

NurseContact Inc. (“NurseContact”) provides this Privacy Policy to let you know our policies and procedures regarding the collection, use and disclosure of information through www.nursecontact.com (the “Site”), and any other websites, features, applications, widgets or online services that are owned or controlled by Pharmaneek and that post a link to this Privacy Policy (together with the Site, the “Service”), as well as any information NurseContact collects offline in connection with the Service. It also describes the choices available to you regarding the use of, your access to, and how to update and correct your personal information. This Privacy Policy incorporates by reference the NurseContact Data Processing Agreement. Note that we combine the information we collect from you from the Site, through the Service generally, or offline.

Please note that certain features or services referenced in this Privacy Policy may not be offered on the Service at all times. Please also review our Terms of Service, which governs your use of the Service.

We’ve provided short summaries in this Privacy Policy to help you understand what information we collect, how we use it, and what choices or rights you may have. While these summaries help explain some of these concepts in a simple and clear way, we encourage you to read the entire Privacy Policy to understand our data practices.

1. INFORMATION COLLECTION

Users of the Service may be Clients, TeleHealth Professionals, or Agencies (as each is defined in the [User Agreement](#)).

Information You Provide to Us

When you use the Service, you may provide us with information about you. This may include your name and contact information, financial information to make or receive payment for services obtained through the NurseContact platform, or information to help us fill out tax forms. When you use the Service, we may also collect information related to your use of the Service and aggregate this with information about other users. This helps us improve our Services for you. You may also provide us with information about your contacts or friends if, for example, you’d like to add those contacts to a message room. Agencies may also provide us with information about TeleHealth Professionals associated with the Agency.

Personal Information: In the course of using the Service (whether as a Client or Qualified Health Professional or Agency), we may require or otherwise collect information that identifies you as a specific individual and can be used to contact or identify you (“Personal Information”). Examples of Personal Information include your name, email address, company address, billing address, and phone number.

Payment Information: If you use the Service to make or receive payments, we will also collect certain payment information, such as credit card or other financial account information, and billing address.

Identity Verification: We may collect Personal Information, such as your date of birth or taxpayer identification number, to validate your identity or as may be required by law, such as to complete tax filings. We may request documents to verify this information, such as a copy of your government-issued identification or photo or a billing statement.

General Audience Service: The Service is general audience and intended for users 18 and older. We do not knowingly collect Personal Information from anyone younger than age 18. If we become aware that a child younger than 18 has provided us with Personal Information, we will use commercially reasonable efforts to delete such information from our files. If you are the parent or legal guardian of a child younger than age 18 and believe that NurseContact has collected Personal Information from your child, please contact us at: info@NurseContact.com.

Non-Identifying Information/Usernames: We also may collect other information, such as zip codes, demographic data, information regarding your use of the Service, and general project-related data ("Non-Identifying Information"). We may aggregate information collected from NurseContact registered and non-registered users ("NurseContact Users"). In some cases, we may render Personal Information (generally, email address) into a form of Non-Identifying Information referred to in this Privacy Policy as "Hashed Information." This is typically accomplished using a mathematical process (commonly known as a hash function) to convert information into a code. The code does not identify you directly, but it may be used to connect your activity and interests.

Combination of Personal and Non-Identifying Information: Certain Non-Identifying Information would be considered a part of your Personal Information if it were combined with other identifiers in a way that enables you to be identified (for example, combining information with your name). But the same pieces of information are considered Non-Identifying Information when they are taken alone or combined only with other non-identifying information (for example, your viewing preferences). We may combine your Personal Information with Non-Identifying Information, but NurseContact will treat the combined information as Personal Information.

Collection of Third-Party Personal Information: We collect the following personal information from you about your contacts or friends: (1) First name, (2) last name, and (3) email address when you provide it to us for the purpose of adding your contacts to a message room.

You do not have a statutory obligation to provide us with any information, but you may have a contractual obligation to do so, and if we do not receive certain information from you, then we will not be able to provide our Service to you. If you have any questions regarding whether provision of information is mandatory and the consequences for withholding such information, please contact us using the contact information below.

Information Received from Third Parties

Third parties may also give us information about you. If we combine that information with information about you collected through the Service, we will still treat that combined information as set forth in this Privacy Policy.

We also may receive information about you from third parties. For example, we may supplement the information we collect with outside records or third parties may provide information in connection with a co-marketing agreement or at your request (such as if you choose to sign in with a third-party service). If we combine the information we receive from others with information we collect through the Service, we will treat the combined information as described in this Privacy Policy.

Information Collected Automatically

Like other online companies, we receive technical information when you use our Services. We use these technologies to analyze how people use the Service, to improve how our Site functions, to save your log-in information for future sessions, and to serve you with advertisements that may interest you.

We and our third-party service providers, including analytics and third-party content providers, may automatically collect certain information from you whenever you access or interact with the Service. This information may include, among other information, the browser and operating system you are using, the URL or advertisement that referred you to the Service, the search terms you entered into a search engine that led you to the Service, areas within the Service that you visited, which links you clicked on, which pages or content you viewed and for how long, other similar information and statistics about your interactions, such as content response times, download errors and length of visits to certain pages and other information commonly shared when browsers communicate with websites. We may combine this automatically collected log information with other information we collect about you. We do this to improve services we offer you, and to improve marketing, analytics, and site functionality.

