

STATE ADDENDUM TO THE SOHOMD PRIVACY POLICY

ADDENDUM DATE: July 11, 2023

This State Addendum to the SohoMD Privacy Policy (“Addendum”) supplements the terms of SohoMD’s Privacy Policy and applies to individuals who are residents of California, Colorado, Connecticut, Virginia, and Utah, as specified below. It describes the rights you may have, depending on the state of your residence, with regard to your personal information, which apply when new or updated laws take effect in these states. This Addendum does not apply to any employees, owners, directors, officers, or contractors of SohoMD or its affiliates.

I. California Privacy Policy

The section relates solely to residents of the State of California, and for purposes of this section, "you" means residents of the State of California. This section will provide you with information about our information practices and your privacy rights under the California Consumer Privacy Act (CCPA), the California Privacy Rights Act (CPRA) and applicable regulations (collectively referred to as "CPRA"). Any terms defined in the CPRA have the same meaning when used in this section.

1) Personal Information we collect

SohoMD collects information that identifies, relates to, describes, references, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular California consumer or household ("CPRA Covered Personal Information" or "personal information"). CPRA Covered Personal Information does not include personal information that has been de-identified or aggregated, or that is publicly available information from government records.

In particular, we have collected the following categories of CPRA Covered Personal Information from consumers (as that term is defined in the CPRA) within the last twelve (12) months:

Category	Examples	Collected
A. Personal Identifiers.	A real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, Account name, Social Security number, driver's license number, passport number, or other similar identifiers.	Yes
B. Personal and financial information categories listed in the California Customer Records statute (Cal. Civ. Code § 1798.80(e)).	A name, signature, Social Security number, physical characteristics or description, address, telephone number, passport number, driver's license or state identification card number, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, medical information, or health insurance information. Some personal information included in this category may overlap with other categories.	Yes

C. Protected classification characteristics under California or federal law.	Age (40 years or older), race, national origin, citizenship, religion or creed, marital status, medical condition, physical or mental disability, sex (including gender, gender identity, gender expression, pregnancy or childbirth and related medical conditions), sexual orientation, veteran or military status.	Yes
D. Commercial information.	Records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.	Yes
E. Biometric information.	Genetic, physiological, behavioral, and biological characteristics, or activity patterns used to extract a template or other identifier or identifying information, such as, fingerprints, faceprints, and voiceprints, iris or retina scans, keystroke, gait, or other physical patterns, and sleep, health, or exercise data.	No
F. Internet or other similar network activity.	Browsing history, search history, information on your interaction with a Services, application, or advertisement.	Yes
G. Geolocation data.	Physical location or movements.	No
H. Sensory data.	Audio, electronic, visual, thermal, olfactory, or similar information.	No
I. Professional or employment related information	Occupation, title, employer information, current or past job history or performance evaluations.	No
J. Non-public education information (per the Family Educational Rights and Privacy Act (20 U.S.C. Section 1232g, 34 C.F.R. Part 99)).	Education records directly related to a student maintained by an educational institution or party acting on its behalf, such as grades, transcripts, class lists, student schedules, student identification codes, student financial information, or student disciplinary records.	No
J. Inferences drawn from other personal information.	Profile reflecting a person's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.	Yes
L. Sensitive Personal Information	Social security, driver's license, state identification or passport numbers; Account log-in, financial account, debit or credit card number in combination with any required security or access code, password or credentials allowing access to an Account; precise geolocation data; racial or ethnic origin, religious or philosophical beliefs or union membership, content of mail, email and text messages unless business is the intended recipient; genetic data; processing of biometric information for the purposes of uniquely identifying a consumer; personal information collected and analyzed concerning your health.	Yes

2) Categories of sources from which we collect personal information

You have the right to know the categories of sources from which we collect your personal information. We make this information available to you in the INFORMATION WE MAY COLLECT section of our Privacy Policy.

3) **Our processing of your personal information**

You have the right to know how we process and use your personal information. We make this information available to you in the USE OF INFORMATION section of our Privacy Policy.

4) **Disclosure of Personal Information**

You have the right to know if we share your personal information with any third parties and the categories of those third parties. We make this information available to you in the SHARING OF INFORMATION section of our Privacy Notice.

5) **No Sales or Sharing of Personal Information**

We do not sell personal information for monetary or other consideration, and we do not share your personal information for cross-context behavioral advertising (as defined in the CPRA). We have also not sold or shared the personal information of consumers under 16 years of age.

