

PRIVACY AND DATA SECURITY STATEMENT

WE RESPECT YOUR PRIVACY AND WILL NOT COLLECT, SELL OR SHARE YOUR INFORMATION EXCEPT AS AUTHORIZED BY YOU AND ALLOWED OR REQUIRED BY LAW.

Trauma Reprocessing.com is a website for licensed Clinical Therapy Providers (e.g., licensed psychologists, psychiatrists, social workers, & counselors, or those in supervision working under a licensed provider). It is not intended for clients.

Disabled users who need these disclosures presented in an alternate medium, may contact us at the email address or telephone number listed further below.

Contacting Our Privacy Office

If you have any questions about our privacy and data security policies, procedures and practices, including anything we say in this privacy statement, we encourage you to contact our Privacy Office.

Trauma Reprocessing Institute, LLC
5441 S. Macadam Ave. Suite N
Portland, OR 97239

Email: warriorrenew@yahoo.com

SOME IMPORTANT VOCABULARY

Although not itself a contract, this privacy statement is an important document that explains how we address some of our legal obligations, and your related legal rights, involving personal information. Clarity is, therefore, important. We'll use this section to let you know about some words that have special meanings whenever you see them in this statement.

Let's start with the word "**statement**" itself: when we reference "**this statement**", "**this privacy statement**" and "**our statement**", we mean the Privacy and Data Security Statement you are reading now. Wherever we say "**Company**", "**we**", "**us**", or "**our**", we mean Trauma Reprocessing Institute, LLC. We use the words "**you**" and "**your**" to mean you, the reader, and other visitors to our online and mobile resources who are, in all cases, over the age of 18. This age requirement is discussed in more detail later in the section titled "Children's Privacy" below. When we talk about our "**online and mobile resources**", we mean all websites, portals or other features we operate to allow you to interact with us and our systems, as well as the mobile apps we've created and distributed to let you interact with the content we provide. An "**affinity action**" is when you "follow" us, "like" us or take a similar or analogous action on our external social media presence. Finally, and perhaps most importantly, when we refer to "**personal**

information", we mean any data or data element, whether in electronic or other form, that, alone or in combination with other elements, can be used to distinguish, trace, or discover your identity. Certain data privacy laws include specific elements or defined terms for what they consider to be the personal information (or personal data) they govern. Where such data privacy laws apply, then the term "personal information" includes the specific elements and defined terms required by such laws.

Your Rights as a Consumer

Depending upon where you live and as more fully explained below, you may have significant rights related to the privacy of your personal information, including:

- Right to access your data.
- Right to correct your data.
- Right to have your data deleted.
- Right to opt-out of certain forms of processing of your data.
- Right to portability of your data.
- Right to opt-out from the sale of your data.
- Right to opt-in for certain sensitive data processing.
- Right against certain forms of automated decision-making about your data.

And, in California, the right to bring a private action to protect your data.

WHO DO WE COLLECT PERSONAL INFORMATION FROM?

We collect personal information from four groups of data subjects:

- visitors to, and users of, our online and mobile resources
- our customers
- members of our workforce and those who apply for posted jobs
- our third-party vendors and business partners

The categories of information we collect from each of these groups, and the ways in which we use it, differs.

It is important to note, however, that **this privacy statement applies only to visitors and users of our online and mobile resources.** Thus, the words "you" and "your" throughout this privacy statement mean only that category of data subject. As you may have noticed, it's possible that the same person could fall into more than one group. For instance, someone who works for us might, on their day off, visit one of our general websites.

PRIVACY LAWS VARY FROM PLACE TO PLACE

Privacy and data protection laws vary around the world and among the individual United States. Our obligations arising under the majority of the world's privacy laws, including U.S. federal and most state laws, are satisfied by individual risk assessments conducted by us to ensure we act

reasonably and responsibly when processing your personal information. We refer to these as, “**General Privacy Laws**”. In some jurisdictions, however, privacy laws grant you, the data subject, certain specific rights regarding your personal information. We refer to these types of privacy laws as data subject rights-based laws or “**DSR Privacy Laws**.” Examples of DSR Privacy Laws include the U.S. State of California’s Consumer Privacy Protection Act or “**CCPA**”, and the European Union’s General Data Protection Regulation or “**GDPR**”.

WHAT PERSONAL INFORMATION DO WE COLLECT?