The information we collect also includes the Internet Protocol (“IP”) address or other unique device identifier (“Device Identifier”) for any device (computer, mobile phone, tablet, etc.) used to access the Service. A Device Identifier is a number that is automatically assigned or connected to the device you use to access the Service, and our servers identify your device by its Device Identifier. Some mobile service providers may also provide us or our third-party service providers with information regarding the physical location of the device used to access the Service.

NurseContact and its partners use cookies or similar technologies to analyze trends, administer the website, track users’ movement around the website, the desktop app, and the mobile app, and to gather demographic information about our user base as a whole. The technology used to collect information automatically from NurseContact Users may include the following:

Cookies: Like many websites, we and our marketing partners, affiliates, analytics, and service providers use “cookies” to collect information. A cookie is a small data file that we transfer to your computer’s hard disk for record-keeping purposes. We use both persistent cookies that remain on your computer or similar device (such as to save your registration ID and login password for future logins to the Service and to track your compliance with the NurseContact Terms of Service) and session ID cookies, which expire at the end of your browser session (for example, to enable certain features of the Service, to better understand how NurseContact Users interact with the Service and to monitor aggregate usage by NurseContact Users and web traffic routing on the Service). You can control the use of cookies at the individual browser level, but if you choose to disable cookies, it may limit your use of certain features or functionality of the Service. For further information on cookies and how they are used for the Service, please read our Cookie Policy.

Web Beacons: We and our marketing partners, affiliates, analytics, and service providers may also employ software technology known as “web beacons” and/or “tracking tags” to help us keep track of what content on our Service is effective and to serve relevant advertising to you. Web beacons are small graphics with a unique identifier that may be invisible to you, and which are used to track the online activity of Internet users. Web beacons are embedded in the web pages you review or email messages you receive. Web beacons or similar technologies may be used for a number of purposes, including, without limitation, to count visitors to our Service, to monitor how NurseContact Users navigate the

Service, to count how many emails that were sent were actually opened, or to count how many particular articles or links were actually viewed.

Embedded Scripts: We and our marketing partners, affiliates, analytics, and service providers may also employ software technology known as an Embedded Script. An Embedded Script is programming code that is designed to collect information about your interactions with the Service, such as the links you click on. The code is temporarily downloaded onto your computer or other device and is deactivated or deleted when you disconnect from the Service.

In addition, we and our marketing partners, affiliates, analytics, and service providers may use a variety of other technologies (such as tags) that collect similar information for security and fraud detection purposes, and we may use third parties to perform these services on our behalf.

HOW WE RESPOND TO DO-NOT-TRACK SIGNALS

NurseContact does not respond to Do-Not-Track signals.

Please note that your browser setting may allow you to automatically transmit a “Do Not Track” signal to websites and online services you visit. There is no consensus among industry participants as to what “Do Not Track” means in this context. Like many websites and online services, NurseContact does not alter its practices when it receives a “Do Not Track” signal from a visitor’s browser. To find out more about “Do Not Track,” please visit <http://www.allaboutdnt.com>.

The General Data Protection Regulation: Data Processing Agreement

To streamline compliance with the General Data Protection Regulation (“GDPR”), NurseContact has posted a Data Processing Agreement (“DPA”) governing the relationship between the Customer (as defined in the DPA) acting as a data controller or processor, as applicable (and as defined in the DPA), of personal data under European Data Protection Legislation; and NurseContact (acting as a data processor or subprocessor, as applicable).

Unless otherwise agreed to in writing by you and NurseContact, to the extent NurseContact processes any EU personal data for you as a controller (as defined by the General Data Protection Regulation (EU) 2016/679) in your role as a Customer, the Data Processing Agreement applies.

Work Diaries and Work View

We collect information about a Qualified Health Professional’s work for a Client, including automatically collected information about work on a particular project. If a Qualified Health Professional enables Work Diaries, we will share Work Diaries with the relevant Client and Agency. We tell TeleHealth Professionals when we are capturing information for the Work Diary and allow TeleHealth Professionals to block such data sharing.

As part of the Service, when enabled by a Qualified Health Professional, we collect information about a Qualified Health Professional’s work on a project for a Client. This feature is known as Work Diary. Work Diaries include information provided by the Qualified Health Professional, such as a memo, as well as automatically gathered information about work on a project, such as number of mouse clicks and keyboard strokes and regularly taken screenshots (which may include a webcam picture of you if you

have enabled this feature in your settings). In order to use Work Diaries, you must download and install the Team App software from www.NurseContact.com.

We will share information contained in Work Diaries with the relevant Client and with any manager or administrator of any applicable Qualified Health Professional Agency. We inform TeleHealth Professionals each time we capture information for Work Diary. As set forth in our Terms of Service, End User License Agreement, and help pages on the Site, a Qualified Health Professional may choose to block or delete the screen shot and associated data for a recorded work interval, but then the Qualified Health Professional may not be paid for that work interval. NurseContact may use de-identified or aggregated information from Work Diaries for statistical analysis, product development, marketing and research.

User Profiles

TeleHealth Professionals may create a profile, with certain or all information publicly available. Clients and Agencies may also create organization profiles.

You may have the opportunity to create a profile, which consists of information about you, and may include Personal Information, photographs, examples of your work, information on work previously performed via the Service and outside the Service, skills, tests taken, test scores, hourly pay rates and earnings information, feedback/rating information and other information, including your username ("Profile"). The information in your Profile may be visible to all NurseContact Users and the general public subject to the privacy choices you make within your NurseContact Profile. You may edit certain information in your Profile via your account and may choose to limit who is able to view certain content you post to your Profile. Clients and Agencies of associated individual users or companies may also have the opportunity to create an organization Profile. If, in any case, you believe that an unauthorized profile has been created about you, you can request for it to be removed by contacting us at info@NurseContact.com.

