Patient Prism LLC
Privacy Policy
Effective 1-June-2025

1. Introduction

This Privacy Policy (this "Policy") describes our practices regarding the information Patient Prism, LLC ("Prism", "we", "our", "us") may collect from you or that you may provide to us when you browse our website (the "Site") or use or products and services (collectively, the "Services"). It also addresses information we may collect on behalf of our clients from their customers.

By visiting the Site, submitting an inquiry to us, signing up for our newsletter, using the Services, or otherwise interacting with us regarding the Services, you represent to us that you have read, understand and agree to the practices described in this Policy. Please note, however, that not all of our uses of information are based on your consent. In some cases, we have other legal bases for collecting and using information, as further described in this Policy. For example, we may be obligated to collect and use some information under the terms of a contract between us and the organization you work for or of which you are a customer or other end user.

If you are an employee, representative or customer of one of our clients, please note that this Policy is part of our client agreement.

If you have questions or concerns about this Policy or our collection and use of your information, please contact us at the address listed below, and we will be happy to address them. If you are an employee or other representative of one of our clients, or if you are a customer of one of our clients, we may direct your question or concern to that client.

2. Applicability

In this Policy, certain terms have specific meanings, as follows:

> "Client Account Data" means information, including Personal Data, relating to your business relationship to us as a Prism client or as an employee or representative of a Prism client for purposes of establishing and maintaining that business relationship, such as your business contact information, role, billing information, access credentials, or other business records.
>
> "Client Content" means information, including Personal Data, relating to interactions and communications between our clients and their customers or personnel in connection with the client's business.
>
> "Client Usage Data" means information, including Personal Data, relating to the use of the Site and/or the Services, such as metadata, operational information, call or messaging logs, data routing information, API requests, origin and termination points (i.e., to/from numbers), and other logging or measurement data associated with the use of the Services.

"Data Protection Laws" means laws and regulations that apply to us or to our clients with respect to our collection and use of your Personal Data. Data Protection Laws may include the U.S. Health Insurance Portability and Accountability Act ("HIPAA"), the EU General Data Protection Regulation and/or its Swiss or U.K. equivalents (individually and collectively, "GDPR"), the California Consumer Privacy Act, as amended ("CCPA"), the Canada Personal Information Protection and Electronic Documents Act and/or superseding Canadian provincial laws (collectively, "PIPEDA"), or other laws and regulations. In some cases, Data Protection Laws may not apply directly to us, but they may apply to our clients, and our obligations relating to those laws are specified in our written agreements with our clients.

"Personal Data" means information in our possession or control that can be used to identify you (such as your name, email address or other contact information) and other information that is linked to your personal identifiers (such as your specific use of our website or our products and services). Personal Data also means any data that is included in the definition of Personal Data (or similar term, such as "Personal Information") under Data Protection Laws.

This Policy applies only to information that is Personal Data collected by us or provided to us through your use of the Site or the Services. For example, if we create aggregated anonymous data that cannot be used by someone else to identify you, that data is not covered by this Policy. This Policy also does not apply to information we may obtain from other sources, to other applications or services that do not link to this Policy, or to the practices of any third parties (including the practices of any of our clients).

3. Changes

We may update this Policy from time to time. Whenever we do so, we will include the applicable effective date at the top of the page. If you are a registered user of the Services or a registered representative of one of our clients, we will notify you, through reasonable means, such as email or via a notice on our platform sign-in area, that we have updated this Policy. Except as otherwise expressly agreed by us in writing, the most recent version of this Policy applies to all uses of the Site and the Services.

4. Information We Collect and the Purposes of Collection

4.1. Information You Choose to Give to Us

In some areas of the Site, you can request a demo of our products or sign up for our mailing list. We collect the information you provide in order to fulfill your request. We may also put out surveys or participate in or host events, and if you respond to the survey or express interest in or sign up for the event, we will collect the information you provide for the reason you provided it.

We may also use your email address, if you have provided it to us, to send you information about the Services or events that you might be interested in. You can choose not to receive

marketing communications from us at any time by following the unsubscribe instructions in any such communication or by contacting us at the address listed below.

4.2. Client Account Data.

We collect Client Account Data in the course of establishing and managing our business relationship with our clients. For example, we collect the names, roles, and business contact information of individual representatives of our clients when we interact with them, such as to negotiate an agreement, establish admin and user accounts, set up billing or client support contacts, and otherwise manage our relationship. In some cases, Client Account Data may be collected directly by one of the service providers we use to help us deliver the Services, such as a payment processing provider.