6) **Use of Sensitive Personal Information**

We do not use or disclose sensitive personal information for purposes other than those specified in section 7027, subsection (m) of the CPRA regulations and we do not collect or process sensitive personal information for purposes of inferring characteristics about you.

7) **Your CPRA Consumer Rights**

- a) Where we are acting as a business (as opposed to a service provider as those terms are defined in the CPRA), you have the following rights:
 - **Right to Access.** You have the right to request that we disclose the categories of personal information we collected about you, the categories of sources for the personal information we collected about you, our business or commercial purpose for collecting your personal information, the categories of third parties with whom we share your personal information; and the specific pieces of personal information we collected about you.
 - **Right to data portability.** You have the right to obtain a copy of your data in a portable, and to the extent technically feasible, readily usable format that allows you to transmit the data to a third party.
 - **Right to delete.** You may have the right to request that we delete your personal information where we act as a business. This right is subject to several exceptions and we may deny your deletion request if retaining the information is necessary for us or our service providers to:
 - o Complete the transaction for which we collected the personal information and take actions reasonably anticipated within the context of our ongoing business relationship with you or our client;
 - o Detect bugs or errors in our Services, detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity, or prosecute those responsible for such activities;
 - o Enable solely internal uses that are reasonably aligned with consumer expectations based on your relationship with us;
 - o Comply with a legal obligation; or

- o Make other internal and lawful uses of that information as permitted by law or that are compatible with the context in which we collected it.
- **Right to correct.** We take reasonable steps to ensure that information we hold about you is accurate and complete. However, you have the right to request that we correct any inaccurate personal information that we have about you.
- **Right to non-discrimination and no retaliation.** We will not discriminate or retaliate against you for exercising any of your rights under the CCPA, including we will not deny you goods or services, charge you different prices for goods or services, provide you a different level or quality of goods or services, or suggest that you will receive a different price for goods or services or a different level of quality of goods and services.

b) Exercising Your Rights

You may exercise your rights to know, delete and correct as described above by submitting a verifiable request to us by either:

- Emailing us at privacy@SohoMD.com; or
- Calling us at 212-369-6757

c) Verification Process

We are only required to fulfill verifiable requests. Only you, you as a parent or a legal guardian on behalf of a minor child, or your authorized agent may make a verifiable request related to personal information. If you submit your request through an authorized agent, we may require you to provide your agent with written permission to do so and verify your identity. We may deny any request by an authorized agent that does not submit proof that the agent has been authorized by you to act on your behalf.

- **For requests for access to categories of personal information,** we will verify your request to a "reasonable degree of certainty." This may include matching at least two data points that you would need to provide with data points we maintain about you and that we have determined to be reliable for the purposes of
- **For requests for specific pieces of personal information (portability request),** we will verify your request to a "reasonably high degree of certainty." This may include matching at least three data points that you would need to provide with the data points we maintain about you and that we have determined to be reliable for the purposes of verification. We will also require you to submit a signed declaration under penalty of perjury that you are the consumer whose personal information is the subject of the request.
- **For requests to delete,** we will verify your request to a "reasonable degree" or a "reasonably high degree of certainty" depending on the sensitivity of the personal information and the risk of harm to the consumer posed by unauthorized deletion.

We will use the personal information you provide in a request only for purposes of verifying your identity or authority to make the request.

d) Response Timing and Format

We will respond to a verifiable request within forty-five (45) days of its receipt, and will notify you within those forty-five (45) days if we require more time to respond and the reasons for the additional time. If you have an Account with us, we will deliver our written response to that Account. If you do not have an Account with us, we will deliver our written response by mail or electronically, at your option. (Note that the law prohibits us from disclosing at any time a consumer's Social Security number, driver's license number or other government-issued identification number, financial account number, any health insurance or medical identification number, an Account password, security questions and answers, or any unique biometric data.) If we cannot comply with a request or a portion of the request, we will include the reasons in our response. If we deny your request on the basis that it is impossible or would involve a disproportionate effort, we will explain our reasons, such as the data is not in a searchable or readily accessible format, is maintained for only legal or compliance purposes, or is not sold or used for any commercial purpose and our inability to disclose it, delete or correct it would not impact you in any material manner.

