state laws.

Legal proceedings

We may use and disclose personal information in responding to a court or administrative order, subpoena, or discovery request. We may also use and disclose your personal information to the extent permitted by law without your authorization, for example, to defend a lawsuit or arbitration.

Law enforcement

We may disclose your personal information to the police or other law enforcement officials as required or permitted by law: (1) in response to a court order, subpoena, warrant, summons, or similar process; (2) to identify or locate a suspect, fugitive, material witness, or missing person; (3) to notify them about the victim of a crime if, under certain limited circumstances, we are unable to obtain the person's agreement; (4) to notify them about a death we believe may be the result of criminal conduct; (5) to notify them about criminal conduct at Viclinic or with one of our health care providers; and (6) in emergency circumstances, to report a crime, the location of a crime or the victims of a crime, or the identity, description, or location of the person who committed the crime.

Food and drug administration

We may disclose your personal information to a person or company required by the food and drug administration for the purpose of quality, safety, or effectiveness of FDA-regulated products or activities including to report adverse events, to report product defects or problems, to report biologic product deviations, to track products, to enable product recalls, to make repairs or replacements, or to conduct post marketing surveillance, as required.

Decedents, coroners, funeral directors, and organ donation

We may disclose your personal information to a coroner or medical examiner for identification purposes, determining cause of death, or for the coroner or medical examiner to perform other duties authorized by law. We may also disclose your personal information to a funeral director, as authorized by law, in order to permit the funeral director to carry out their duties. We may also disclose such information in reasonable anticipation of your death. Your personal information may additionally be used and disclosed for cadaveric organ, eye, or tissue donation purposes.

Research that does not involve your treatment

We may disclose your personal information to researchers when their research has been approved by an institutional review board that has reviewed the research proposal and established protocols to ensure the privacy of your personal information. When a research study does not involve any treatment, we may disclose your personal information to researchers. To do this, we will either ask your permission to use your personal information or we will use a special process that protects the privacy of your personal information. In addition, we may use information that cannot be identified as your personal information, but that includes certain limited information (such as your date of birth and dates of service). We will use this information for research, quality assurance activities, and other similar purposes and we will obtain special protections for the information disclosed.

Military activity and national security

We may use and disclose your personal information to units of the government with special functions, such as the U.S. military or the U.S. department of state, under certain circumstances. We may use and disclose your personal information to authorized federal officials for intelligence, counterintelligence, and other national security activities authorized by law. We may use and disclose your personal information to authorized federal officials so they may provide protection to the president, other authorized persons, or foreign heads of state, or conduct special investigations.

Criminal activity

Consistent with applicable federal and state laws, we may disclose your personal information if we believe that the use or disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public. We may also disclose your personal information if it is necessary for law enforcement authorities to identify or apprehend an individual.

Inmates

If you are an inmate of a correctional institution or under custody of a law enforcement official, we may disclose your personal information to the correctional institution or the law enforcement official. This is necessary for the correctional institution to provide you with health care, to protect your health and safety and the health and safety of others, and to protect the safety and security of the correctional institution.

Public health risks

We may disclose your personal information for public health activities. These activities generally include the following: to prevent or control disease, injury, or disability; to report births and deaths; to report reactions to medications or problems with products; to notify people of recalls of products they may be using; and to notify a person who may have been exposed to a disease or may be at risk for contracting or spreading a disease or condition. We will only make this disclosure when required or authorized by law or if you authorize such disclosure.

Workers' compensation

We may disclose your personal information as authorized to comply with workers' compensation laws and other similar legally-established programs.

Third Parties With Which We May Share Personal Information

We may share Personal Information with third parties for business purposes. These third parties include, but are not limited to:

- **For business purposes.** We may share your Personal Information with vendors and service providers, including our data hosting and data storage partners, analytics and advertising providers, technology services and support, and data security. We also may share Personal Information with professional advisors, such as auditors, law firms, and accounting firms. We may disclose your name, email address, date of birth, phone number, and address if you provided it to us via a form on the website or during an incomplete or failed registration to service providers.
- **With your direction or consent.** We may share your Personal Information with third parties if you request or direct us to do so. This includes your use of social media widgets on our Sites.
- **With affiliates within our corporate group.** We may share your Personal Information with any subsidiaries within our corporate group.
- **Compliance with law.** We may share your Personal Information to comply with applicable law or any obligations thereunder, including cooperation with law enforcement, judicial orders, and regulatory inquiries.
- **In the context of a transaction.** We may share your Personal Information connection with an asset sale, merger, bankruptcy, or other business transaction.
- **For other business reasons.** We may share your Personal Information to enforce any applicable Terms of Use, and to ensure the safety and security of the Sites and/or our users.

