RESTASSURED ONLINE, LLC ("RAO")
Effective Date: JANUARY 1, 2020
WEBSITE AND MOBILE PRIVACY POLICY

RESTASSURED ONLINE, LLC ("**RAO**", "**we**" or "**us**") offers a telehealth platform that may be accessed through the RAO website ("**Site**") and its mobile application ("**App**") (collectively, the "**Platform**"). This Privacy Policy applies to the data collected through the Platform. By using the Platform, you consent that we may process the data that we collect from you in accordance with this Privacy Policy.

This Privacy Policy is incorporated into and made part of our Terms and Conditions of Use ("**Terms**"). We encourage you to review our Terms, because they contain important limitations on our liability to you when you use the Platform.

Our Data Collection Practices

When you use the Platform, we may ask you to provide certain "**Personal Data**", which means any data that can be used alone or in combination with other data to identify you (such as your name, email address and photograph). We also may collect "**Non-Personal Data**", which means data that we collect automatically about your use of the Platform but does not identify you (such as your IP Address, device ID, browser type and pages visited). Finally, we also collect "**Health Data**", which means data that does not necessarily identify you but we recognize may be more private to you than other data (see out HIPAA Privacy Policy for more information regarding this.).

We may collect your data when you:

- **Create an Account.** When you create an account on the Site or App, we ask for some Personal Data and Non-Personal Data, including but not limited to, your name, email address, birthdate, payment information, gender and mailing/physical address. Whenever you add this type of data, we collect it and store it in your account. Your email address will be your username, which you will use to log into and access your account.

- **Activate and use an App or Device.** You may need to download an App to access certain features of the Platform. In such event, you may be asked and enter information about yourself.

- **Use the Site.** When you use the Site through your computer or mobile device, we automatically collect Non-Personal Data about your visit through the use of cookies, web beacons, and other data collection technologies. To learn more about our data collection technologies and how we use them, see the "Data Collection Technologies" section below.

- **Contact Us.** We may collect your Personal Data, including your name, phone number, and email address, if you contact us with questions, concerns, or feedback via our online

form, through email, or by other means. When you contact us, we will only use your Personal Data to respond to your communication and fulfil your request.

Why We Collect Data

We use your data to provide you with customer service that we hope makes you feel supported, motivated and reassured. Here are some examples:

- Non-Personal Data is used for our internal business purposes so that we can understand and improve the Platform, troubleshoot Devices, and detect and protect against fraud and criminal activity.
- We may use your Personal Data for marketing and promotional use. This may include, but is not limited to, new products, newsletters, a new application to access your account, etc. You may opt out of receiving promotional/marketing communications at any time by emailing us at info@restassuredonline.com or clicking on the "Opt-out Link" within the promotional/marketing email.

How We May Share your Data

We only share your data with third parties in accordance with this Privacy Policy and under the following circumstances:

- **With Notice at the Time of Collection.** If we collect your data and intend to disclose it in a way not already disclosed in this Privacy Policy, we will notify you of such intended disclosure at the time of collection.

- **Service Providers.** We may share your data with companies that we contract with to help us deliver the Platform, such as email management, credit card processing, order fulfillment, technology hosting, and website analytics.

- **Business Transaction.** We may sell, transfer or otherwise share some or all of our assets to a third party in connection with a merger, acquisition, reorganization or sale of assets, or in the event of bankruptcy. In such event, your Personal Data and Health Data may be transferred to that third party.

- **As Required or Permitted by Law.** We may disclose your data as we, in our sole discretion, believe necessary or appropriate to respond to claims and legal process (including, but not limited to, subpoenas), to protect the property and rights of RAO or a third party, to protect the safety of the public or any person, or to prevent or stop activity we may consider to be, or to pose a risk of being, any illegal, unethical or legally actionable activity, and to otherwise to comply with law.

Data Collection Technologies

We and third parties acting on our behalf use various technologies that help us to manage the operations of the Platform and track usage behavior so that we can tailor information to make your visits more enjoyable and meaningful.

Our data collection technologies include:

- **Cookies:** Cookies are text files containing small amounts of information that are stored on your computer or mobile device's browser directory. Cookies are created when you visit a website that uses cookies to keep track of your movements within the website. Cookies are useful because they allow us to recognize your device, remember your preferences, automatically log you in to your account, and provide us with information that we can use to further personalize your user experience. You can find more information about cookies at www.allaboutcookies.org.
- **Web beacons and GIFs:** Certain pages on the Platform contain web beacons (also known as web bugs, pixel tags and clear GIFs), which we use to monitor how users use the Site. We use web beacons in combination with Cookies to understand how our users navigate through and process the content contained on our Website.
- **Local Storage and Local Shared Objects:** We use local shared objects (LSOs) such as Flash Cookies and local storage, such as HTML5 Local Storage, to enhance user experience by, for example, storing your user preferences and settings (e.g., volume/mute) in connection with animated content on the Platform. Local storage is similar to browser cookies but can store data more complex than simple text. By itself, local storage cannot do anything to or with the data stored on your device. Like cookies, local storage can only access personal data that you have provided on the Platform. Third parties with whom we partner to provide certain features on the Platform or to display advertising based upon your web browsing activity also use Flash cookies or HTML5 to collect and store information. Various browsers may offer their own management tools for removing HTML5.