We also collect information from you when you interact with our client support, sales or account management teams, and we use the information we collect from you to help you with your questions or whatever the interaction is about so that we can serve your needs.

If you provide us with a physical address in order to obtain a telephone number for which we are required to have your physical address on file, we will use that address to confirm we can assign that number to you. We may also check the physical address you provide and/or your billing address, as well as other information you provide or that we obtained from your use of the Services about your identity such as your name, email address, and IP address, with our fraud prevention and identity validation providers (to confirm you have provided us with accurate details). We may also use your address information to calculate taxes. We may also have to share these addresses with the telecommunications provider from whom we obtained the phone number or local authorities upon their request.

We use Client Account Data to carry out our obligations under our client contracts and for our legitimate interests, including:

- Establishing and managing our relationship with our clients, including recognizing you when you communicate to us through our user portals, communicating with you about your account, authenticating your user credentials, or responding to your inquiries;
- Carrying out our core business operations, such as billing, accounting, filing taxes, and fulfilling regulatory obligations;
- Understanding who our clients and potential clients are and their interests in the Services;
- Improving our internal processes and the Services, or training our personnel;
- Helping to detect, prevent, or investigate security incidents, fraud or misuse of the Site and the Services; and
- Complying with regulatory requirements.

4.3. Client Usage Data

When you use the Services, we collect Client Usage Data. We use Client Usage Data to carry out our obligations under our client contracts and for our legitimate interests, including:

- Providing the Site and the Services;
- Responding to your requests, including support requests;
- Allowing our clients to monitor and manage the use of the Services they have purchased from us;
- Managing and routing communications traffic, including Client Content;
- Supporting our billing and accounting operations;
- Understanding, maintaining and improving the Site and the Services and training our personnel;
- Helping our clients understand how their personnel and customers use the Services;
- De-identifying and aggregating data for statistical and analytic purposes;
- Helping to detect, prevent, or investigate security incidents, fraud or misuse of the Site and the Services; and
- Complying with regulatory requirements.

4.4. Client Content

We collect Client Content that our clients ask us to collect as part of the Services. In general, Client Content is transmitted between our clients and their customers or personnel through the use of Services, like the body of a text message or phone call.

We may collect Client Content from you in connection with your use of the Services. For example, if you use our messaging services, we collect the messages being sent and received so that we can convey those messages to and from the carrier networks and cause the content to be available in your account portal and in our API. Similarly, to transmit voice calls to and from the telecommunications carrier networks, we have to collect the voice communications being sent and received to route them appropriately, and then cause that information to be available in our portal and our API. You can also use the Service to record voice communications or have them transcribed, in which case, we will also collect those voice recordings or transcriptions.

If you are using our tracking code on your website, we also collect on your behalf the information about the visitors to your website such as their IP address, their landing page, referring URL, and the online ads that led them to your website. The tracking code uses cookies to identify the visitors to your websites so that the tracking code can display the correct tracking number to your end users and associate phone, form, or text activity to the correct website visit.

If you are using caller ID services that we make available through a third-party service provider, we will collect information about your end users such as the caller's name, phone number, and the city in which the phone number is registered (not available in all countries or for all phone numbers). In addition, if we make a premium caller ID service available through a third-party service provider, then for clients who elect to use the premium caller ID service, we will collect address and other available demographic information about a caller.

We use Client Content to:

- Provide the Services our clients request;
- Deliver communications to their intended destination;
- Record or transcribe communications according to client instructions;
- Provide reporting on communications programs to our clients;
- Understand, maintain and improve the Services and train our personnel;
- De-identifying and aggregating data for statistical and analytic purposes; and
- Detect, prevent, or investigate security incidents, fraud or misuse of the Services.

Please note that our clients have control over which Client Content they want us to collect as well as what they do with that Client Content. We provide the tools to collect the Client Content, and we use Client Content for the limited purposes listed above. If you are an end user or customer of one of our clients and you believe that your Personal Data is being collected by that client through the Services, you should review that client's terms of service and/or privacy policy to find out how they collect, use, store, and share your Personal Data. We are not responsible for our clients' privacy policies or privacy practices.

You must not use the Site or the Services to receive, send, or otherwise process Protected Health Information ("PHI"), as defined under HIPAA, unless you have a Business Associate Agreement ("BAA") in place with us. Prism disclaims all liability for PHI sent, received, or processed through the Site or the Services without an appropriate BAA in place.

Please contact our sales team to discuss HIPAA-compliant uses of the Services.