Generally, we collect personal information in two ways: that which you voluntarily provide to us, and that which we collect through automated/technical means. We describe that type of voluntary submission immediately below and we describe our automatic collection in the section titled “Automatically Collected Information” below. ***By using our online and mobile resources, you are signifying to us that you agree with this section of our privacy statement and that we may use and disclose your information as described.***

When you type your name and email into our website and submit the same to us, you agree that this shall act as your electronic signature and express written consent that we, along with its agents, assigns and listed partners, may send you email with marketing offers and other information. Consent is not a condition of purchase and you may opt-out later. By consenting, you are specifically requesting that we share your information in this manner and for these purposes. You agree to do business with us electronically and to receive copies of these terms electronically. You may withdraw your electronic signature or request a paper copy by emailing us at warrriorrenew@yahoo.com

Voluntarily Submitted Information

If you choose to participate in, or make use of certain activities and features available via our website, you will need to provide us with information about yourself. The types of personal information you will be submitting to us in those situations is almost always limited to basic **identifiers** such as your name, email address, mailing address and phone number. Here are some of the ways you voluntarily give us your personal information:

- **Emails and Texts** – If you choose to send us an email from our “contact us” link or a similar link, you will be giving us your email address and any other personal information that may be in your message or attached to it. The same is true if you send us a text message.
- **Creating accounts as a subscriber** – If we make an account creation feature available to the general public (that is, to visitors/users who are not our customers or workforce members) you will be giving us at least your email address and potentially other identifiers. The same is true if you sign up to receive a newsletter or other informational or marketing material we publish.

- **Registering for Events** – When you register for events, conferences or programs we ourselves may host (rather than outsource to a third-party event manager with its own privacy policies), you will be submitting the types of identifiers described above. If the event requires a fee, we may also ask you to submit **credit card or other financial information**.
- **Social Media and Community Features** – Some of our online and mobile resources may offer social media-like community features letting users post messages and comments, and/or upload image or other files and materials. If you choose to make use of these features, the information you post, including your screen name and any other personal information, will be in the public domain and **not covered/protected by this statement**.
- **Customer Portals and Job Applicants** – Some of our online and mobile resources are used to help us serve our customers and allow candidates to apply for available jobs.

Personally Identifiable Information (PII) - name, postal address, phone and credit card information – provided by you when purchasing our products.

Demographic Information – used to improve our marketing, products and services.

All such information is strictly protected and used only for delivering the content and products the user has signed up for or purchased, or for finding other individuals who may find our information valuable.

A note about demographic information: We contract with information providers that help us better understand people visiting our sites and advertise to those who find our content relevant. We may share PII with such companies provided that they have explicit policies to not share our data with any other parties and solely for the purpose of helping us understand our customers better. This technique is also called “database marketing.” It is practiced by virtually every US corporation. Every US consumer can assume that there is a fair amount of available data about them, including personal data such as buying preferences and education level. There is no central “opt out” place that we are aware of. There are efforts underway to reach a standard that would apply automatically based on browser settings. Regardless of the state of privacy as a whole, you can avoid us finding out extra demographic information about you by doing the following:

1. Email us using our contact page
2. In the subject line write: “Privacy – opt out of demographic information”
3. Make sure you enter the same email that you provided as customer or subscriber

If you prefer, we not receive the above-described personal information, please don’t submit it. This means you shouldn’t participate in the applicable activities on, or use the applicable features available from our online and mobile resources. Such participation and use is strictly your choice. By not participating, you may limit your ability to take full advantage of the online and

mobile resources, but most of the content in our online and mobile resources will still be available to you.

Automatically Collected Information

When you visit or use our online and mobile resources, **basic information about your internet/electronic activity** is automatically collected through your browser via tracking technologies, such as “cookies.” As just about everyone knows by now, cookies are small text files downloaded onto your computer or mobile device. Cookies allow us to collect your **IP address** and recognize your computer or mobile device and store some information about your preferences for using our online and mobile resources or past actions, such as:

- the type of browser and operating system you use
- the date and time and length of your visit
- the pages visited, graphics viewed and any documents downloaded
- links to other sites you accessed from our online and mobile resources or used to navigate to our online and mobile resources

Our websites do not currently have the capability to opt you out from the use of cookies – we do currently recognize any do-not-track browser signaling.

We may at times engage in web session and web chat recording.

