WEBSITE PRIVACY POLICY

Last Updated: May 6, 2025

Resonately, Inc. **(**"**Resonately,**" or "**we,**" "**our,**" or "**us**"**)** considers the privacy of the users of this Website to be extremely important. As a result, Resonately is committed to maintaining robust protections for any user of this Website and protecting your privacy through our compliance with this Privacy Policy. This Website Privacy Policy (this "**Privacy Policy**") describes in detail the type of Personal Information that Resonately may collect from you or that you may provide when you visit or use our website, located at www.getresonately.com, including any platform, subdomain, or other website to which you are redirected from this website (collectively, the "Website") and/or Resonately's mobile application (our "**App**") and our practices for collecting, using, maintaining, protecting, and disclosing that information in order to assist you in making informed decisions when using any version of our Digital Services. For purposes of this Privacy Policy, this Website, our App and all related services and functionality that we provide through them are referred to as our "**Digital Services**". To the extent applicable, these Digital Services also include access to our proprietary, cloud-based, AI-powered medical scribe and transcription solution that supports both clinical and non-clinical workflows (the "**Solution**"). The Solution includes functionality to capture patient-provider conversations, generate real-time clinical documentation, enable provider queries and insights, and facilitate internal collaboration, together with any future enhancements, modules, updates, or features. The Solution is designed to support audiologists, hearing care professionals, and other licensed healthcare providers in both clinical and administrative workflows.

The Solution may collect, process, and transmit protected health information ("**PHI**") as defined under the Health Insurance Portability and Accountability Act of 1996 ("**HIPAA**"). Accordingly, our privacy practices reflect our obligations as a business associate under HIPAA and other applicable healthcare privacy laws.

The terms "**User**," "**user**," "**You**," "**you**," "**Your**," and "**your**" refer to Digital Services visitors, customers, clients, any other users of this Digital Services, and anyone who attempts to interact with the Digital Services.

This Privacy Policy applies to information we collect: (i) through our Digital Services, (ii) in email, text, and other electronic messages between you and our Digital Services, (iii) through mobile and desktop applications that provide dedicated interactions between you and this Website, or (iv) when you interact with our advertising and applications on third-party websites and services, including, but not limited to, YouTube, Facebook, and/or Instagram, if those applications or advertising include links to this Privacy Policy.

This Privacy Policy does not apply to information collected by: (i) us offline or through any other means, including on any other website operated by Resonately or any third party, or (ii) any third party, including through any application or content (including advertising) that may link to or be accessible from or through the Digital Services.

PLEASE READ THIS PRIVACY POLICY CAREFULLY TO UNDERSTAND OUR POLICIES AND PRACTICES REGARDING YOUR INFORMATION AND HOW WE WILL TREAT IT. IF YOU DO NOT AGREE WITH OUR POLICIES AND PRACTICES, YOUR CHOICE IS NOT TO USE OUR DIGITAL SERVICES. BY ACCESSING THE DIGITAL SERVICES, YOU ACCEPT THIS PRIVACY POLICY, OUR TERMS OF USE, AND OUR USAGE POLICY, AND YOU CONSENT TO THE COLLECTION, USE, STORAGE, AND DISCLOSURE OF YOUR PERSONAL INFORMATION (INCLUDING, WHERE APPLICABLE, PHI) AS DESCRIBED IN THIS PRIVACY POLICY.

Our Solution is exclusively for use by licensed healthcare professionals and their authorized administrative staff. However, certain features of the Solution may be used to facilitate limited patient-facing interactions, such as when a provider shares a visit summary with a patient or initiates the delivery of a patient intake form. The Solution is not designed for or marketed to patients or members of the general public. This Privacy Policy may change from time to time (see *Changes to this Privacy Policy*). Your continued use of any of the Digital Services after we make changes is deemed to be acceptance of those changes, so please check the policy periodically for updates.

1. Health Information.

Some information we collect constitutes or may constitute health and/or medical information, including PHI under HIPAA. Resonately is not a health care provider or a health insurance plan or insurance provider. Any healthcare-related functionality available in the Solution through our Digital Services is accessible only to authorized users of the Solution that have signed a Cloud Services Agreement. The general public may access our Website and download our App, but access to the Solution itself is restricted to healthcare professionals who have been granted credentials under a Cloud Services Agreement. Any healthcare-related functionality available through our Digital Services is accessible only through the Solution and only to authorized, licensed medical professionals (each a "**Provider**" and collectively, the "**Providers**"). Resonately does not provide medical care and is not responsible for any treatment decisions made by Providers using the Solution.