4.5. Information We Collect Automatically

We may use various tracking technologies to collect information, and this may include sending cookies to you. Cookies are small data files stored on your hard drive or in device memory that help us to improve the Services and your experience, to see which areas and features of the Services are used more or less in relation to other areas and features, to count visits. Certain cookie technologies are employed to make the Services function for their intended purposes. By choosing to use our Services after having been notified of our use of such cookie technologies in the ways described in this Policy, and, in applicable jurisdictions, through notice and unambiguous acknowledgement of your consent, you agree to such use. Please note that if you set your browser to disable cookies, some of our Services may not work or function properly or with full functionality.

We use the following types of cookies:

- **Essential**: cookies required for access to the Site or web-based areas of the Services and for the core functionality of the Site and those areas of the Services.
- **Behavioral/Analytical**: cookies used to gather behavioral information through the Site or web-based areas of the Services, provide customized content and recommendations, and analytics.
- **Marketing/Retargeting**: cookies that are used to deliver relevant advertising or track the source of referrals to the Site.

Additionally we may use the following tracking technologies to improve the Services:

- **Web beacons**: also known as "pixel tags" or "clear GIFs" to track when some of our emails are accessed or opened or when certain content is viewed or clicked. The statistics from web beacons help us understand which marketing campaigns are successful and who is interested in our products or services; over time, this helps us calibrate and improve our results so we are sending the most interesting content to the most interested people.
- **Social media widgets**: which are links to social media platforms, such as Facebook, and LinkedIn (that might include widgets, such as the "share this" button or other interactive mini-programs). These features may collect your IP address and which page you are visiting on the website and may set a cookie to enable the feature to function properly. These social media features are either hosted by a third party or hosted directly on our website(s). Your interactions with these features are governed by the privacy policy of the company providing it.
- **Google Analytics**: we also use Google Analytics to collect information regarding visitor behavior and demographics on some of the Services. This analytics data is not tied to any Personal Data other than location data. For more information about Google Analytics, please visit www.google.com/policies/privacy/partners/. You can opt-out of Google's collection and processing of data generated by your use of the Services by going to http://tools.google.com/dlpage/gaoptout.
- **Other third-party platforms**: When you choose to connect with third-party platform when using any of the Services, we may collect information about you from that platform, including any information that you choose to import into the Services. You may also be able to access posting and sharing tools on the Services that allow you to post information to a social media or third-party platform. By using these tools, you acknowledge that some account information may be transmitted from the applicable platform account to us; our treatment of that information is covered by this Policy. Additionally, when you use one of these tools, the third-party platform may be collecting information about your online activity through its own tracking technologies, subject to its own privacy policy. We encourage you to read the privacy and other policies of any third-party platform you use in connection with any of the Services.

5. Information We Share

We share information, including Personal Data, with certain third parties as described below.

- Clients: We share certain data with our clients. For example, if a client has asked us to collect messages or record voice calls from its customers and prospective customers, we provide the data requested. We also share data related to the client's and its customers' use of the Services. This may include Client Content, Client Usage Data or other types of data. As described above, we collect this data at our client's request. Our use of this data is subject to this Policy, but the client's use of that same data is in the client's control and is subject to the client's own policies.

- Cloud communication providers and telephony operators used to operate the Services: We may share (or such providers and operators may collect and share with us) certain Client Content and Client Usage Data as necessary for proper routing and connectivity of your communications. How those providers and operators handle your Clients Content and Client Usage Data is generally determined by those providers' and operators' own policies and local regulations.
- Third-party service providers or consultants used to operate the Services: We may share data collected from you on the Site and via the Services with third-party service providers or consultants who need access to such data to perform their work on our behalf, such as hosting services or cloud storage provider, website analytics company, telephony services provider, medical/dental practice management companies used by our clients or third-party advertising partner. These third-party service providers are limited to only accessing or using such data to provide services to us and must provide contractual assurances that they will appropriately safeguard Personal Data.
- Third-party service providers for general business purposes: Customer relationship management providers, payment processors, messaging services, IT service management systems, teleconferencing services, and AI Notetaking services.
- Compliance with Laws: We may disclose your Personal Data to a third party if (i) we believe that disclosure is reasonably necessary to comply with any applicable law, regulation, legal process, or government request (including to meet national security or law enforcement requirements), (ii) to obtain legal advice, (iii) to enforce our agreements and policies, (iv) to protect the security or integrity of the Site or the Services, (v) to protect ourselves, our other customers, or the public from harm or illegal activities, or (vi) to respond to an emergency which we believe in good faith requires us to disclose information to assist in preventing a death or serious bodily injury. If we are required by law to disclose any of your Personal Data that directly identifies you, then we will use reasonable efforts to provide you with notice of that disclosure requirement, unless we are prohibited from doing so by applicable law, regulation or administrative order. We will object to requests that we do not believe were issued properly.
- Affiliates: We may share data collected from you from the Site or via the Services with our affiliates. Our affiliates will use the information for the same purposes as Prism, as described in this policy.
- Business transfers: If we go through a corporate sale, merger, reorganization, dissolution, or similar event, data we gather from you through our website may be part of the assets transferred or shared in connection with due diligence for any such transaction. Information disclosed for due diligence purposes will be subject to a confidentiality agreement restricting the potential acquiror or other party to such transaction from using such information other than for purposes of due diligence. Any acquirer or successor of Prism may continue to use the information we collect from you through our website as described in this policy.