We also may disclose de-identified information. Note that if you make any Personal Information publicly available on the Sites, anyone may see and use such information.

USES AND DISCLOSURES OF PERSONAL INFORMATION BASED UPON YOUR WRITTEN AUTHORIZATION

Other uses and disclosures of your Personal Information will be made only with your written authorization, unless otherwise permitted or required by law as described in this Notice. You may revoke this authorization in writing at any time. If you revoke your authorization, we will no longer use or disclose your Personal Information for the reasons covered by your written authorization. Please

understand that we are unable to take back any disclosures already made with your authorization, and we are required to retain our records of the care we provide to you. If you are not present or able to agree or object to the use or disclosure of the Personal Information, then your provider may, using professional judgement, determine whether the disclosure is in your best interest.

YOUR RIGHTS REGARDING YOUR PERSONAL INFORMATION

You have the following rights with respect to your Personal Information. You may contact Viclinc to obtain additional information and instructions for exercising the following rights.

You have the right to inspect and copy your Personal Information

You may request access to your medical and billing records maintained by us, for so long as we maintain such information. You may inspect and request copies of the records. Under federal law, however, you may not inspect or copy the following records: psychotherapy notes; information compiled in reasonable anticipation of, or use in, a civil, criminal, or administrative action or proceeding; and laboratory results that are subject to law that prohibits access to Personal Information. Under such limited circumstances, we may deny you access to a portion of your records. If you are denied access to your Personal Information, you may request that the denial be reviewed. Another licensed health care professional chosen by us will review your request and the denial. The person conducting the review will not be the person who denied your request. We will comply with the outcome of the review. Please contact support@viclinic.com if you have questions about access to your Personal Information. If you desire access to your records, you must submit your request in writing. If your medical information is maintained in an electronic health record, you may obtain an electronic copy of your medical information and, if you choose, instruct us to transmit such copy directly to an entity or person you designate in a clear, conspicuous, and specific manner. If you request paper copies, we will charge you for the costs of copying, mailing, labor, and supplies associated with your request. Our fee for providing you an electronic copy of your medical information will not exceed our labor costs in responding to your request for the electronic copy (or summary or explanation). You should take note that, if you are a parent or legal guardian of a minor, certain portions of the minor's Personal Information will not be accessible to you (for example, records pertaining to health care services for which the minor can lawfully give consent and therefore for which the minor has the right to inspect or obtain copies of the record, or where the health care provider determines, in good faith, that access to the records requested by the representative would have a detrimental effect on the provider's professional relationship with the minor or on the minor's physical safety or psychological well-being).

You have the right to request a restriction of your Personal Information

You may ask us not to use or disclose any part of your Personal Information for the purposes of treatment, payment, or health care operations. You may also request that any part of your Personal Information not be disclosed to family members or friends who may be involved in your care or for notification purposes, such as assisting in the notification of such individuals regarding your location and general condition. While we will consider all requests for additional restrictions carefully, we are not required to agree to a requested restriction, unless the disclosure is to a health plan for a payment or health care operation purpose and the medical information relates solely to a health care item or service for which we have been paid out-of-pocket in full. Your request must state the specific restriction requested and to whom you want the restriction to apply. This request must be in writing. We will send you a written response.

You have the right to request to receive confidential communications

You may request to receive your Personal Information by alternative means of communication or at alternative locations. For example, you can request that we only contact you at work or by mail. To request confidential communications, you must make your request in writing. We will not ask you for the reason for your request. We will accommodate all reasonable requests. Your request must specify how or where you wish to be contacted.

You have the right to amend your records

You have the right to request that we amend personal information maintained in your medical or billing records generated by us or our providers. If you desire to amend your records, your request must be in writing. We will comply with your request unless we believe that the information that would be amended is accurate and complete or other special circumstances apply. If we deny your request, you will be permitted to submit a statement of disagreement for inclusion in your records. You have the right to add a 250-word document addendum to your personal information.