Identity Verification

We place a premium on trust in our Service, so we may take steps to verify your identity.

Before a Qualified Health Professional can complete registration on the Service, or at any time thereafter, we may request or re-request identity verification. Without limiting the manner in which we request identity verification, we may require TeleHealth Professionals to participate in a video call after submitting their government issued ID to enable us to confirm that the Qualified Health Professional is indeed the individual in the ID. We may record such video calls and take screenshots of the user during the call. NurseContact may use the information obtained from Identity Verification for purposes of verifying your identity, enforcing our Terms of Service and other agreements, and preventing fraud.

Messaging

TeleHealth Professionals, Agencies, and Clients may communicate with each other through the Service. For example, TeleHealth Professionals, Agencies, and Clients may wish to discuss Client needs and Qualified Health Professional work proposals. If you communicate with an Agency or Client, that Agency or Client will also be a "data controller" with respect to such communications.

Community Forums

We may offer public forums or blogs. If you participate, your comments and questions will be publicly displayed.

The Service may provide you the opportunity to participate and post content publicly in forums, on blogs, through interactive features on NurseContact and through other communication functionality (“Community Forums”). You may choose, through such features or otherwise, to submit or post questions, comments, or other content (collectively, “User Forum Content”). Please note that certain information, such as your name and Profile may be publicly displayed on the Service along with your User Forum Content. Please note that your use of Community Forums is subject to the NurseContact Forum Rules and our Terms of Service.

Note that anything you post to a Community Forum is public — others will have access to your User Forum Content and may use it or share it with third parties. If you choose to voluntarily disclose Personal Information in your User Forum Content or use Community Forums to link to your Profile, that information will be considered public information and the protections of this Privacy Policy will not apply.

To request removal of your personal information from our blog or community forum, contact us at info@NurseContact.com. In some cases, we may not be able to remove your Personal Information, in which case we will let you know if we are unable to do so and why.

Testimonials

We display personal testimonials of satisfied customers on our Service, in addition to other endorsements. With your consent we may post your testimonial along with your name. If you wish to update or delete your testimonial, you can contact us at info@NurseContact.com.

Work Listings Through the Service

If you choose to post a work listing via the Service as a Client, the contents of such listing will be viewable publicly, unless you designate the listing as only viewable through the Service or as private using the settings available on the applicable website. Work listings include information such as budget, location, history of work listing(s) by the Client, the names of other TeleHealth Professionals performing work for the Client, Client feedback and rating information and timing of project performance.

Feedback

We collect feedback from NurseContact Users about their experience with other NurseContact Users of our Service. Please note that any feedback you provide via the Service or feedback provided about you is publicly viewable via the Service. On very rare occasions, we may remove feedback pursuant to the relevant provisions of our Terms of Service, including the Terms of Use.

Email to Friends and Referral Program

NurseContact lets you send project postings to friends via email. NurseContact also offers the ability to send friends emails about providing or purchasing services through the Service. If you choose to use either feature, your friend’s email address will be used to send the requested posting and your email address will be used to copy you on the message to your friend or to send the message on your behalf.

NurseContact stores this information for the sole purpose of sending this one-time email and tracking the success of our referral program.

Your friend may contact us at info@NurseContact.com to request that we remove this information from our database.

Social Networking Services

You may register for an account directly with our Site, or through a social networking service. If you register with a social networking service (or later link your account to one), we will collect certain information about you from that social networking service, and what we collect depends on your privacy settings with that social networking service. The Service may also allow you to “like” or share content with social networking services.

You may register to join the Service directly via the Service or by logging into your account with a third-party social networking service (“SNS”) via our Service (e.g., Facebook, Github and other third-party services that let you sign in using your existing credentials with those services). If you choose to register via an SNS, or to later link your account with the Service to your account with an SNS, we will use the Personal Information you have provided to the SNS (such as your name, email address, gender and other information you make publicly available via the SNS) to create your account. Note that the information we collect from and through an SNS may depend on the privacy settings you have set with the SNS and the permissions you grant to us in connection with linking your account with the Service to your account with an SNS. Other than what we may share with the SNS as described below, the Personal Information an SNS has about you is obtained by the SNS independent of our Service, and NurseContact is not responsible for it.

The NurseContact Service also may permit additional interactions between it and a third-party website, service, or other content provider, such as enabling you to “like” or share content to a third-party SNS. If you choose to “like” or share content, or to otherwise share information from or via our Service with a third-party site or service, that information may be publicly displayed, and the third-party may have access to information about you and your use of our Service (and we may have access to information about you from that third-party). These features may collect your IP address, which page you are visiting on our site, and may set a cookie to enable the feature to function properly. Your interactions with third parties through an SNS or similar features are governed by the respective privacy policies of those third parties.

You represent that you are entitled to use your SNS account for the purposes described herein without breach by you of any of the terms and conditions that govern the SNS, and without obligating NurseContact to pay any fees or making NurseContact subject to any usage limitations imposed by such SNS. You can disable the link between your NurseContact account and your SNS account at any time through the “Settings” section of our Service. Please note that your relationship with any SNS is governed solely by your agreement(s) with such SNS. If your SNS account terminates, then functions enabled through the link between your NurseContact account and your SNS account will terminate as well.