Your browser may allow you to manage your cookies and local storage. Because each browser is a little different, we encourage you to check your browsers' "Help" feature to learn how to block cookies, how to receive notification of new cookies, and how to disable existing cookies. For more information about managing cookies, please visit www.allaboutcookies.org/manage-cookies/.

Children's Privacy

The Platform is not directed to children under the age of 18, and RAO does not knowingly collect any Personal Data from children under 18. If you are aware of a child providing his or her Personal Data, please contact us at info@restassuredonline.com. We will endeavor to delete all data we collected from a child under 18.

Changes to this Privacy Policy

The Effective Date of this Privacy Policy is set forth at the top of this page. Because we are always looking for innovative ways to help you monitor your health, this Privacy Policy may

change over time. If any modifications materially change your rights, we will notify you of these changes either by posting notice on the Platform or by sending you an email to the email address we have on file for you. By continuing to access or use the Platform after such changes take effect, you agree to be bound by the modified Privacy Policy. The amended terms of the Privacy Policy supersede all previous versions of or agreements, notices or statements about the Privacy Policy.

Security

We employ reasonable security measures designed to safeguard the Personal Data under our control from unauthorized access, use, and disclosure. Despite these measures, the confidentiality of your Personal Data cannot be guaranteed. We encourage you to take appropriate steps to protect your Personal Data, such as using a password that is not easy to guess. If you have a security related question or concern, please contact us at info@restassuredonline.com.

How to Access, Modify or Delete Data

Personal Data that you provide to us may be modified by accessing your account and profile and changing the data stored within. Please note that if you remove data from your account, it will no longer be visible to you. If you have any questions about accessing, modifying or deleting your data, please contact us at info@restassuredonline.com.

Your California Rights (See CA Website Policy below by clicking "here")

Under California Civil Code §1798.83, RAO is required, once per calendar year and upon request, to disclose to California residents: (i) the identity of any third party to whom we disclosed Personal Data within the previous calendar year for the third party's direct marketing purposes; and (ii) the type of Personal Data disclosed. To request such information, please send an email to info@restassuredonline.com with the subject line "California Privacy Rights" or write us at the following address:

- RESTASSURED ONLINE, LLC
  Attn: California Privacy Rights
  13401 RAILWAY DR.
  OKC, OK 73104

PRIVACY INFORMATION FOR NEVADA RESIDENTS

Under Nevada law, certain Nevada consumers may opt out of the sale of "personally identifiable information" for monetary consideration (as such terms are defined under Nevada law) to a person for that person to license or sell such information to additional persons. We do not engage in such activity; however, if you are a Nevada resident who has purchased services from us, you may submit a request to opt out of any potential future sales under Nevada law by info@restassuredonline.com . Please note we will

take reasonable steps to verify your identity and the authenticity of the request. Once verified, we will maintain your request in the event our practices change.

Notice to our International Users

The Platform is hosted in the United States and subject to U.S. law. If you are accessing the Platform from outside the United States, please be advised that U.S. law may not offer the same privacy protections as the law of your jurisdiction. By accessing and using the Platform, you consent to the transfer to and processing of your Personal Data in the United States.

Contact Us

You can email or write to us with any questions or comments at the following contact information:

- RESTASSURED ONLINE ,LLC
  Attn: WEBSITE PRIVACY OFFICER
  13401 RAILWAY DR.
  OKC, OK 73104
  info@restassuredonline.com

WEBSITE AND MOBILE PRIVACY NOTICE FOR CALIFORNIA RESIDENTS

CCPA Effective Date: January 1, 2020

This PRIVACY NOTICE FOR CALIFORNIA RESIDENTS supplements the information contained in the WEBSITE and MOBILE Privacy Policy of RESTASSURED ONLINE, LLC (collectively, "we," "us," or "our") and applies solely to visitors, users, and others who reside in the State of California ("consumers" or "you"). We provide this notice under: (1) effective as of the CCPA Effective Date, the California Consumer Privacy Act of 2018, Cal. Civ. Code § 1798.100 et seq., as amended or supplemented from time to time ("CCPA"), and (2) California's "Shine the Light" law, Cal. Civ. Code § 1798.83. Any terms defined in the CCPA have the same meaning when used in this notice.