We do not share your data (including, but not limited to, your Personal Data and the Personal Data of your customers and other end users) with third parties for their direct marketing purposes, unless you give us your consent to do so.

6. Aggregated De-identified Data

In addition to the various uses of data described above, except as otherwise agreed by us in writing (such as in our client agreement), and except as may be prohibited by applicable law, we may use any category of data described above to generate aggregated, de-identified data for our legitimate interests in creating data sets that help us understand, evaluate, maintain and improve the Site and the Services, and develop and provide tools and reports useful to our clients. So long as such aggregated, de-identified data does not contain any Personal Data and cannot be reverse engineered to product Personal Data, we may use such aggregated, de-identified data without restriction.

7. Information From or About Children

The Site and the Services are not intended for children, and we do not knowingly collect any Personal Data directly from children under the age of 16. If we discover we have received any Personal Data from a child under the age of 16 in violation of this Policy, we will take reasonable steps to delete that information as quickly as possible. If you believe we have any information from or about anyone under the age of 16, please contact us at privacy@patientprism.com.

8. Links to other websites

We are not responsible for the practices employed by websites or services linked to or from the Site or the Services, or for any content or other information provided by the owners or operators of those websites or services. Please note that when you use a link to go from the Site or the Services to a third-party website or other service, this Policy does not apply to the third-party websites or service. Your browsing and interactions on any third-party website or service are subject to that third party's own rules and policies.

9. Advertising and Promotions

We partner with third-party ad networks to either display advertising on the Site or to manage our advertising on other sites. Our ad network partner uses cookies and web beacons to collect non-personal information about your activities on the Site and other websites to provide you targeted advertising based upon your interests. If you wish to not have this information used for the purpose of serving you targeted ads, you may opt-out by clicking here: http://optout.networkadvertising.org/ or here: http://www.youronlinechoices.com. Please note this does not opt you out of being served advertising in general. You will continue to receive generic ads.

If you receive promotional emails from us, you can choose to stop receiving them at any time by following the unsubscribe/opt-out instructions in those emails. You can also opt-out by contacting us at privacy@patientprism.com. Please note that even if you opt out of promotional communications, we may still send you non-promotional messages relating to things like updates to our terms of service or privacy notices, security alerts, and other notices relating to your access to or use of the Services. We will respond to your request within a reasonable timeframe and notify you of the action we have taken.

10. Data Security and Retention

We use reasonable and appropriate security measures to protect the security of Personal Data, both online and offline. These measures vary based on the sensitivity of the Personal Data that we collect, process, and store, and on the current state of technology. Specific measures may be included in our written agreements with our clients. Please note, though, that no website or internet transmission is completely secure, so while we strive to protect your Personal Data, we cannot guarantee that unauthorized access, hacking, data loss, or a data breach will never occur.

If you are a Prism client or authorized personnel of a Prism client, you share in the responsibility for the security of your Personal Data. For example, you must use appropriate measures to protect your passwords or other login credentials, as well as the access to and use of Personal Data we may have collected on your behalf, but which you control.

We will store your Personal Data for as long as is reasonably necessary for the purposes for which it was collected, as explained in this Policy and as may be further specified in our written agreement with you or your organization. In some circumstances we may store your Personal Data for longer periods of time; for instance, where we are required to do so in accordance with legal, regulatory, tax, or accounting requirements.

In specific circumstances we may store your Personal Data for longer periods of time so that we have an accurate record of your dealings with us in the event of any disputes, or if we reasonably believe there is a prospect of a dispute relating to your Personal Data.