2. USE OF INFORMATION

We use information collected through the Service to provide and improve the Service, process your requests, prevent fraud, provide you with information and advertising that may interest you, comply with the law, and as otherwise permitted with your consent.

WE USE INFORMATION WE COLLECT:

- To provide and improve the Service, complete your transactions, address your inquiries, process your registration, verify the information you provide is valid, and for compliance and internal business purposes.
- To contact you with administrative communications and NurseContact newsletters, marketing or promotional materials (on behalf of NurseContact or third parties) and other information that may be of interest to you. If you decide at any time that you no longer wish to receive such communications from us, please follow the instructions in the Your Choices and Rights section, below.
- To tailor content we display to you and offers we may present to you, both on the Service and elsewhere online.
- To administer and develop our business relationship with you and, if applicable, the corporation or other legal entity you represent.
- To assess your proposal to perform a freelance project for NurseContact and prepare related governmental and internal statistics reports.
- To enforce and comply with the law, including to conduct an investigation, to protect the property and rights of NurseContact 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, illegal, fraudulent, unethical or legally actionable activity. We may also use Device Identifiers to identify NurseContact Users.
- For the purposes disclosed at the time you provide your information, with your consent, and as further described in this Privacy Policy.

We use your Personal Information for the purposes described above:

- *To Honor Our Contractual Commitments to You.* Much of our processing of Personal Information is to meet our contractual obligations to our investors, or to take steps at Users' request in anticipation of entering into a contract with them.
- *For Our Legitimate Interests.* In many cases, we handle Personal Information on the grounds that it furthers our legitimate interests in commercial activities, such as the following, in ways that are not overridden by the interests or fundamental rights and freedoms of the affected individuals:
 - Providing our Site and Service.
 - Analyzing and improving our business.

- Communications, including marketing and responding to your inquiries about our services.
 - Addressing information security needs and protecting our Users, NurseContact, and others.
 - Managing legal issues.
- *To Comply with Legal Obligations.* We need to use and disclose Personal Information in certain ways to comply with our legal obligations.

3. DATA RETENTION

Unless you request that we delete certain information (see Your Choices and Rights below), we retain the information you submit to verify your identity for 30 days and we retain other information we collect for at least 5 years. Your information may persist in copies made for backup and business continuity purposes for additional time. If you choose to provide us with Personal Information, we encourage you to routinely update the data to ensure that we have accurate and up-to-date information about you.

4. INFORMATION SHARING AND DISCLOSURE

We may share information about you to provide the Services, for legal and investigative purposes, in connection with sweepstakes and promotions, or if we are part of a merger or acquisition. We may also share non-identifying information with third parties. You have choices as to whether we share your personal information with third parties for their own marketing purposes.

We may share aggregated Non-Identifying Information and we may otherwise disclose Non-Identifying Information (including, without limitation, Hashed Information) to third parties. We do not share your Personal Information with third parties for those third parties' marketing purposes unless we first provide you with the opportunity to opt-in to or opt-out of such sharing. We may also share the information we have collected about you, including Personal Information, as disclosed at the time you provide your information, with your consent, as otherwise described in this Privacy Policy, or in the following circumstances:

Information about TeleHealth Professionals Shared with Clients, Agencies, NurseContact Payroll Vendors, and Partners of The NurseContact Foundation Initiative: We share information regarding TeleHealth Professionals who have entered into a contract with a Client or who have elected to participate in NurseContact Payroll, including information in Work Diaries and work history, with Clients, Agencies and NurseContact Payroll vendors. Note that if a Qualified Health Professional is suspended from the NurseContact Service, we may share that information with Clients for whom that Qualified Health Professional has worked or submitted proposals for work. We may also share information with Agencies to whom TeleHealth Professionals are associated for a particular work project. If you choose to view a job post or submit a proposal for work as a Qualified Health Professional via the Service, we may share relevant information with the applicable Client(s), including, but not limited to, the information contained in your Qualified Health Professional Profile. If you choose to participate in The NurseContact Foundation Initiative as a Qualified Health Professional, we may share information relevant to your participation in the program with partners of NurseContact who provide support to TeleHealth Professionals through that program.

Information about Clients and Agencies Shared with TeleHealth Professionals: If you have entered into a service contract or agreed to use NurseContact Payroll with another user, we may provide him/her with your name, company address, billing address, or tax ID or VAT number in order to complete the transaction or to facilitate the resolution of a claim or dispute. The user receiving your information is not allowed to use it for purposes unrelated to the transaction, such as to contact you for marketing purposes, unless you have expressly consented to it.

Service Providers: We may employ third-party companies and individuals to facilitate our Service, to provide the Service on our behalf, to perform Service-related services (e.g., without limitation, maintenance services, database management, web analytics and online advertising, payment processing, fraud detection and improvement of NurseContact's features) or to assist us in analyzing how our Service is used. These third parties may have access to your Personal Information in order to perform these tasks on our behalf.

What Happens If You Agree to Receive Information from Third Parties or Request that We Share Your Information: You may be presented with an opportunity to receive information and/or marketing offers from one or more third parties. If you agree at that time to have your Personal Information shared, your Personal Information will be disclosed to that third-party (or parties) and will be subject to the privacy policy and practices of that third-party. We are not responsible for the privacy policies and practices of third parties, and, if you later decide that you no longer want to receive communications from a third-party, you will need to contact that third-party directly. You also may request, sometimes through your use of an SNS or similar interactive feature or third-party application, that we share information about you with a third-party and we will typically do so under those circumstances.