If you are a patient, your Provider, not Resonately, is legally required to provide you with their Notice of Privacy Practices which describes their collection, use and disclosure of your PHI. Resonately operates as a "**business associate**" (as defined under HIPAA) on behalf of these Providers ("**covered entities**") and may collect, receive, create, maintain, or transmit PHI in connection with our Solution's functionality. This includes capturing audio of patient-provider encounters, transcribing clinical interactions, generating structured chart notes, and delivering query-based assistance through co-pilot features. In some cases, the Solution may facilitate limited, provider-directed communications with patients—for example, by enabling a Provider to share a visit summary or send an intake form to a patient. These interactions are initiated and managed solely by the Provider and are governed by the Provider's own Notice of Privacy Practices. Resonately does not have a direct relationship with patients and does not use or disclose PHI for any independent purpose.

Where required by law, Resonately will enter into a Business Associate Agreement ("**BAA**") with each covered entity. All PHI handling will be performed in accordance with such BAA(s), HIPAA, and other applicable federal and state healthcare privacy laws. PHI will be used and disclosed only as permitted by HIPAA and the applicable BAA.

2. Children Under the Age of 18.

Our Digital Services are not intended for children under 18 years of age. No one under the age of 18 may provide any Personal Information to or through the Digital Services. We do not knowingly collect Personal Information from children under 18. If you are under 18, do not use or provide any information on through our Digital Services or through any of its features or provide any information about yourself to us, including your name, address, telephone number, email address, or any screen name or username you may use. If we learn we have collected or received Personal Information from a child under 18 without the consent of a parent or guardian, we will delete that information as soon as possible. If you believe we have collected such information, please contact us using the contact details set forth in Section 18 (*How to Contact Us*).

The Solution, which is accessed through our Digital Services, is not intended for use by individuals under the age of 18. Due to the nature of the Solution and its role in clinical documentation and healthcare workflows, minors are strictly prohibited from accessing or using the Solution, whether directly or indirectly. Healthcare providers are not permitted to make the Solution available to minors under any circumstances. The Solution is designed exclusively for use by licensed professionals and their authorized administrative staff. While the Solution may facilitate limited patient-facing interactions—such as the delivery of intake forms or visit summaries—these interactions are initiated and controlled solely by the Provider and do not involve direct access to the Solution by the patient.

California residents under 16 years of age may have additional rights regarding the collection and sale of their Personal Information.

3. Changes to this Privacy Policy.

This Privacy Policy is subject to change without notice from time to time in Resonately's sole discretion. All changes made to this Privacy Policy are effective immediately when we post them and apply to all access to and use of the Digital Services after they are posted. However, any changes to the dispute resolution provisions set out in *Arbitration* or *Governing Law and Jurisdiction* sections will not apply to any disputes for which the parties have actual notice before the date the change is posted on the Digital Services.

Please note that if you have entered into a separate written agreement with Resonately—such as a Cloud Services Agreement (CSA)—that agreement may include its own dispute resolution terms, which will govern in the event of any conflict with this Privacy Policy.

Your continued access to and use of the Digital Services following the posting of revised Privacy Policy means that you accept and agree to the changes. You are expected to check this page on a regular basis, so you are aware of any changes, as they are binding on you.

4. Information We Collect and How We Collect It.

We collect "Non-Personal Information" and "Personal Information." "**Non-Personal Information**" includes information about you but that cannot be used to personally identify you, such as anonymous usage data (including, but not limited to, your device's IP address, browser type, browser version, the pages of the Digital Services that you visit, the time and date of your visit, the time spent on those pages, unique device identifiers, and other diagnostic data), general demographic information we may collect, referring/exit pages and URLs, platform types, preferences you submit and preferences that are generated based on the data you submit and number of clicks. "**Personal Information**" includes information that may personally identify you such as name, postal address, email address, telephone number, date of birth, marital status, or any other identifier by which you may be contacted online or offline, which you submit to us through the Digital Services. We may also collect information about your internet connection, the equipment you use to access our Digital Services, and usage details.

When you access the Digital Services by or through a mobile device, we may collect certain information automatically, including, but not limited to, the type of mobile device you use, your mobile device unique ID, the IP address of your mobile device, your mobile operating system, the type of mobile Internet browser you use, unique device identifiers and other diagnostic data.