As of the CCPA Effective Date the California regulations implementing the CCPA had not been promulgated. Accordingly, the details on how we are to provide notice to consumers, and verify and respond to them upon receiving a consumer request, is not yet clear. This notice and our initial CCPA compliance program reflect our good faith effort to interpret the law and are subject to revisions as regulatory guidance and industry consensus develops.

1. Our Personal Information Practices

Information We Collect

We collect information that identifies, relates to, describes, references, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular patient ("personal information").

Category	Brief Description
A. Identifiers	A real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, or other similar identifiers.
B. Personal Records	A name, signature, physical characteristics or description, address, telephone number,, employment, employment history, bank account number, credit card number, debit card number, or any other financial information, medical information, or health insurance information. Some personal information included in this category may overlap with other categories.
C. Protected classification characteristics under California or federal law	Age (40 years or older), race, color, ancestry, 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, genetic information (including familial genetic information).

Personal information does not include:

- Publicly available information from government records.
- De-identified or aggregated consumer information.
- Information excluded from the CCPA's scope, like:
    - health or medical information covered by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the California Confidentiality of Medical Information Act (CMIA) or clinical trial data;
    - personal information covered by 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.

We obtain the categories of personal information listed above from the following categories of sources:

- Directly from our patients from our website and portal.
- Directly and indirectly from activity on our websites.

Use of Personal Information

We may use or disclose the personal information we collect for one or more of the following business purposes:

- To fulfill or meet the reason for which the information is provided. For example, if you provide us with personal information to order products or services, we will use that information to fulfill the order.
- To provide you with email and other notices concerning our products or services, or products or services of third parties, that may be of interest to you.
- To carry out our obligations and enforce our rights arising from any transactions and the relationship between you and us, including for billing and collection.
- To improve our websites and present advertising and content to you.

- For testing, research, analysis and product development.
- To respond to law enforcement requests and as required by applicable law, court order, or governmental regulations.
- As described to you when collecting your personal information or as otherwise set forth in our Privacy Policy or the CCPA.
- To evaluate or conduct a merger, divestiture, restructuring, reorganization, dissolution, or other sale or transfer of some or 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 is among the assets transferred.

Sharing Personal Information

We may disclose your personal information to a third party for a business purpose as set forth in the CCPA, including as follows (parenthetical references are to subsections of CCPA § 1798.140(d)):

Auditing (1)	Categories A, B, E, F & G
Short-term, transient use (4)	Categories A, B, E, F & G
Performing services (5)	Categories A – G
Research for technological development (6)	Categories A, B, E, F & G
To verify or maintain quality or safety (7)	Categories A, B, E, F & G

When we disclose personal information for a business purpose, we enter into a contract for that purpose requiring the recipient to keep that personal information confidential and only use it as necessary to perform the business purpose, or as otherwise permitted by applicable law.

We disclose your personal information for a business purpose to the following categories of third parties:

- Our affiliates.
- Service providers.
- Third parties to whom you or your agents authorize us to disclose your personal information in connection with products or services we provide to you.

There is not currently a consensus as to whether or not collection of your data and disclosure of it to third parties by cookies and other tracking technologies should be deemed a sell of your personal information by us under the CCPA. However, we use one or more types of technology to signal to cookie operators when a device you use has registered a do not sell request with us, and we may offer you other ways to control cookies associated with our services. We are not responsible for the effectiveness of these tools or the manner in which third parties treat your choices or our signals. For more information on cookies and your choices regarding them, including how to opt-out of certain interest-based advertising, see our Privacy Policy.

1. Your Rights and Choices

The CCPA provides California consumers with specific rights regarding their personal information. This section describes your CCPA rights and explains how to exercise those rights from and after the CCPA Effective Date.

Do Not Sell
You have the right to opt out of the sale of your personal information. Once we receive and confirm your verifiable consumer request, we will refrain from selling personal information we collected about you; provided, however with respect to cookies your do not sell request to us will result in our use of one or

more types of technology to signal to cookie operators when a device you used at the time of opt-out has registered a do not sell request with us, and we may offer you other ways to control cookies associated with our services. We are not responsible for the effectiveness of these tools or the manner in which third parties treat your choices or our signals. For more information on cookies and your choices regarding them, including how to opt-out of certain interest-based advertising, see our Privacy Policy above.

Access to Specific Information

You have the right to request that we disclose certain information to you about our collection and use of your personal information over the past 12 months. Once we receive and confirm your verifiable consumer request, we will disclose to you as you requested:

- 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 or selling that personal information.
- The categories of third parties with whom we share that personal information.
- The specific pieces of personal information we collected about you (a data portability request).
- If we sold or disclosed your personal information for a business purpose, two separate lists disclosing:
    - sales, identifying the personal information categories that each category of recipient purchased; and
    - disclosures for a business purpose, identifying the personal information categories that each category of recipient obtained.