If you access our online and mobile resources from a phone or other mobile device, the mobile services provider may transmit to us certain information such as uniquely identifiable mobile device information. That, in turn, allows us to collect **mobile phone numbers and associate them with the mobile device identification information**. Some mobile phone service providers also operate systems that pinpoint the physical location of devices and we may receive this **geolocation data** as well.

Clear GIFs: At times, we work with third-party service partners that employ clear GIFs (also known as pixel tags, single pixel GIFs, web beacons or action tags) for our benefit to help us measure advertising effectiveness. Clear GIFs are tiny graphics with a unique identifier, similar in function to cookies, and are used to track the online movements of our users. The main difference between the two is that clear GIFs are invisible on the page and are much smaller, about the size of the period at the end of this sentence. Clear GIFs are not tied to your Personally Identifiable Information and only track the visitor traffic and behavior to and on our Site. Clear GIFs can “work with” existing cookies on a computer if they are both from the same website or advertising company. That means, for example, that if a person visited “www.companyX.com”, which uses an advertising company’s clear GIF, the website would match the clear GIFs identifier and the advertising company’s cookie ID number, to show the past online behavior for that computer. This collected information can be shared with the advertising company. We do, at times, provide such information to our third-party advertising service partners, but that information never includes personally identifiable information.

When you use our online and mobile resources, we may allow third party service providers to place their own cookies or similar technologies in order to engage in the same types of collection we describe above. For example, we use third party “web analytics” services such as those offered by Google Analytics. For more information on how Google specifically uses this data, go to www.google.com/policies/privacy/partners/. You can learn more about how to opt out of Google Analytics by going to <https://tools.google.com/dlpage/gaoptout>.

Finally, there’s a category of personal information we may collect that does not fit neatly into the “voluntarily submitted” or “automatically collected” categories. If you use both our app and a third party mail service (such as Google’s Gmail, Yahoo! Mail and the like) on your mobile device, you may have activated a setting that allows us to use certain technologies such as application programming interfaces, to automatically access (sometimes referred to as “parse”) your mail **as it relates to your use of our app**. If you did activate the setting allowing us to do so, our use of any information we receive from those technologies will adhere to their requirements of the publisher of the applicable technology. This includes, if we use Google APIs, adhering to the [Google API Services User Data Policy](#) and its Limited Use requirements.

User Beware: External Sites, Apps, Links and Social Media

We maintain a presence on one or more external social media platforms such as Twitter, Facebook, YouTube and LinkedIn. We may further allow the community features of our online and mobile resources to connect with, or be viewable from, that external social media presence. Similarly, our online and mobile resources may contain links to other websites or apps controlled by third parties.

We are not responsible for the content on, or the privacy practices of, social media platforms, or any third party sites or apps to which we link. Those apps, sites and platforms are not controlled by us and therefore have their own privacy policies and terms of use. **To be clear: neither this statement nor the terms of service appearing on or in any of our online and mobile resources apply to our social media presence or any third party sites or apps to which we may link.** That means even if you take an affinity action on our specific social media profile, and identifiers about you are automatically collected and given to us as a result, that collection and transfer is governed by the privacy policies and other terms of the applicable social media platform and are not our responsibility. If you have questions about how those apps, sites and platforms collect and use personal information, you should carefully read their privacy policies and contact them using the information they provide.

HOW DO WE USE THE PERSONAL INFORMATION WE COLLECT?

We use the personal information we collect only in the manner and through the means allowed by applicable law. That means we determine whether we have a lawful basis/legitimate business purpose to use your personal information before doing so. As stated in applicable law, such lawful bases/legitimate business purposes may include receiving express consent, operating our business, performing a contract, and complying with a legal obligation. More specifically, we use the personal information we collect as follows:

We use the automatically collected personal information described in the section titled “Automatically Collected Information” to compile generic reports about popular pages/features of our online and mobile resources, and to see how users are accessing our online and mobile resources and in some cases (such as affinity actions) send materials to you. We use the personal information you voluntarily submitted, as described in the section titled “Voluntarily Submitted Information,” to respond back directly to you and/or send you the information you requested or about which you inquired. We also may use any such personal information you provide to customize our programs and newsletters to make them more relevant to you. **We do not sell or rent personal information automatically collected by, or which you voluntarily provide when using our online and mobile resources.**

We use and retain your personal information in accordance with applicable law and as long as necessary to carry out the purposes described above in accordance with our internal data retention procedures.