Legal and Investigative Purposes: NurseContact will share information with government agencies as required by law in response to lawful requests by public authorities, including to meet national security or law enforcement requirements and, including without limitation, in connection with reporting earnings. We cooperate with government and law enforcement officials and private parties to enforce and comply with the law. We will disclose information about you to government or law enforcement officials or private parties as we, in our sole discretion, believe necessary or appropriate to respond to claims and legal process (including but not limited to subpoenas), or, at the request of governmental authorities or other third parties conducting an investigation where we determine in our sole discretion the disclosure is necessary to (a) protect the property and rights of NurseContact or a third-party, (b) protect the safety of the public or any person, or (c) prevent or stop activity we may consider to be, or pose a risk of being, illegal, fraudulent, unethical or legally actionable activity.

Internal and Business Transfers: NurseContact may share information, including Personal Information, with its parent company NurseContact Inc., and any current or future subsidiaries or affiliates, primarily for business and operational purposes. We may sell, transfer, or otherwise share some or all of our assets, including your Personal Information, in connection with a merger, acquisition, reorganization or sale of assets (including, in each case, as part of the due-diligence process with any potential acquiring entity) or in the event of bankruptcy.

Sweepstakes, Contests, and Promotions: We may offer sweepstakes, contests, and other promotions (any, a "Promotion") that may require registration. By participating in a Promotion, you are agreeing to the official rules that govern that Promotion, which may contain specific requirements of you, including, except where prohibited by law, allowing the sponsor(s) of the Promotion to use your name, voice,

likeness, or other indicia of persona in advertising or marketing associated with the Promotion. If you choose to enter a Promotion, your Personal Information may be disclosed to third parties or the public in connection with the administration of such Promotion, including, without limitation, in connection with winner selection, prize fulfillment, and as required by law or permitted by the Promotion's official rules, such as on a winner's list.

5. THIRD-PARTY ANALYTICS PROVIDERS, AD SERVERS AND SIMILAR THIRD PARTIES

We may work with advertising agencies and vendors who use technology to help us understand how people use our Site. These vendors may use technologies to serve you advertisements that may interest you. You can choose to opt out of receiving interest-based advertising.

NurseContact works with (or may in the future work with) network advertisers, ad agencies, analytics service providers and other vendors to provide us with information regarding traffic on the Service, including pages viewed and the actions taken when visiting the Service; to serve our advertisements on other websites, within mobile apps and elsewhere online; and to provide us with information regarding the use of the Service and the effectiveness of our advertisements. Our service providers may collect certain information about your visits to and activity on the Service as well as other websites or services, they may set and access their own tracking technologies on your device (including cookies and web beacons), and may use that information to show you targeted advertisements. Some of these parties may collect Personal Information when you visit the Service or other online websites and services. We may also share certain Non-Identifying Information with these parties, including Hashed Information, in connection with the services they provide to us. If you wish to opt out of interest-based advertising, click [here](#) (or if located in the European Union, click [here](#)). If you choose to opt out, please note you will continue to receive generic ads.

While we may use a variety of service providers to perform advertising services, some of these companies are members of the Network Advertising Initiative ("NAI") or the Digital Advertising Alliance ("DAA") Self-Regulatory Program for Online Behavioral Advertising. You may want to visit http://www.networkadvertising.org/managing/opt_out.asp, which provides information regarding targeted advertising and the "opt-out" procedures of NAI members. You may also want to visit <http://www.aboutads.info/choices/>, which provides information regarding targeted advertising and offers an "opt-out" by participating companies in the DAA Self-Regulatory Program.

6. YOUR CHOICES AND RIGHTS

You have certain choices regarding how we may communicate with you.

Registered NurseContact Users may update their choices regarding the types of communications you receive from us through your online account. You also may opt-out of receiving marketing emails from us by following the opt-out instructions provided in those emails. Please note that we reserve the right to send you certain communications relating to your account or use of the Service (for example, administrative and service announcements) via email and other means and these transactional account messages may be unaffected if you opt-out from receiving marketing communications. You may opt-out of receiving text messages by replying "STOP" to any text message received. Registered NurseContact Users who access the Service by using a NurseContact mobile application may, with permission, receive push notifications. Similarly, registered NurseContact Users who access the Service by using certain

desktop browsers may, with permission, receive push notifications. Notification preferences can be modified in the settings menu for the mobile application or the applicable browser.

All Users may request access to or correction of any Personal Information we have about them or close their account and/or request deletion of all Personal Information we have about them. In certain jurisdictions, Users may have certain rights with regard to their Personal Information. We will honor User requests to the extent we can reasonably do so and as required by law, but some information will remain on the Services, such as information you posted publicly.

Upon request NurseContact will provide you with information about whether we hold any of your personal information. You are responsible for maintaining the accuracy of the information you submit to us, such as your contact information. You may access, correct, or request deletion of your personal information by making updates to that information or by contacting NurseContact through your online account. If you request to access all personal information you've submitted, we will respond to your request to access within 30 days or as otherwise required by law. If your information is deleted, then your account may become deactivated. If your account is deactivated or you ask to close your account, you will no longer be able to use the Service. If you would like to close your account in our system, you can do so through the NurseContact Service (once you have logged in, visit settings / user settings, and then click on the close my account link).