To determine the appropriate retention period for Personal Data, we consider the amount, nature and sensitivity of the Personal Data, the potential risk of harm from unauthorized use or disclosure of the Personal Data, the purposes for which we process the Personal Data and whether we can achieve those purposes through other means, and the applicable legal, regulatory, tax, accounting or other requirements.

11. Your Choices and Rights

11.1. Access, Rectify/Update, Delete

To request access to or deletion of your Personal Data we have collected via the Site, or to request that we correct any errors, outdated information, or omissions in such Personal Data, please email us at privacy@patientprism.com. Please note that even if you request that we delete data we've collected from you, we may still retain information collected from you in an aggregated or anonymized form that does not identify you. We also will not delete your information if we are legally required to maintain it.

If you are a Prism client, you may access and make changes to certain parts of your Client Account Data through the Prism portal. You may also have access to certain Client Content and Client Usage Data through the portal.

In many cases, our collection and use of Personal Data is at the request of our clients, and we are contractually obligated to provide the Services that our clients request. If you are a customer of a Prism client, please direct any requests or inquiries you may have regarding Personal Data about you directly to that client. That client is primarily responsible for handling any requests to access Personal Data about you, or to rectify/update or delete that Personal Data, and/or to place any other limits on our use or disclosure of your Personal Data. As their service provider, Prism will act on any Personal-Data request of yours that they forward to us. If you submit a request to us regarding Personal Data that we have collected for a client, we will forward that request to the client.

We may ask you for additional information to confirm your identity and for security purposes, before taking any action in respect of your Personal Data. We reserve the right to charge a fee where permitted by law; for instance, if your request is manifestly unfounded, excessive or repetitive.

11.2. Advertising and Promotional Communications

You can opt out of advertising and promotional communications as described in "Advertising and Promotions" section above.

11.3. Cookies and tracking technologies

You can manage cookies and similar technologies by following the instructions in your browser and by making the appropriate selections when cookie notices are presented to you. For more information, please see the "Information We Collect Automatically" section above.

11.4. General Notice to Non-US Residents

Prism is based in the United States and our data processing activities occur in the United States. Except as otherwise expressly agreed by us, the Personal Data we collect is governed by United States law, which may be different from the laws applicable to Personal Data in your country of residence. To the fullest extent permitted by applicable law, by providing your Personal Data to us or by using the Services, you acknowledge and agree to our collection, transfer, processing, and storage of your Personal Data in the United States in accordance with this Policy and the contract between us and the applicable client relating to the Services.

11.5. Information for EU, EEA, Swiss and UK Residents

If you live and use the Services in an EU or EEA member state, Switzerland or the UK, you may have additional rights under GDPR. Various sections of this Policy explain our practices regarding collection, use, disclosure and retention of your Personal Data, as well as your choices and rights, and how to exercise your rights. In addition, you may have the right to object to certain processing based on a "legitimate interests" justification, to ask us to restrict our processing of your Personal Data in some circumstances, and to lodge a complaint about our privacy practices with your local supervisory authority.

Our primary lawful basis for processing your Personal Data as described in this Policy is necessity for providing the Services you or your organization (or our client, where you are a customer of that client) request under our client contracts. We also process your Personal Data for our legitimate interests, which include product development, analytics, marketing and advertising, as further described in the "Information We Collect and Purposes of Collection" section above. We make sure we consider and balance any potential impact on you (both positive and negative) and your rights before we process your Personal Data for our legitimate interests. We do not use your Personal Data for activities where our interests are overridden by the impact on you (unless we have your consent or are otherwise required or permitted to by law).

In some cases, we process your Personal Data based on your consent obtained from you by us or by our client prior to or at the time of collection. Where that is the case, you may withdraw your consent at any time by contacting us at privacy@patientprism.com or the applicable client. If we wish to use your Personal Data for a purpose inconsistent with those described in this Policy or our client contracts, we will notify you or our client, as applicable, and, where required, ask for your consent. Again, where our client controls what Personal Data we collect and the purposes of collection, it will be the client's obligation to obtain your consent.

Please contact us at privacy@patientprism.com if you have any questions about this section. Alternatively, you may contact:

Our representative in the EU:
DPO Europe GmbH
Berlin Amtsgericht Berlin (Charlottenburg)
HRB 235801
Auguste-Viktoria-Allee, 20A, 13403, Berlin, Germany
+49 5361 389 4118
https://data-privacy-office.eu
info@data-privacy-office.eu

Our representative in the UK:
The Virtual CISO Limited
43 Rosslyn Hill, London NW3 5UH
+44 2074311143
marina@thevirtualciso.io
https://thevirtualciso.io

You are not required to pay us for exercising your rights. We try to respond to all legitimate requests within a reasonable time. Occasionally our response could be delayed if your request is complex or you have made a number of requests.