Deletion Request Rights

You have the right to request that we delete any of your personal information that we collected from you and retained, subject to certain exceptions. Once we receive and confirm your verifiable consumer request, we will delete (and direct our service providers to delete) your personal information from our records, unless an exception applies.

We may deny your deletion request if retaining the information is necessary for us or our service providers to:

- Complete the transaction for which we collected the personal information, provide a good or service that you requested, take actions reasonably anticipated within the context of our ongoing business relationship with you, or otherwise perform our contract with you.
- Detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity, or prosecute those responsible for such activities.
- Debug products to identify and repair errors that impair existing intended functionality.
- Exercise free speech, ensure the right of another consumer to exercise their free speech rights, or exercise another right provided for by law.
- Comply with the California Electronic Communications Privacy Act (Cal. Penal Code § 1546 *seq.*).
- Engage in public or peer-reviewed scientific, historical, or statistical research in the public interest that adheres to all other applicable ethics and privacy laws, when the information's deletion may likely render impossible or seriously impair the research's achievement, if you previously provided informed consent.
- Enable solely internal uses that are reasonably aligned with consumer expectations based on your relationship with us.
- Comply with a legal obligation.
- Make other internal and lawful uses of that information that are compatible with the context in which you provided it.

Exercising Do Not Sell, Access and Deletion Rights

To exercise the do not sell, access and deletion rights described above from and after the CCPA Effective Date, please submit a verifiable consumer request to us as follows:

Do Not Sell

- Email us at info@restassuredonline.com
- Write to us at RESTASSURED ONLINE, LLC 13401 RAILWAY DR., OKC, OK 73104 Attn: CCPA Do Not Sell

Access Requests

- Email us at info@restassuredonline.com
- Write to us at RESTASSURED ONLINE, LLC 13401 RAILWAY DR., OKC, OK Attn: CCPA Access Requests

Deletion Requests

- Email us at info@restassuredonline.com
- Write to us at RESTASSURED ONLINE, LLC 13401 RAILWAY DR., OKC, OK Attn: CCPA Deletion Requests

Follow the instructions that you will be provided to help us verify you and respond to your requests.

Only you or an authorized agent verified to act on your behalf, may make a verifiable consumer request related to your personal information. You may also make a verifiable consumer request on behalf of your minor child.

You may only make a verifiable consumer request for access twice within a 12-month period. The verifiable consumer request must:

- Provide sufficient information that allows us to reasonably verify you are the person about whom we collected personal information or an authorized representative. We may require an authorized representative both to verify their identity and submit proof they have been authorized by the consumer to act on the consumer's behalf.
- Describe your request with sufficient detail that allows us to properly understand, evaluate, and respond to it.

We cannot respond to your request or provide you with personal information if we cannot verify your identity or authority to make the request and confirm the personal information relates to you. Making a verifiable consumer request does not require you to create an account with us. We will only use personal information provided in a verifiable consumer request to verify the requestor's identity or authority to make the request.

Response Timing and Format

We endeavor to respond to a verifiable consumer request within 45 days of its receipt. If we require more time (up to 90 days), we will inform you of the reason and extension period in writing. If you have an account with us, we will deliver our written response to that account, or by mail or electronically. If you do not have an account with us, we will deliver our written response by mail or electronically. Any disclosures we provide need only cover the 12-month period preceding the verifiable consumer request's receipt. The response we provide will also explain the reasons we cannot comply with a request, if applicable. For data portability requests, we will provide your personal information in a standard CSV file.

We do not charge a fee to process or respond to your verifiable consumer request unless it is excessive, repetitive, or unfounded, in which case we may limit the response and/or condition it on payment of our costs. 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.

Non-Discrimination

We will not discriminate against you for exercising any of your CCPA rights. Unless permitted by the CCPA, we will not:

- Deny you goods or services.
- Charge you different prices or rates for goods or services, including through granting discounts or other benefits, or imposing penalties.
- Provide you a different level or quality of goods or services.
- Suggest that you may receive a different price or rate for goods or services or a different level or quality of goods or services.

Changes to this Privacy Notice

We reserve the right to amend this privacy notice at our discretion and at any time. When we make changes to this privacy notice, we will update the date of this notice below. Please bookmark this page and check it periodically. We will post any changes online.

Contact Information

If you have any questions or comments about this notice, our Privacy Policy, the ways in which we collect and use your personal information, your choices and rights regarding such use, or wish to exercise your rights under California law, please contact us through the means set forth above for Do Not Sell requests under "*Exercising Do Not Sell, Access and Deletion Rights*".