We collect this information: (i) directly from you when you provide it to us, (ii) automatically as you navigate through the Digital Services. Information collected automatically may include usage details, IP addresses, and information collected through cookies, web beacons, and other tracking technologies, and (iii) from third parties.

In connection with the use of the Solution by healthcare professionals, we may also collect or process information that is considered PHI under HIPAA. This may include audio recordings of clinical encounters, transcribed medical notes, and query responses generated using our co-pilot features. Collection and use of PHI is subject to the terms of any applicable BAA and applicable healthcare privacy laws.

5. Information You Provide to Us.

The information we collect on or through the Digital Services may include but is not limited to: (i) information that you provide by filling in forms on our Digital Services. This includes information provided at the time of registering to use our Digital Services, subscribing to our service, posting material, or requesting further services. We may also ask you for information when you enter a contest or promotion sponsored by us, and when you report a problem with our Digital Services, (ii) records and copies of your correspondence (including email addresses), if you contact us, (iii) your responses to surveys that we might ask you to complete for research purposes, (iv) details of transactions you carry out through our Digital Services and of the fulfillment of your orders. You may be required to provide financial information before placing an order through our Digital Services, (v) your search queries on the Digital Services, and/or (vi) clinical or administrative data submitted or uploaded to the Solution by authorized healthcare providers, including audio recordings, dictations, manual entries, and user-initiated prompts for clinical note generation or query responses. Such data may include PHI and is governed by applicable BAAs and privacy laws. You also may provide information to be published or displayed ("**posted**") on public areas of the Digital Services or transmitted to other users of the Digital Services or third parties (collectively, "**User Contributions**").

Your User Contributions are posted on and transmitted to others at your own risk. Although we limit access to certain pages, please be aware that no security measures are perfect or impenetrable. Additionally, we cannot control the actions of other users of the Digital Services with whom you may choose to share your User Contributions. Therefore, we cannot and do not guarantee that your User Contributions will not be viewed by unauthorized persons.

6. Information We Collect Through Automatic Data Collection Technologies.

As you navigate through and interact with the Digital Services, we may use automatic data collection technologies to collect certain information about your equipment, browsing actions, and patterns, including, but not limited to: (i) details of your visits to the Digital Services, including, but not limited to, traffic data, location data, logs, and other communication data and the resources that you access and use on the Digital Services, and/or (ii) information about your computer and internet connection, including, but not limited to, your IP address, operating system, and browser type. We also may use these technologies to collect information about your online activities over time and across third-party websites or other online services (also known as behavioral tracking). You may contact us to request more information about how to opt out of behavioral tracking on our Digital Services and how we respond to web browser signals and other mechanisms that allow consumers to exercise choice regarding such tracking.

The information we collect automatically may include Personal Information, or we may maintain it or associate it with Personal Information we collect in other ways or receive from third parties. It helps us to improve our Digital Services and to deliver a better and more personalized service, including by enabling us to: (i) estimate our audience size and usage patterns, (ii) store information about your preferences, allowing us to customize the Digital Services according to your individual interests, (iii) speed up your searches, and/or (iv) recognize you when you return to our Digital Services.

In connection with our Solution, we may also collect metadata and usage analytics related to how authorized users engage with clinical features, such as time spent using transcription tools, frequency of co-pilot queries, or navigation patterns within the dashboard. This information may help us enhance clinical workflow support, optimize product performance, and fulfill obligations under customer agreements. Any PHI collected through automated technologies is handled in accordance with applicable BAAs and HIPAA.

The technologies we use for this automatic data collection may include:

a. Cookies (or browser cookies). A cookie is a small file placed on the hard drive of your computer. You may refuse to accept browser cookies by activating the appropriate setting on your browser. However, if you select this setting you may be unable to access certain parts of our Digital Services. Unless you have adjusted your browser setting so that it will refuse cookies, our system will issue cookies when you direct your browser to the Digital Services.

b. Web Beacons. Pages of our the Website, videos, and our e-mails may contain small electronic files known as web beacons (also referred to as clear gifs, pixel tags, and single-pixel gifs) that permit Resonately, for example, to count users who have visited those pages, viewed a video, or opened an email and for other related website statistics (for example, recording the popularity of certain website content and verifying system and server integrity).

c. Flash Cookies. Certain features of the Digital Services may use local stored objects (or Flash cookies) to collect and store information about your preferences and navigation to, from, and on our Digital Services. Flash cookies are not managed by the same browser settings as are used for browser cookies.