Depending on where you are located, you may have certain rights with regard to your Personal Information (including, in certain cases, under the Privacy Shield, described below). For example, if you are located in the European Economic Area ("EEA"), in addition to the rights described above, you may contact us at the contact information provided below to (1) request a restriction on the processing of your Personal Information, (2) object to the processing of your Personal Information, or (3) exercise other rights with respect to your Personal Information. If you are a California resident, you may have other rights. Please see our Privacy Center for more information or to submit a request to us regarding your Personal Information. NurseContact uses automated means to calculate the Job Success Score of TeleHealth Professionals. If you believe that our services have miscalculated your Job Success Score or you would like to exercise any other rights with regard to your Personal Information, please email us at info@NurseContact.com for assistance. We may be able to assist you by conducting a manual review of your Job Success Score, such as by assessing whether the information you've provided us is accurate. While we strongly encourage you to first raise any questions or concerns about your Personal Information directly with us, you have a right to lodge a complaint with the relevant supervisory authority and to seek judicial remedy.

We will use commercially reasonable efforts to honor your requests for deletion; however, certain information will actively persist on the Service even if you close your account, including information in your Work Diaries and messages you posted to the Service. In addition, the rights described above may be limited, for example, if fulfilling your request would reveal personal information about another person, or if you ask us to delete information we are required by law to keep or have compelling legitimate interests in keeping (such as for fraud prevention purposes). Your Personal Information may remain in our archives and information you update or delete, or information within a closed account, may persist internally for our administrative purposes, to the extent permitted by law. In addition, we typically will not remove information you posted publicly through or on the Service. Bear in mind that

neither you nor NurseContact can delete all copies of information that has been previously shared with others on the Service.

7. SECURITY

We take a number of steps to protect your data, but no security is guaranteed.

NurseContact takes commercially reasonable steps to help protect and secure the information it collects and stores about NurseContact Users. All access to the Site is encrypted using industry-standard transport layer security technology (“TLS”). When you enter sensitive information (such as tax identification number), we encrypt the transmission of that information using secure socket layer technology (“SSL”). We also use HTTP strict transport security to add an additional layer of protection for our NurseContact Users. But remember that no method of transmission over the Internet, or method of electronic storage, is 100% secure. Thus, while we strive to protect your Personal Information, NurseContact cannot ensure and does not warrant the security of any information you transmit to us.

8. INTERNATIONAL TRANSFER OF PERSONAL INFORMATION

Because we are a U.S. company, we process and store your information in the United States and our service providers may process and store it elsewhere.

NurseContact is a U.S. company. If you are located outside the United States and choose to provide information to us, NurseContact transfers Personal Information to the United States for processing, and our service providers may process Personal Information in the United States and elsewhere. These countries may not have the same data protection laws as the country in which you initially provided the information. When we transfer your information to the United States, we will protect it as described in this Privacy Policy.

When we transfer Personal Information from territories in the EEA or with similar laws to our affiliates or service providers in the United States and elsewhere outside the EEA, we rely on approved data transfer mechanisms, including standard contractual clauses approved by the European Commission and the Privacy Shield, as described below. You may request a copy of the standard contractual clauses relevant to your Personal Information, if any, using the contact information below.

9. LINKS TO OTHER SITES

Our Service contains links to other websites. If you choose to click on a third-party link, you will be directed to that third-party’s website. The fact that we link to a website is not an endorsement, authorization or representation of our affiliation with that third-party, nor is it an endorsement of their privacy or information security policies or practices. We do not exercise control over third-party websites. These other websites may place their own cookies or other files on your computer, collect data or solicit Personal Information from you. We encourage you to read the privacy policies or statements of the other websites you visit.

10. PUBLIC PROFILE

The profile you create on our Site will be publicly accessible unless otherwise indicated. You may change the privacy settings of your profile through your account portal.

11. PHISHING

Phishing websites imitate legitimate websites in order to obtain personal or financial information. Identity theft and the practice currently known as “phishing” are of great concern to NurseContact. For more information about phishing, visit the website of the Federal Trade Commission at <http://www.consumer.ftc.gov/articles/0003-phishing>. In addition, if you believe you have received an email or had a similar interaction with a third-party pretending to be NurseContact, please report it to info@nursecontact.com

12. CALIFORNIA AND NEVADA RESIDENTS – YOUR PRIVACY RIGHTS

NOTICE FOR CALIFORNIA RESIDENTS

Please see the Supplemental Notice for California Residents below for additional details on rights available to California residents, and how to exercise such rights.

NOTICE FOR NEVADA RESIDENTS

Under Nevada law, certain Nevada residents may opt out of the sale of “personally identifiable information” for monetary consideration to a person for that person to license or sell such information to additional persons. “Personally identifiable information” includes first and last name, address, email address, phone number, Social Security Number, or an identifier that allows a specific person to be contacted either physically or online.

We do not engage in such activity; however, if you are a Nevada resident who has purchased or leased goods or services from us, you may submit a request to opt out of any potential future sales under Nevada law by emailing info@NurseContact.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.

13. CHANGES TO THIS POLICY

We may change this Privacy Policy. If we make substantial changes, we will provide notice.

NurseContact may update this Privacy Policy at any time and any changes will be effective upon posting. In the event that there are substantial changes to the way we treat your Personal Information, we will display a notice through the Services prior to the change becoming effective. We may also notify you by email, in our discretion. However, we will use your Personal Information in a manner consistent with the Privacy Policy in effect at the time you submitted the information, unless you consent to the new or revised policy.