You have the right to receive an accounting of disclosures.

Upon written request, you may obtain an accounting of certain disclosures of your personal information made by us during any period of time six years prior to the date of your request, except that for requests made on or after January 1, 2011 that relate to treatment, payment, or health care operation disclosures from our electronic health record system, the accounting period is three years. Your written request should indicate in what form you want the list (for example, on paper or electronically). If you request an accounting more than once during a twelve month period, we will charge you for the costs involved in fulfilling your additional request. We will inform you of such costs in advance, so that you may modify or withdraw your request to save costs. In addition, we will notify you as required by law if there has been a breach of the security of your personal information.

You have the right to obtain a paper copy of this notice

Upon request, you may obtain a paper copy of this notice. Even if you have agreed to receive such notice electronically, you are still entitled to a paper copy of this notice. To obtain a paper copy of this notice, please contact support@viclinic.com .

Social media

In order to maintain a professional relationship consistent with professional standards, Medical Providers are not permitted to have interactions and communications with patients outside of the normal practices necessary for treatment. Interactions and communications between Members and Medical Provides must adhere to applicable federal and state laws and be supported by the Medical Provider's code of ethics. Member and Medical Providers are required to respect the privacy of each other's presence on social media and to maintain strict professional boundaries and an overall professional relationship focused on treatment.

Protocol for communications

All communications between Members and Medical Providers must occur via phone or the use of the Viclinic secure platform. In the event a Members needs to reach a Medical Provider prior to the next scheduled session to communicate information that is of importance to the scheduling of the next session, treatment, or for another Member reason, member should contact support@viclinic.com during normal business hours. If Viclinic cannot assist with the matter, Viclinic will send an email to the Medical Provider requesting assistance. However, a Medical Provider's response may take up to 72 hours.

We Do Not Sell Your Personal Information

We do not and will not sell Personal Information. However, we may disclose your personal information to our subsidiaries, affiliates, service providers, business partners, and other third-party processors to provide you with Services.

Please be aware that the information that you choose to post to a public area of the Services, will not be protected by this Privacy Policy because you have made an active choice to make that information public.

VICLINIC IS NOT RESPONSIBLE FOR PROTECTING ANY PERSONAL INFORMATION YOU CHOOSE TO SUBMIT IN ANY PUBLIC AREA OF THE SERVICES.

Additional Information Regarding Our Collection, Use, and Sharing of Personal Information

We may also collect and share Personal Information with third parties to comply with legal obligations; when we believe in good faith that an applicable law requires it; at the request of governmental authorities or other third parties conducting an investigation; to detect and protect against fraud, or any technical or security vulnerabilities; to respond to an emergency; or otherwise to protect the rights, property, safety, or security of our business, third parties, visitors to the Sites, or the public. We may also share Personal Information with any person to whom we transfer any of our rights or obligations under any agreement, or in connection with a sale, merger, or consolidation of our business or other transfer of our assets, whether voluntarily or by operation of law, or who is otherwise deemed to be our successor or transferee.

Do Not Track

"Do Not Track" is a privacy preference that users can set in certain web browsers. We do not comply with automated browser signals regarding tracking mechanisms, which may include "do not track" instructions.

California Data Privacy Rights

If you are a California resident, you may have certain rights with respect to Personal Information as set forth under California law and explained below.

Shine the Light

California Civil Code Section 1798.83, also known as the "Shine the Light" law, permits California

residents to annually request, free of charge, information about the Personal Information (if any) disclosed to third parties for direct marketing purposes in the preceding calendar year. We do not share Personal Information with third parties for their own marketing purposes.

CCPA Rights of Individuals

This section addresses rights provided to California residents under the California Consumer Privacy Act of 2018 (“CCPA”) regarding the Personal Information we collect. Those rights include the right to know about the Personal Information we collect, the right to request that we delete it, and the right to request that we refrain from selling any Personal Information (the “CCPA Rights”). The CCPA Rights are described in greater detail below.