The Digital Services do not collect Personal Information automatically, but we may tie this information to Personal Information about you that we collect from other sources or you provide to us. If you are an authorized user accessing the Solution through our Digital Services, we may collect certain Personal Information during the authentication process. For example, when you log in using single sign-on (SSO) functionality, such as “Continue with Google,” our authentication provider may provide us with your name and other account-related details to enable secure access to the Solution. This information is collected only in connection with verified Solution access and is not collected automatically from visitors who do not log in or use the Solution.

7. Third-Party Use of Cookies and Other Tracking Technologies.

Some content or applications, including advertisements, on the Website are served by third parties, including advertisers, ad networks and servers, content providers, and application providers. These third parties may use cookies alone or in conjunction with web beacons or other tracking technologies to collect information about you when you use our Digital Services. The information they collect may be associated with your Personal Information or they may collect information, including Personal Information, about your online activities over time and across different websites and other online services. They may use this information to provide you with interest-based (behavioral) advertising or other targeted content. We do not use or disclose PHI for marketing, advertising, or behavioral tracking purposes without your prior written authorization, as required under HIPAA and applicable law. Any PHI that may be processed by service providers is subject to BAAs and HIPAA-compliant safeguards.

If we use third-party service providers for analytics, infrastructure support, or security monitoring, those vendors are subject to contractual obligations that include appropriate privacy and data protection safeguards. Where required by law, we enter into BAAs with service providers that may access PHI. We do not control these third parties' tracking technologies or how they may be used. If you have any questions about an advertisement or other targeted content, you should contact the responsible provider directly.

8. Information Sharing.

a. Disclosure of Personal Information. Resonately may use or disclose Personal Information for the following purposes or in the following ways:

i. To present our Digital Services and its contents to you;

ii. To provide and maintain the Digital Services, including to monitor the usage of our Digital Services;

iii. To notify you about changes to our Digital Services or any products or services we offer or provide though it;

iv. To provide you with information, products, or services that you request from us;

v. To provide you with news, special offers and general information about other goods, services and events which we offer that are similar to those that you have already purchased or inquired about unless you have opted not to receive such information;

vi. To enter you into a promotion or share your information with the co-sponsor of that promotion;

vii. To enforce or apply our Terms of Use and Usage Policy, and other agreements, including for billing and collection purposes;

viii. To contact you by email, telephone calls, SMS, or other equivalent forms of electronic communication, such as a mobile application's push notifications regarding updates or informative communications related to the functionalities, products or contracted services, including, but not limited to, the security updates, when necessary or reasonable for their implementation;

ix. To our subsidiaries and affiliates;

x. To subprocessors and service providers who help us operate the Solution or support its functionality, such as secure cloud hosting providers, data analytics vendors, transcription engines, or infrastructure support. If these parties may have access to PHI, they will be subject to BAAs and HIPAA-compliant safeguards;

xi. To affiliates, strategic partners, agents, third party marketers, or other unaffiliated parties who are offering products or services that we believe may be of interest to you or who require your name, contact information or any behavioral or geolocation data that we have collected from you, for research, administrative, and/or internal business purposes;

xii. To unaffiliated third-party service providers, agents, or independent contractors who help us maintain the Digital Services and provide other administrative services to us, including, but not limited to, order processing and fulfillment, providing customer service, maintaining and analyzing data, sending customer communications on our behalf, and entry collection, winner selection, and prize fulfillment for contests, sweepstakes, and other promotions;

xiii. PHI will be used and disclosed only as permitted by HIPAA and the applicable BAAs. We do not use or disclose PHI for advertising, marketing, or behavioral tracking purposes;

xiv. For our own internal business purposes, such as to evaluate, audit, debug, or improve the usage, quality, and performance of programs and technologies related to interactions with us or third parties; design new services; process and catalog your responses to surveys or questionnaires (e.g., customer satisfaction reviews); perform internal research for technological development and demonstration; conduct data analysis and testing; and maintain proper business records and other relevant records;

xv. With third parties such as law enforcement or other government agencies to comply with law or legal requirements; to enforce agreements between you and us; and to protect our rights, property, and safety, and of our users and third parties;

xvi. To comply with applicable law, or in the good faith belief that such action is necessary in order to conform to the requirements of applicable law or comply with legal process served on us; protect and defend our rights or property; or act in urgent circumstances to protect the personal safety of our end users;