14. CONTACTING US

If you have any questions about this Privacy Policy, please contact us at info@NurseContact.com, or by mail addressed to 7345 Woodland Dr, Indianapolis, IN 46278.

15. SUPPLEMENTAL PRIVACY NOTICE FOR CALIFORNIA RESIDENTS

This Supplemental Privacy Notice for California Residents supplements the information in our Privacy Policy above, and except as provided herein, applies solely to California residents. It applies to personal

information we collect on or through the Service and through other means (such as information collected offline, in person, and over the telephone). It does not apply to personal information we collect from our employees or job applicants in their capacity as employees and job applicants. It also does not apply to information we collect about businesses that use our Service -- including any employees, owners, directors, officers, or contractors of those businesses -- in the course of our provision or receipt of business-related services.

Summary of Information We Collect

California law requires us to disclose information regarding the categories of personal information that we have collected about California consumers (as that term is defined in the California Consumer Privacy Act ("CCPA")), the categories of sources from which the information was collected, the business or commercial purposes (as those terms are defined by applicable law) for which the information was collected, and the categories of parties with whom we share personal information.

We or our service providers may collect the below categories of information for the following business or commercial purposes (as those terms are defined in applicable law):

- Providing the Service (e.g., account servicing and maintenance, matching Qualified Health Professional talent with client needs, customer service, advertising and marketing, analytics, and communication about the Service);
- Our or our service providers' operational purposes;
- Auditing consumer interactions on our site (e.g., measuring ad impressions);
- Detecting, protecting against, and prosecuting privacy and security incidents and fraudulent or illegal activity;
- Bug detection, error reporting, and activities to maintain the quality or safety of our Service;
- Investigating compliance with, enforcing, and/or complying with the law;
- Short-term, transient use, such as customizing content that we or our service providers display on the Service;
- Improving our existing Service and developing new services (e.g., by conducting research to develop new products or features);
- Other uses that advance our commercial or economic interests, such as third-party advertising and communicating with you about relevant offers from us or third-party partners;
- Other uses about which we notify you.

Examples of these types of uses are identified below. We may also use the below categories of personal information for compliance with applicable laws and regulations, and we may combine the information we collect ("aggregate") or remove pieces of information ("de-identify") to limit or prevent identification of any particular user or device.

Categories of Personal Information We Collect	Categories of Sources	Examples of Uses	Categories of Third Parties With Which We May Share That Information
Identifiers (such as account information, name, email address, address, phone number, or social network account and profile data)	<p>You</p> <p>Your use of the Service/automatically collected from you</p> <p>Affiliates</p> <p>Third Parties (such as agents/service providers and other users)</p>	<p>Providing the Service, including to process your transactions, address your inquiries, provide assistance to you in using the Service, and in connection with Upwork’s Enterprise Compliance and other premium offerings</p> <p>Fixing and improving the Service</p> <p>Personalizing content</p> <p>Marketing and advertising</p> <p>Administering promotional activities</p> <p>Communicating with you</p> <p>Preventing, detecting, investigating, and responding to possible fraud, unauthorized access/use of the Service, breaches of terms and policies</p> <p>Legal and investigative purposes, such as responding to lawful subpoenas or other requests for information, in order to investigate compliance with, enforce and/or comply with the law</p>	<p>Third parties, such as service providers, Clients (e.g. where a Freelancer makes his/her information available to a Client), Agencies, Upwork Payroll vendors, and government agencies</p> <p>Affiliates</p>
Commercial information (such as transaction data)	<p>You</p> <p>Your use of the Service/automatically collected from you</p> <p>Affiliates</p>	<p>Providing the Service, including to process your transactions, address your inquiries, provide assistance to you in using the Service, and in connection with Upwork’s</p>	<p>Third parties, such as service providers, Clients (e.g. where a Freelancer makes his/her information available to a Client), Agencies, Upwork</p>

	<p>Third Parties (such as agents/service providers and other users)</p>	<p>Enterprise Compliance and other premium offerings</p> <p>Fixing and improving the Service</p> <p>Personalizing content</p> <p>Marketing and advertising</p> <p>Communicating with you</p> <p>Preventing, detecting, investigating, and responding to possible fraud, unauthorized access/use of the Service, breaches of terms and policies</p> <p>Legal and investigative purposes, such as responding to lawful subpoenas or other requests for information, in order to investigate compliance with, enforce and/or comply with the law</p>	<p>Payroll vendors, and government agencies</p> <p>Affiliates</p>
<p>Financial data (such as payment information)</p>	<p>You</p> <p>Your use of the Service/automatically collected from you</p> <p>Affiliates</p> <p>Third Parties (such as agents/service providers)</p>	<p>Providing the Service, including to process your transactions, address your inquiries, provide assistance to you in using the Service, and in connection with Upwork’s Enterprise Compliance and other premium offerings</p> <p>Fixing and improving the Service</p> <p>Communicating with you</p> <p>Preventing, detecting, investigating, and responding to possible fraud, unauthorized access/use of the Service, breaches of terms and policies</p> <p>Legal and investigative purposes, such as responding to lawful</p>	<p>Third parties, such as service providers, Clients (e.g. where a Freelancer makes his/her information available to a Client), Agencies, Upwork Payroll vendors, and government agencies</p> <p>Affiliates</p>