Your Right To Request Disclosure of Information We Collect and Share About You

You can request the following information from us, with respect to the Personal Information that we have collected about you in the 12 months prior to our receipt of your request:

- The categories of Personal Information we have collected about you
- The categories of sources from which we collected your Personal Information
- The business or commercial purposes for which we collected the Personal Information
- The categories of third parties with which we shared your Personal Information
- The categories of Personal Information we have disclosed or shared for a business purpose
- The specific pieces of Personal Information we collected

Your Right To Request Deletion of Personal Information We Have Collected From You

Upon request, we will delete the Personal Information we have collected about you that is covered by the CCPA, situations where the CCPA authorizes us to retain specific information, including when it is necessary for us to provide you with a good or service that you requested; perform a contract we entered into with you; maintain the functionality or security of our systems; or comply with or exercise rights provided by the law. The law also permits us to retain specific information for our exclusively internal use, but only in ways that are compatible with the context in which you provided the information to us or that are reasonably aligned with your expectations based on your relationship with us.

We Are Service Providers to Our Clients

When we collect and process Personal Information on our clients, we act as their “service provider,” as that term is defined in the CCPA. We do not disclose, use, or retain any of the Personal Information we collect when collecting or processing Personal Information on behalf of our clients for any purpose other than the specific purpose of performing the services specified in our contracts with our clients. This means that the Company does not own the Personal Information we collect on behalf of our clients.

Exercising Your Rights and How We Will Respond

To exercise any of the rights above, or to ask a question, you may contact us using the contact information provided on our Sites.

For requests for access or deletion, we will first acknowledge receipt of your request within 10 days of

receipt of your request. We provide a substantive response to your request as soon as we can, generally within 45 days from when we receive your request, although we may be allowed to take longer to process your request in certain jurisdictions or under certain circumstances. If we expect your request is going to take us longer than normal to fulfill, we will let you know.

Verification of Identity – Access or Deletion Requests

If we are unable to verify your identity with the degree of certainty required based on the type of information or action you are requesting, we will not be able to respond to the request. We will notify you to explain the basis of the denial.

Authorized Agents

You may designate an agent to submit requests on your behalf. The agent can be a natural person or a business entity that is registered with the California Secretary of State.

If you would like to designate an agent to act on your behalf, you and the agent will need to comply with our agent verification process. You will be required to verify your identity by providing us with certain Personal Information as described above, depending on whether you hold an account with us or not and the nature of the information you require, which we will endeavor to match the information submitted to information we maintain about you. Additionally, we will require that you provide us with written confirmation that you have authorized the agent to act on your behalf, and the scope of that authorization. The agent will be required to provide us with proof of the agency relationship, which may be a declaration attesting to the agent's identity and authorization by you to act on their behalf, signed under penalty of perjury. If the agent is a business entity, it will also need to submit evidence that it is registered and in good standing with the California Secretary of State. Information to identify and verify your agent can be submitted through the same mechanism and at the same time that you submit information to verify your identity.

Please note that this subsection does not apply when an agent is authorized to act on your behalf pursuant to a valid power of attorney. Any such requests will be processed in accordance with California law pertaining to powers of attorney.

Requests for Household Information

There may be some types of Personal Information that can be associated with a household (a group of people living together in a single dwelling). Requests for access or deletion of household Personal Information must be made by each member of the household. We will verify each member of the household using the verification criteria explained above.

If we are unable to verify the identity of each household member with the degree of certainty required, we will not be able to respond to the request. We will notify you to explain the basis of our denial.

Our Commitment to Honoring Your Rights

If you exercise any of your rights described in this Agreement, including any CCPA Rights you may have, we will continue to treat you fairly and you will not be denied or charged different prices or rates for goods or services, or provided a different level or quality of goods or services than others.

Personal Information of Minors

Our Sites are intended for use by parents and guardians and children, including children under the age of 13. Viclinic, Inc. will handle children's personal information as described in the COPPA Policy ("COPPA Policy" at Viclinic [COPPA Policy link](#)). The COPPA Policy is incorporated by referenced into this Privacy Policy and Terms of Service.

Social Features

Certain features of the Sites permit you to initiate interactions between the Sites and third-party services or platforms, such as social networks ("Social Features"). Social Features include features that allow you to click and access Viclinic's pages on certain third-party platforms, such as Facebook, Twitter and LinkedIn as applicable, and from there to "like" or "share" our content on those platforms. Use of Social Features may entail a third party's collection and/or use of your data. If you use Social Features or similar third-party services, information you post or otherwise make accessible may be publicly displayed by the third-party service you are using. Both Viclinic and the third party may have access to information about you and your use of both the Sites and the third-party service.