xvii. To third parties as part of any corporate reorganization process including, but not limited to, mergers, divestitures, restructures, reorganizations, dissolutions, or other sales or transfers of all or substantially all of our assets, whether as a going concern or as part of bankruptcy, liquidation, or similar proceeding, in which Personal Information held by us about our users is among the assets transferred;

xviii. To track and analyze non-identifying and aggregate usage and volume statistical information from our visitors, clients, and instructors and provide such information to third parties;

xix. To protect against potential fraud, we may verify with third parties the information collected from the Digital Services;

xx. To comply with any court order, law, or legal process, including to respond to any government or regulatory request;

xxi. In any other way we may describe when you provide the information; and/or

xxii. For any other purpose with your consent.

Except as described in this Privacy Policy or at the time we request the information, we do not otherwise use, share, or otherwise disclose your personally identifiable information to any third parties.

b. Disclosure of Non-Personal Information. In general, we use Non-Personal Information to help us improve the Digital Services and customize the user experience. We may also aggregate Non-Personal Information in order to track trends and analyze use patterns across our Digital Services, including this Website and the App. This Privacy Policy does not limit in any way our use or disclosure of Non-Personal Information and we reserve the right to use and disclose such Non-Personal Information to our partners and other third parties at our discretion.

Resonately expressly reserves the right to disclose your Personal Information and Non-Personal Information if Resonately reasonably believes it is required: (i) to do so by applicable law, (ii) to protect itself or to protect the rights of another user, (iii) to reduce risk of credit or other kind of fraud, or (iv) to comply with a court order.

9. Choices About How We Use and Disclose Your Information.

We strive to provide you with choices regarding the Personal Information that you provide to us. We have created mechanisms to provide you with the following control over your information:

a. Tracking Technologies and Advertising. You can set your browser to refuse all or some browser cookies, or to alert you when cookies are being sent. We may use technologies such as Google Analytics, Mixpanel, Hotjar, or similar tools to better understand how users interact with our Digital Services. These tools may use cookies or other tracking technologies to collect usage data. If you disable or refuse cookies, please note that some parts of our Digital Services may then be inaccessible or not function properly.

We do not control third parties' collection or use of your information to serve interest-based advertising. However, these third parties may provide you with ways to choose not to have your

information collected or used in this way. You can opt out of receiving targeted ads from members of the Network Advertising Initiative ("**NAI**") on the NAI's website.

We do not use or disclose Protected Health Information (PHI) for marketing, advertising, or behavioral tracking purposes without your prior written authorization, as required under HIPAA and applicable law.

Residents of certain states, such as California, Colorado, Connecticut, Delaware, Florida, Indiana, Iowa, Montana, Oregon, Tennessee, Texas, Utah, and Virginia, may have additional Personal Information rights and choices.

10. How we use Cookies.

A cookie is a small file which asks permission to be placed on your computer's hard drive. Once you agree, the file is added and the cookie helps analyze web traffic or lets you know when you visit a particular site. Cookies allow web applications to respond to you as an individual. The web application can tailor its operations to your needs, likes and dislikes by gathering and remembering information about your preferences.

We use traffic log cookies and similar tracking technologies to identify which areas of our Digital Services are being used. This helps us analyze data about user interactions and improve our Website and App in order to tailor the experience to customer needs. We only use this information for statistical analysis purposes and then the data is removed from the system.

Overall, cookies help us provide you with a better website by enabling us to monitor which pages you find useful and which you do not. A cookie in no way gives us access to your computer or any information about you, other than the data you choose to share with us.

Cookies are not used to track or process clinical content, transcriptions, audio recordings, or any PHI generated through the use of the Solution. However, when an authorized user accesses the Solution through our Digital Services, we may use cookies to store authentication-related information—such as a user's name or login credentials—for the purpose of identifying and securely authenticating the user.

For general visitors to our publicly accessible Website and App, we may use cookies and similar technologies to analyze usage patterns, remember preferences, and improve user experience. We seek your consent before placing any cookies used for advertising, marketing, or other tracking purposes not essential to site functionality.

You can choose to accept or decline cookies. Most web browsers automatically accept cookies, but you can usually modify your browser setting to decline cookies if you prefer. This may prevent you from taking full advantage of the Digital Services.