11.6 Participation in the EU-US Data Privacy Framework, with UK Extension

Prism complies with the EU-U.S. Data Privacy Framework and the UK Extension to the EU-US Data Privacy Framework (collectively, the "DPF") as set forth by the U.S. Department of

Commerce. Prism has certified to the U.S. Department of Commerce that it adheres to the Principles set forth in the DPF (the "DPF Principles") with regard to the processing of any Personal Data transferred from the European Economic Area (that is, the EU Member States, plus Iceland, Liechtenstein and Norway, collectively, the "EEA") and/or UK (including Gibraltar) to the US in reliance on the DPF. Further details of the DPF and our certification are available at https://www.dataprivacyframework.gov/. In the event of any conflict between the terms of this Policy and the DPF Principles, the DPF Principles shall govern.

Prism is fully committed to apply all the Principles of the DPF to any data received in the EEA or the UK.

For any unresolved complaints you may contact the appropriate authority:

If you reside in	Authority for Complaints
European Union/European Economic Area	EU data protection authorities (DPAs)
United Kingdom	Information Commissioner's Office (ICO) Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF, United Kingdom 0303 123 1113 (local rate) or +44 1625 545 700 (international) casework@ico.org.uk www.ico.org.uk For complaints relating to the US-EU Data Privacy Framework (UK Extension): https://ico.org.uk/make-a-complaint/uk-extension-to-the-eu-us-data-privacy-framework-complaints-tool/

In compliance with the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF, Prism commits to cooperate and comply respectively with the advice of the panel established by the EU data protection authorities (DPAs) and the UK Information Commissioner's Office (ICO) with regard to unresolved complaints concerning our handling of personal data received in reliance on the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF.

As part of our participation in the DPF, Prism is further subject to the investigatory and enforcement powers of the U.S. Federal Trade Commission.

Under certain conditions, described at the DPF website, if you have an unresolved dispute with us, you may have the option to invoke binding arbitration.

Under the DPF, we are responsible for the processing of Personal Data we receive and subsequently transfer to a third party acting as an agent on our behalf. We comply with the DPF Principles for onward transfers of Personal Data, including the onward transfer liability provisions of those Principles.

11.6. Information for California Residents

If you live and use the Services in California, you may have additional rights under California law, including CCPA. Please note, however, that some Personal Data is outside the scope of

the CCPA and is not covered by this section of this Policy. Specifically, this section does not address our handling of Personal Data about California consumers that is exempt from the CCPA because it is covered by existing qualifying privacy laws. It also does not address Personal Data collected in a business-to-business context or our handling of Personal Data about consumers which we undertake on behalf of our clients in the context of providing those clients with the Services.

Various sections of this Policy explain our practices regarding collection, use, disclosure and retention of specific categories of your Personal Data, as well as your choices and rights, and how to exercise your rights, including the right to access your Personal Data and to request that we delete your Personal Data. In addition, you may have the right to opt-out of the "sale" and "sharing" of your Personal Data, as those terms are defined under the CCPA.

We do not sell Personal Data. If we wish to share your Personal Data for cross-context behavioral advertising, we will post an opt-out-of-sharing link on the Site, which you may use to instruct us not to share your Personal Data for such purpose. You may also opt-out by contacting us at privacy@patientprism.com.

We do not discriminate against anyone for exercising their rights under Data Protection Laws.

11.7 Information for Canadian Residents

Prism's policies and procedures include compliance with PIPEDA, where applicable. If you would like to understand these regulations and/or your rights under PIPEDA, please contact:

Office of the Privacy Commissioner of Canada (OPC)
30 Victoria Street, Gatineau, Quebec, K1A 1H3, Canada
1-800-282-1376 (toll-free)
or
613-995-8210
613-947-6850 (fax)
inquiries@priv.gc.ca
www.priv.gc.ca

12. Contact Information

If you have questions or concerns about this Policy, or if have a dispute with us regarding or wish to exercise your rights regarding your Personal Data, please contact us by email at privacy@patientprism.com or by writing to us as:

Data Protection Officer
Patient Prism LLC
707 N. Franklin St., Unit 3
Tampa, Florida 33602 USA.