Third Party Sites

From time to time, we may advertise certain third party services through our Sites which we feel will be helpful or relevant to you (collectively, "Third Party Services").

When you click on a link for a Third Party Service, your web browser will be re-directed to the third party provider of the Third Party Service that you selected. Third party providers may have privacy policies that are different than this Agreement, and you should read carefully the privacy policies of those vendors prior to releasing any of your information to them, financial or otherwise.

Third Party Services may also require you to agree to certain terms and conditions of use (collectively, "Third Party Conditions") before using or accessing those services. Often, Third Party Conditions describe and govern how third party providers use your Personal Information, so you should read carefully all Third Party Conditions prior to releasing any of your information to such third party sites.

We do not endorse, warrant, or guaranty the nature, scope, quantity, availability, or quality of any Third Party Services. We make you aware of such services solely for your convenience. If you have any questions, comments, or concerns about any Third Party Service, you are instructed to contact directly the vendor offering the service.

Security

We implement and maintain reasonable security appropriate to the nature of the Personal Information that we collect, use, retain, transfer, or otherwise process. Our reasonable security program is implemented and maintained in accordance with applicable law and relevant standards; however, there is no perfect security, and reasonable security is a process that involves risk management rather than risk elimination. While we are committed to developing, implementing, maintaining, monitoring, and updating a reasonable information security program, no such program can be perfect; in other words, all risk cannot reasonably be eliminated. Data security incidents and breaches can occur due to

vulnerabilities, criminal exploits, or other factors that cannot reasonably be prevented. Accordingly, while our reasonable security program is designed to manage data security risks and thus help prevent data security incidents and breaches, it cannot be assumed that the occurrence of any given incident or breach results from our failure to implement and maintain reasonable security.

Accuracy & Access

Your Personal Information is accurate to the extent that you provide it correctly and accurately to us or to the party collecting such information. Errors that you make when entering your Personal Information may result in erroneous information in our database. We provide the ability to review and/or correct information.

To protect your privacy and security, we may take reasonable steps to verify your identity, such as requiring a password and user ID, before we permit any changes to be made to the Personal Information in our database. To view and change the Personal Information that you directly provided to us, contact us using the information provided on our Sites.

Changes to this Agreement

We reserve the right to amend, alter, or otherwise change this Agreement in our sole and absolute discretion.

Contact Us

If you have any questions about this Agreement, or to request a copy of this Agreement in another format, you may email support@viclinic.com.

When contacting the Privacy Officer please be sure to provide your name, your physical address, your email address, your phone number (if you wish to be contacted by telephone), and a description of the question or issue that you wish to have resolved.

COPPA PRIVACY POLICY

Children's Online Privacy Protection Act

Last modified: May 2023

Viclinic, Inc. ("Viclinic") values the privacy of children and of all of its users. This COPPA Privacy Policy ("COPPA Policy") is designed to comply with the Children's Online Privacy Protection Act ("COPPA") and contains important information about how we collect, use, and disclose the personal information we

collect from or about children under thirteen (13) years old who use our website, (the “Site”) and the services provided on our Site (the “Services”).

Viclinic is assisting children and their parents with connecting to their Healthcare Provider.

Viclinic will handle children’s personal information as described in this COPPA Policy. Any personal information we collect about other users (e.g., teens and adults) will be treated in accordance with the Viclinic Privacy Policy (“Privacy Policy”). The use of our Site and any dispute over privacy, is subject to this COPPA Policy, the Privacy Policy, and our Terms of Service, including its applicable limitations on damages and the resolution of disputes. Our Terms of Service and Privacy Policy are incorporated by reference into this COPPA Policy.

Who Will Collect Information About Children?

Viclinic operates the Site and Services and will collect children’s personal information as described in this COPPA Policy and our Privacy Policy. We can be contacted at: support@viclinic.com.

Even if Viclinic Services are offered in conjunction with an outside partner, the partner will not receive any individual personal information from users of the Site, including children. Viclinic may provide partners with aggregate or de-identified information about users.

What Information Do We Collect About Children and Why?