11. How We Protect and Secure Your Information.

We implement a combination of administrative, physical, and technical safeguards designed to protect your Personal Information and, where applicable, PHI from unauthorized access, disclosure, alteration, and destruction. These safeguards include, but are not limited to: (i) encryption of data in transit and at rest; (ii) access controls and authentication protocols; (iii) secure, HIPAA-compliant hosting environments; (iv) audit logging and activity monitoring; and (v) role-based access limitations for Solution users and internal personnel.

We follow industry standards and comply with applicable requirements under the HIPAA Security Rule when handling PHI on behalf of covered entities. Our security practices are designed to align with our obligations under any BAAs and relevant healthcare privacy laws. Despite our efforts to implement robust security measures, no method of transmission over the internet or electronic

storage is completely secure. As such, we cannot guarantee the absolute security of any information transmitted through the Digital Services. Any transmission is at your own risk.

The safety and confidentiality of your information also depends on you. If you are provided with account credentials or choose your own, you are responsible for maintaining the confidentiality of those credentials and for limiting access to your device. We ask that you do not share your password or other authentication information with anyone and that you take appropriate steps to safeguard your login credentials.

We are not responsible for circumvention of any privacy settings or security measures contained in the Digital Services.

12. How We Store Your Personal Information.

PHI is stored on secure servers located in the United States, unless otherwise disclosed or required by law. In very limited circumstances, we may transfer data outside the United States for processing or storage. By providing your Personal Information to us, you agree to this transfer, storing and processing.

We do our utmost to ensure that all reasonable steps are taken to make sure that your data is stored and transmitted securely. To the extent any PHI is stored or processed on our behalf, we use secure, HIPAA-compliant data hosting providers and industry-standard encryption measures that meet applicable privacy and data protection laws.

Unfortunately, the sending of information via the internet is not totally secure and on occasion such information can be intercepted. We cannot guarantee the security of data that you choose to send us electronically; sending and storing such information is entirely at your own risk.

13. How to Restrict the Collection or Use of Your Personal Information.

You may choose to restrict the collection or use of your Personal Information in the following ways: (i) whenever you receive an email or text message we will provide you with an “unsubscribe” link. Click on the link and follow further instructions to remove yourself from future communications; (ii) whenever you receive a phone call from us you may request that we do not contact you by phone in future, and (iii) if you have previously agreed to us using your Personal Information for direct marketing purposes, you may change your mind at any time by writing to or emailing us at hello@getresonately.com.

We reserve the right to contact you with important account information deemed necessary to ensure you receive an effective service. This includes the communication of results and other information deemed by Resonately to be relevant and important in ensuring you receive the best possible service and results. Resonately distinguishes between important account information and communications intended to keep you informed generally about Resonately promotions, discounts, products and services which you will receive unless you inform us you do not want to.

PHI will only be used or disclosed as permitted by HIPAA and the applicable BAAs, and not for marketing without valid written authorization.

Resonately will not sell, distribute or lease your Personal Information to third parties unless we have your permission or are required by law to do so. We may use your Personal Information to send you promotional information about Resonately services.

If you believe that any information we are holding on you is incorrect or incomplete, please email us as soon as possible at hello@getresonately.com and we will correct it in line with your request.

14. State Privacy Disclosures.

Certain data processed by Resonately may be exempt from state consumer privacy laws under applicable federal laws, including HIPAA. Where Resonately acts as business associate to a HIPAA-covered entity, the rights described in this section may not apply to PHI handled under a BAA.

These state privacy disclosures apply solely to residents of California and other states that have adopted generally applicable privacy laws (collectively, the "**State Privacy Laws**") whose personal information is covered under the State Privacy Laws and supplements the information contained elsewhere in this Privacy Policy.

a. Your Rights. If you live in California or other states that have adopted State Privacy Laws, you may have several rights in relation to your personal information, as summarized below. These rights apply only to Personal Information governed by State Privacy Laws. Information subject to HIPAA, including PHI processed under a BAA, is governed by HIPAA and is not subject to these state-level consumer rights:

The Right to Access	You may have the right to obtain confirmation regarding whether we are processing your personal information and to access that personal information, including the right to know (i) the specific pieces of personal information the business has collected about you and (ii) the categories of personal information collected, the sources of collection, the business/commercial purpose for collecting or "selling/sharing for targeted advertising" personal information, and the categories of third party to whom the business discloses personal information. For a list of the categories of personal information we have collected, please see *Additional Data Processing Disclosures/Notice at Collection* below.
The Right to Know	You have the right to request that we disclose the following about your personal information, as defined by the applicable State Privacy Law: (i) the specific personal information we have collected; (ii) the categories of personal information we have collected; (iii) the categories of sources from which we have collected your personal information; (iv) the business purpose(s) for collecting or sharing your personal information; (v) the categories of personal information we disclosed for business purposes; and (vi) the categories of third parties to whom we disclosed your personal information.