We do not charge a fee to process or respond to your verifiable request unless it is excessive, repetitive, or manifestly unfounded. If we determine that the request warrants a fee, we will tell you why we made that decision and provide you with a cost estimate before completing your request.

*Please note that in certain cases we may collect your personal information as a service provider (as opposed to a business, as those terms are defined in the CPRA) pursuant to a contract we have with a commercial client (the CPRA business) to provide a service. In such a case, we are required to collect and process your information only based on the instructions received from the business. Should you direct your requests to exercise your rights to us, we may be required to share your request with the business, who is the party responsible under the CPRA for receiving, verifying and responding to your requests, or we may direct you to make your request directly to the business.

8) CPRA exemptions

This section (California Privacy Policy) does not apply to the following data which is exempt from the CPRA, including but not limited to: medical information governed by the California Confidentiality of Medical Information Act (CMIA); protected health information collected by a covered entity or business associate governed by the Health Insurance Portability and Accountability Act of 1996 (HIPAA), or personal information collected, processed, sold, or disclosed pursuant to certain sector-specific privacy laws, including the Fair Credit Reporting Act (FCRA), the Gramm-Leach-Bliley Act (GLBA) or California Financial Information Privacy Act (FIPA), and the Driver's Privacy Protection Act of 1994 (DPPA).

9) Other California Privacy Rights

California's "Shine the Light" law (Civil Code Section § 1798.83) permits users of our Services who are California residents to request certain information regarding our disclosure of personal information to affiliates and other third parties for their direct marketing purposes. To make such a request, please send an email to privacy@SohoMD.com.

II. Notice of Colorado, Connecticut, Virginia and Utah Privacy Rights

The section relates solely to residents of the States of Colorado, Connecticut, Virginia and Utah, and provides you with information about your privacy rights under the Colorado Privacy Act (CPA), the Connecticut Data Privacy Act (CDPA), the Virginia Consumer Data Protection Act (VCDPA) and the Utah Consumer Privacy Act (UCPA).

This section shall be effective for the residents of those States on the dates set forth below:

- Effective January 1, 2023, for residents of the State of Virginia
- Effective July 1, 2023, for residents of the States of Colorado and Connecticut
- Effective December 31, 2023, for residents of the State of Utah

For purposes of this section, "residents", "consumers" or "you" means individuals of those states who are acting in their individual or household context. This section does not apply to individuals acting in their commercial or employment context.

1) Personal Information we collect

You have a right to know the categories and types of personal information we collect about you. We make this information available to you in the INFORMATION WE MAY COLLECT section of our Privacy Policy.

2) Categories of sources from which we collect personal information

You have the right to know the categories of sources from which we collect your personal information. We make this information available to you in the INFORMATION WE MAY COLLECT section of our Privacy Policy.

3) Our processing of your personal information

You have the right to know how we process and use your personal information. We make this information available to you in the USE OF INFORMATION section of our Privacy Policy.

*For residents of the State of Virginia, to the extent that we maintain de-identified data, we take reasonable measures to ensure that de-identified data cannot be associated with a natural person, we publicly commit to maintaining and using de-identified data without attempting to re-identify the data, and we contractually obligate any recipient of the data to comply with the same obligations.

4) Disclosure of Personal Information

You have the right to know if we share your personal information with any third parties. We make this information available to you in the SHARING OF INFORMATION section of our Privacy Policy.

5) No Sale of Data or Use of Data for Targeted Advertising

We do not sell your personal information and we do not use your data for targeted advertising (as that term is defined by your applicable state law). We may send you advertising in response to your request for information or feedback or based on your activities with our Services, including your search queries and visits to our Services. However, we will not send you targeted

advertising based on your activities across non-affiliated websites, applications or platforms to predict your preferences or interests.