As described in further detail below, we collect some personal information from or about children to accurately manage the child’s medical need. Data is retained for provision of the Medical Services only.

How Information is Collected?

We may collect information about children directly from the child’s parent or guardian, as well as automatically through a child’s use of our Site and Services. We will not require a child to disclose more information than is reasonably necessary to use our Services.

Information We Collect Directly

From children under 13, we only use child's name to provide the Services. We will not contact a child using his or her email address or username. Parents may ask us to stop collecting personal information from their child by emailing us at support@viclinic.com, however, in such cases the child will not be able to utilize the Services. If a parent directs us to stop collecting and using a child's personal information, we must disable his or her use of our Services to ensure that no information is collected.

Information We Collect Automatically

We may automatically collect the following information about a child's use of our Site through cookies and other technologies: domain name; browser type and operating system; web pages viewed; links clicked; the length of time spent on our Site; Google Analytics statistics; the referring URL, or the webpage that led the child to our Site; language information; device name and model; operating system type, name, and version; and activities within our Site. We may also collect IP address, device identifier or a similar unique identifier from users of our Site, including children; we only use such identifiers to support the internal operations of our Site and we do not use such identifiers to collect information about the child outside of our Site

How We Use Children's Information

We use personal information collected from children for the following purposes:

- To provide our Services; and
- To respond to customer service and technical support issues and requests.

We de-identify and/or aggregate the information we collect from children under 13 before we use it for any other purposes, as noted below.

Unique Identifiers. We only collect and use unique identifiers, such as IP addresses, as necessary to operate our Site or Services, including to maintain or analyze their functioning; perform network communications; authenticate users or personalize content; and protect the security or integrity of users and our Site and Services. We never use unique identifiers to track users across third-party apps or websites.

Aggregate or De-identified Information. We may use aggregate or de-identified information about children for research, analysis, and similar purposes. When we do so, we strip out names, e-mail, contact

information, and other personal identifiers. We may use aggregate or de-identified information for the following purposes:

- To better understand how users access and use our Site and Services;
- To improve our Site and Services and respond to user desires and preferences; and
- To conduct research or analysis, including research and analysis by third parties.

How We Share Children’s Information

We do not sell children’s personal information, and a child may not make his or her personal information public through our services. In general, we may disclose the personal information that we collect about children to provide our Services, to comply with the law, and to protect Rocket Visa and other users of our Services. For example, we may share children’s personal information as follows:

- Service Providers. We may disclose the information we collect from children to third-party vendors, service providers, contractors, or agents who perform functions on our behalf.
- Business Transfers. If we are acquired by or merged with another company, if substantially all of our assets are transferred to another company, or as part of a bankruptcy proceeding, we may transfer the personal information we have collected from our users to the other company.
- In Response to Legal Process. We also may disclose the personal information we collect in order to comply with the law, a judicial proceeding, court order, subpoena, or other legal process.
- To Protect Us and Others. We also may disclose the personal information we collect where we believe it is necessary to investigate, prevent, or take action regarding illegal activities, suspected fraud, situations involving potential threats to the safety of any person, violations of our Terms of Service, Privacy Policy, or this COPPA Policy, or as evidence in litigation in which Rocket Visa is involved.
- With Parents. Parents may request information about the information we have collected from their child by contacting us at support@viclinic.com.
- Aggregate and De-Identified Information. We may also use and share aggregate or de-identified information about users with third parties for marketing, research, or similar purposes.

Your Rights to Review, Delete, and Control Our Use of Children’s Personal Information

Parents have a right to review the information we have collected about their children and students, respectively, and to delete it, and to tell us to stop using it. To exercise these rights, you may contact us at support@viclinic.com. You will be required to authenticate yourself as the child’s parent to receive

information about that child. Please note that copies of information may remain in cached or archived form on our systems after you request us to delete it.

Changes to This COPPA Policy

This COPPA Policy is current as of the Effective Date set forth above. We may change this COPPA Policy from time to time, so please be sure to check back periodically. We will post any changes to this COPPA Policy on our Site, at support@viclinic.com. If we make any changes to this COPPA Policy that materially affect our practices with regard to the personal information we have previously collected from a child, we will endeavor to provide you with notice in advance of such change by highlighting the change on our Site.