The Right to Request Deletion	You may have the right to request the deletion of personal information we have collected from you, subject to certain exceptions.
The Right to Correct	You may have the right to request that any inaccuracies in your personal data be corrected, taking into account the nature of the personal data and the purposes of the processing of your personal information.
The Right to Opt-Out of “Sales” or “Sharing”/Processing for Targeted Advertising	You may have the right to opt-out of: • The “sale” of personal information to third parties; and • The processing of personal information for purposes of “targeted advertising” (including the “sharing” of personal information for that purpose). • To the extent required by law, we will honor opt-out preference signals sent in a format commonly used and recognized by businesses, such as via Global Privacy Control (GPC). Your Privacy Choices Note that we don’t “sell” or “share” (and process for “targeted advertising” more generally) your personal information, as such terms are broadly defined under the State Privacy Laws. Specifically, we consider disclosures of identifiers, commercial information, geolocation data, and internet or other network information described in this Privacy Policy to our advertising/marketing and analytics partners (such as ad agencies, social media networks, adtech partners, customer intelligence firms, social media companies) for advertising and marketing purposes as "sales" or “shares” (and processing for “targeted advertising” more generally). We do not have actual knowledge of “selling” or “sharing” personal information of those under 16 years of age. We do not “sell” or “share” PHI as defined by HIPAA. PHI is governed by HIPAA and the

	applicable BAAs and is not subject to state consumer privacy rights or obligations.
“Sensitive” Personal Information	We may use and disclose Sensitive Personal Information only for the following purposes: (i) performing services or providing goods reasonably expected by an average consumer; (ii) detecting security incidents; (iii) resisting malicious, deceptive, or illegal actions; (iv) ensuring the physical safety of individuals; (v) for short-term, transient use, including non-personalized advertising; (vi) performing or providing internal business services; (vii) verifying or maintaining the quality or safety of a service or device; or (viii) for purposes that do not infer characteristics about you.
Right to non-discrimination	You have the right not to receive discriminatory treatment for exercising the rights set forth in the table above. Unless permitted by the applicable State Privacy Law, we will not: (i) deny you goods or services; (ii) charge you different prices or rates for goods or services, including through granting discounts or other benefits, or imposing penalties; (iii) provide you with a different level or quality of goods or services; or (iv) suggest that you receive a different price or rate for goods or services or a different level or quality of goods or services. However, if the exercise of these rights limits our ability to process personal information (such as in the case of a deletion request) in certain contexts, we may no longer be able to provide you certain related products and services or engage with you in the same manner.

b. Shine the Light (California). If you have an established business relationship with us, you may have rights to know how your information is disclosed to third parties for their direct marketing purposes under California’s “Shine the Light” law (Civ. Code § 1798.83). To make such a request, please use the following email address: hello@getresonately.com or the following mailing address: Resonately, Inc. 700 Soldiers Field Road. Boston, MA 02163.

c. Submitting Rights Requests.

i. You may exercise your right to request access, deletion, and correction of your personal information (as such rights are described above) by emailing us at hello@getresonately.com.

ii. For the rights to opt-out of "sales," "shares," and processing of personal information for "targeted advertising," (as such rights are described above), please use the Your Privacy Choices link(referenced in the table above or otherwise activate the opt-out preference signal on the browsers or browser extensions that support such signal (for example, the GPC signal).

iii. As permitted by applicable law, we may require verification of your, or your authorized agent's, identity for security of your personal information (such as by requesting certain information that cross-references with information we have internally, or for authorized agents, ensuring that they are duly authorized by you, such as name, email address, zip code, keytag number, and first five digits of your payment method).