6) Your Rights

a) Where we act as the Controller of your personal information (as opposed to a Processor as those terms are defined in your applicable State law), you have the right to submit a request to us for the following:

- **Right to access.** You have the right to know if we process your personal information and have access to such information and certain details of how we use it.
- **Right to correct.** We take reasonable steps to ensure that information we hold about you is accurate and complete. However, you have the right to request that we correct any inaccurate personal information that we have about you.
- **Right to delete.** You may have the right to request that we delete your personal information where we act as a controller. This right is subject to several exceptions and we may deny your deletion request if retaining the information is necessary for us or our processors to:
 - Complete the transaction for which we collected the personal information and take actions reasonably anticipated within the context of our ongoing business relationship with you or our client;
 - Detect bugs or errors in our Services, detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity, or prosecute those responsible for such activities;
 - Enable solely internal uses that are reasonably aligned with consumer expectations based on your relationship with us;
 - Comply with a legal obligation; or
 - Make other internal and lawful uses of that information as permitted by law or that are compatible with the context in which we collected it.
- **Right to restriction of processing (opt-out).** You have the right to opt-out of processing your personal information for purposes of profiling in furtherance of any automated processing of your data that produce legal or similarly significant effects concerning you. (This right only applies to residents of the States of Colorado, Connecticut and Virginia.)
- **Right to data portability.** You have the right to obtain a copy of your data in a portable, and to the extent technically feasible, readily usable format that allows you to transmit the data to a third party.
- **Right to non-discrimination and no retaliation.** We will not discriminate or retaliate against you for exercising any of your rights, including but not limited to, by denying you goods or services, charging you different prices for goods or services, or providing you a different level or quality of goods or services.
- **Right to restrict the processing of sensitive information**

Unless we are processing your sensitive information pursuant to any of the legal exemptions listed in Section 8 (Exemptions) below or as otherwise allowed by law:

 - For residents of the States of Connecticut, Virginia and Colorado, we will not process your sensitive information without first obtaining your consent; and
 - For residents of the State of Utah, we will not process your sensitive personal information without providing you with notice and an opportunity to opt out.

b) Exercising Your Rights

You may exercise your rights to know, delete and correct as described above by submitting a verifiable request to us by either:

- o Emailing us at privacy@SohoMD.com; or
- o Calling us at 212-369-6757

c) Authentication Process

We will only fulfill request when we can verify your identify and confirm that you are authority to make such a request. Only you, you as the parent or legal guardian on behalf of your minor child, or your authorized agent, guardian or conservator may make a request related to personal information. If an authorized agent, legal guardian or conservator submits the request, we may require your written permission to do so and may require additional information to authenticate your identity. We may deny a request by an authorized agent, legal guardian or conservator who does not submit proof of authorization to act on your behalf. We will only use the personal information you provide in a request to verify your identity or authority to make the request.

d) Response Timing and Format

We will respond to an authenticated request within forty- five (45) days of its receipt, and will notify you within those forty-five (45) days if we require more time to respond and the reasons for the additional time. If you have an Account with us, we will deliver our written response to that Account. If you do not have an Account with us, we will deliver our written response by mail or electronically, at your option. If we cannot comply with a request or a portion of the request, we will include the reasons in our response.

*For residents of the States of Colorado, Connecticut and Utah, you may make one request within a twelve-month period at no charge.

*For residents of the State of Virginia, you may make a request up to two (2) times within a twelve (12) month period at no charge. We reserve the right to charge a fee to process or respond to any request that we consider excessive, repetitive, or manifestly unfounded. If we determine that the request warrants a fee, we will tell you why we made that decision and provide you with a cost estimate before completing your request.

7) Right to Appeal

You have the right to appeal our decision within a reasonable period of time after receipt of our response. You may appeal our decision by sending us an email at privacy@SohoMD.com. We will respond to your appeal within 60 days of receipt (45 days of receipt for residents of Colorado) and will inform you of any decisions and the reasons for such decisions.

* Please note that in certain cases we may collect your personal information as a processor (as opposed to a controller, as those terms are defined in your applicable state privacy law) pursuant to a contract we have with a commercial client (the controller) to provide a service. In such a case, we are required to collect and process your information only based on the instructions received from the controller. Should you direct your requests to exercise your rights to us, we

may be required to share your request with the controller, who is the party responsible under your applicable state privacy law for receiving, authenticating and responding to your requests.

8) Exemptions

This section (Notice of Colorado, Connecticut, Virginia and Utah Privacy Rights) does not apply to certain entities and data that are exempt from your applicable state privacy law, including but not limited to the following: covered entities, business associates and protected health information governed by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH); financial institutions and personal information subject to the Gramm-Leach-Bliley Act (GLBA); and personal information collected, processed, sold, or disclosed pursuant to certain sector-specific privacy laws, including the Fair Credit Reporting Act (FCRA), the Family Educational Rights and Privacy Act, the Farm Credit Act and the Driver's Privacy Protection Act of 1994 (DPPA).