		subpoenas or other requests for information, in order to investigate compliance with, enforce and/or comply with the law	
Internet or other network or device activity (such as IP address, unique device and app identifiers, browsing history or other usage data)	<p>You</p> <p>Your use of the Service/automatically collected from you</p> <p>Affiliates</p> <p>Third Parties (such as agents/service providers)</p>	<p>Providing the Service, including to process your transactions, address your inquiries, provide assistance to you in using the Service, and in connection with Upwork’s Enterprise Compliance and other premium offerings</p> <p>Fixing and improving the Service</p> <p>Personalizing content</p> <p>Marketing and advertising</p> <p>Preventing, detecting, investigating, and responding to possible fraud, unauthorized access/use of the Service, breaches of terms and policies</p> <p>Legal and investigative purposes, such as responding to lawful subpoenas or other requests for information, in order to investigate compliance with, enforce and/or comply with the law</p>	<p>Third parties, such as service providers, Clients (e.g. where a Freelancer makes his/her information available to a Client), Agencies, Upwork Payroll vendors, and government agencies</p> <p>Affiliates</p>
General Location information	<p>You</p> <p>Your use of the Service/automatically collected from you</p> <p>Affiliates</p> <p>Third Parties (such as agents/service providers)</p>	<p>Providing the Service, including to process your transactions, address your inquiries, provide assistance to you in using the Service, and in connection with Upwork’s Enterprise Compliance and other premium offerings</p> <p>Fixing and improving the Service</p>	<p>Third parties, such as service providers, Clients (e.g. where a Freelancer makes his/her information available to a Client), Agencies, Upwork Payroll vendors, and government agencies</p> <p>Affiliates</p>

		<p>Personalizing content</p> <p>Marketing and advertising</p> <p>Preventing, detecting, investigating, and responding to possible fraud, unauthorized access/use of the Service, breaches of terms and policies</p> <p>Legal and investigative purposes, such as responding to lawful subpoenas or other requests for information, in order to investigate compliance with, enforce and/or comply with the law</p>	
<p>Sensory information (such as audio recordings if you call our customer service, video recording (if you provide permission), or screenshots from Work Diaries)</p>	<p>You</p> <p>Your use of the Service/automatically collected from you</p> <p>Affiliates</p> <p>Third Parties (such as agents/service providers)</p>	<p>Providing the Service, including to process your transactions, address your inquiries, provide assistance to you in using the Service, and in connection with Upwork’s Enterprise Compliance and other premium offerings</p> <p>Fixing and improving the Service</p> <p>Preventing, detecting, investigating, and responding to possible fraud, unauthorized access/use of the Service, breaches of terms and policies</p> <p>Legal and investigative purposes, such as responding to lawful subpoenas or other requests for information, in order to investigate compliance with, enforce and/or comply with the law</p>	<p>Third parties, such as service providers, Clients (e.g. where a Freelancer makes his/her information available to a Client), Agencies, Upwork Payroll vendors, and government agencies</p> <p>Affiliates</p>
<p>Other information that identifies or can be</p>	<p>You</p>	<p>Providing the Service, including to process your transactions, address</p>	<p>Third parties, such as service providers, Clients (e.g. where a</p>

<p>reasonably associated with you (such as user generated content, e.g. community posts, feedback and job postings, in each case, when the content can be used to identify you)</p>	<p>Your use of the Service/automatically collected from you</p> <p>Affiliates</p> <p>Third Parties (such as agents/service providers)</p>	<p>your inquiries, provide assistance to you in using the Service, and in connection with Upwork’s Enterprise Compliance and other premium offerings</p> <p>Fixing and improving the Service</p> <p>Personalizing content</p> <p>Marketing and advertising</p> <p>Administer promotional activities</p> <p>Communicating with you</p> <p>Preventing, detecting, investigating, and responding to possible fraud, unauthorized access/use of the Service, breaches of terms and policies</p> <p>Legal and investigative purposes, such as responding to lawful subpoenas or other requests for information, in order to investigate compliance with, enforce and/or comply with the law</p>	<p>Freelancer makes his/her information available to a Client), Agencies, Upwork Payroll vendors, and government agencies</p> <p>Affiliates</p> <p>The public if you or other users post content publicly</p>
---	---	--	---

Rights

If you are a California resident, you may have certain rights. California law may permit you to request that we:

- Provide you the categories of personal information we have collected or disclosed about you in the last twelve months; the categories of sources of such information; the business or commercial purpose for collecting or selling your personal information; and the categories of third parties with whom we shared personal information.
- Provide access to and/or a copy of certain information we hold about you.
- Delete certain information we have about you.

You may have the right to receive information about the financial incentives that we offer to you, if any. You also have the right to not be discriminated against (as provided for in applicable law) for exercising certain of your rights.

If you would like to exercise any of these rights, please submit a request through the Data Request Form available in our Privacy Center or email us at info@NurseContact.com. You will be required to verify your identity before we fulfill your request. You can also designate an authorized agent to make a request on your behalf. To do so, you must provide us with written authorization or a power of attorney, signed by you, for the agent to act on your behalf. You will still need to verify your identity directly with us.

Certain information may be exempt from such requests under applicable law. For example, we need certain types of information so that we can provide the Service to you. If you ask us to delete it, you may no longer be able to access or use the Service.

The CCPA sets forth certain obligations for businesses that “sell” personal information. Based on the definition of “sell” under the CCPA and under current regulatory guidance, we do not believe we engage in such activity and have not engaged in such activity in the past twelve months.