Except as provided for under applicable privacy laws, there is no charge to exercise any of your legal rights. However, if your requests are manifestly unfounded or excessive, in particular because of their repetitive character, we may (as permitted under applicable State Privacy Law): (i) Charge a reasonable fee taking in account the administrative costs of providing the information or taking the action requested; or (ii) refuse to act on the request and notify you of the reason for refusing the request.

d. Appeals. In the event that we decline to take action on a request exercising one of your rights set forth above, you may have the right to appeal our decision. To appeal a decision regarding a consumer rights request email us at hello@getresonately.com.

e. Authorized Agents. You are permitted to use an authorized agent to submit requests on your behalf through the designated methods set forth above, though we must verify the authorized agent's authority to act on your behalf before acting on such request. For requests to access, delete, and correct personal information, we require the following for verification purposes: (i) a power of attorney valid under the laws of the relevant state from you or your authorized agent; or (ii) sufficient evidence to show that you have: (a) provided the authorized agent signed permission to act on your behalf; and (b) verified your own identity directly with us.

f. Additional Data Processing Disclosures / Notice at Collection.

i. *List of categories of personal information collected*.

1. Identifiers, such as your name, e-mail address, date of birth, or other similar identifiers.
2. California Customer Records (Cal. Civ. Code § 1798.80(e)), such as birth date, contact information, and payment information.
3. Protected Classification Characteristics, such as age and gender.
4. Commercial Information, such as payment information and purchase history.
5. Internet/Network Information, such as device information, logs, and analytics data.
6. Non-Precise Geolocation Data, such as location information from your device or generated based on IP address or Wi-Fi.
7. Audio, Electronic, Visual or Other Sensory Information, such as photographs and audio/video recordings of our Facilities and call center.
8. Profession/Employment Information, such as your employer if your subscription is tied to an account managed by your employer.
9. Sensitive Personal Information, such as driver's license or other government identifiers, account log-in and password, or data concerning health.

Sensitive Personal Information is used for the limited purposes specified under the CCPA that do not require a corresponding opt-out right, such as the provision of goods or services reasonably expected by the consumer requesting such goods or services. For example, the Visitor's driver's license or similar identifier may be used to provide a guest pass or register for services, and limited health-related data (like height and weight) may be used to suggest a recommended workout routine or training regime.

ii. The purposes for which the categories of personal information are used (but see above for Sensitive Personal Information):

1. To provide our products or services;
2. To communicate with you about our products or services (or to communicate with you about products or services of third parties), such as in connection with renewing your subscription, updating your information, or informing you about new offerings from us or third parties;
3. To better understand your use of, and improve, our products and services, such as through internal research and generation/analysis of analytics data and usage trends;
4. To target you or others with advertising and to measure the effectiveness of such advertising campaigns, such as: (i) to market the Resonately's products or services to you (or the products or services of third parties) including through marketing e-mails or text messages, where applicable, and to alert you to special promotions, discounts, offers, and the like; or (ii) o match your use or purchase of Facilities, products, and services with your online activity on our Online Services (for example, we may connect your offline activity at our Facilities with activity on our Online Services or share the personal information you provide when you sign up for a membership with advertising/marketing and analytics partners to facilitate or track the effectiveness of advertising campaigns);
5. To assist with customer service or otherwise respond to requests;
6. To distribute surveys and collect feedback;
7. To facilitate transactions;
8. To coordinate sweepstakes and contests;
9. To protect the safety, security, and integrity of our Facilities, Visitors, and Online Services;
10. To monitor and prevent fraud;
11. To recognize you and your devices (for example, such as when you check-in at a Facility or when you use our Online Services);
12. To support employee training;
13. To conduct audits; and
14. To fulfill contractual obligations or otherwise take steps to effectuate or defend our rights.

iii. The following categories of personal information may be "sold" or "shared" (as such terms are broadly defined under the CCPA) to our advertising/marketing and analytics partners

for the purposes of advertising/ marketing and analytics services: Identifiers, Commercial Information, Geolocation Data, and Internet/Network Information. You may opt-out of these “sales” and “shares”.

iv. *Data Retention*. We retain the categories of personal information above as reasonably necessary to fulfill the purposes outlined in this notice, unless a longer retention period is required or permitted by law. In many situations, we must obtain all, or a portion, of your personal information to comply with legal obligations, resolve disputes, enforce our agreements, protect against fraudulent, deceptive, or illegal activity, or for another one of our business purposes.

15. How to Contact Us.

To ask questions or make comments about Privacy Policy and our privacy practices, you may contact us as follows:

Email: hello@getresonately.com

Mail: Resonately, Inc.
Attn: Privacy Officer
700 Soldiers Field Road
Boston, MA 02163