We use the information we collect from you while you are using the Site in a variety of ways, including using the information to customize features; advertising that appear on the Site; and, making other offers available to you via email, direct mail or otherwise. We also may provide your information to third parties, such as service providers, contractors and third-party publishers and advertisers for a variety of purposes. Unless you inform us in accordance with the process described below, we reserve the right to use, and to disclose to third parties, all of the information collected from and about you while you are using the Site in any way and for any purpose, such as to enable us or a third party to provide you with information about products and services. If you do not wish your information to be used for these purposes, you must send a letter to the Online Privacy Coordinator whose address is listed at the end of this Privacy Policy requesting to be taken off any lists of information that may be used for these purposes or that may be given or sold to third-parties.

WHEN/WITH WHOM DO WE SHARE PERSONAL INFORMATION?

We may share your personal information as described below. This sharing applies to the personal information of all four groups of data subjects.

Affiliates

We may share personal information with other corporate affiliates who will use such information in the same way as we can under this statement.

Legal Requirements

We may disclose personal information to government authorities, and to other third parties when compelled to do so by such government authorities, or at our discretion or otherwise as required or permitted by law, including responding to court orders and subpoenas.

To Prevent Harm

We also may disclose such information when we have reason to believe that someone is causing injury to or interference with our rights or property, or harming or potentially harming other persons or property.

Business Sale/Purchase

If we, or any of our affiliates, sell or transfer all or substantially all of our assets, equity interests or securities, or are acquired by one or more third parties as a result of an acquisition, merger, sale, reorganization, divestiture, consolidation, or liquidation, personal information may be one of the transferred assets.

Vendors and Business Partners

We also share personal information with those of our vendors and business partners who need it to perform under the contracts we have with them. As part of our Data Security Program, we have adopted standards for those vendors and business partners who receive personal information from us. We attempt to bind such vendors and business partners to those standards via written contracts. Such standards include expectations that when we share personal information with our vendors and business partners, they will comply with all applicable privacy and data security laws and regulations and our Security Program, and will contractually require and cause their subcontractors and agents to do the same.

For any personal information our vendors and business partners process or store at their own locations, we further expect them to use technology infrastructure meeting, at least at the facilities level, minimum recognized standards for security controls. Such recognized standards include those published by the International Standards Organization, the National Institute of Standards and Technology or any reasonably equivalent standards.

Please note, however, that we cannot guarantee that all of our vendors and business partners will agree to the above-described contractual requirements; nor can we ensure that, even when they do agree, they will always fully comply.

Facebook

We may opt to advertise on Facebook and through a Facebook page, we, (not Facebook) may collect content or information from a Facebook user and such information may be used in the same manner specified in this Privacy Policy. You consent to our collection of such information.

We abide by Facebook's Data Use Restrictions.

Any ad data collected, received or derived from our Facebook ad ("Facebook advertising data") is only shared with someone acting on our behalf, such as our service provider. We are responsible for ensuring that our service providers protect any Facebook advertising data or any other information obtained from us, limit our use of all of that information, and keep it confidential and secure.

We do not use Facebook advertising data for any purpose (including retargeting, commingling data across multiple advertisers' campaigns, or allowing piggybacking or redirecting with tags), except on an aggregate and anonymous basis (unless authorized by Facebook) and only to assess the performance and effectiveness of our Facebook advertising campaigns.

We do not use Facebook advertising data, including the targeting criteria for a Facebook ad, to build, append to, edit, influence, or augment user profiles, including profiles associated with any mobile device identifier or other unique identifier that identifies any particular user, browser, computer or device.

We do not transfer any Facebook advertising data (including anonymous, aggregate, or derived data) to any ad network, ad exchange, data broker or other advertising or monetization related service.

HOW DO WE PROTECT COLLECTED PERSONAL INFORMATION?

Our Data Security Program

We have adopted, implemented and maintain an enterprise-wide corporate information security and privacy program that includes technical, organizational, administrative, and other security measures designed to protect, as required by applicable law, against reasonably anticipated or actual threats to the security of your personal information (the “**Security Program**”). Our Security Program was created with reference to widely recognized industry standards such as those published by the International Standards Organization and the National Institute of Standards and Technology. It includes, among many other things, procedures for assessing the need for and employing encryption and multi-factor authentication as appropriate, or using equivalent compensating controls. We therefore have every reason to believe our Security Program is reasonable and appropriate for our business and the nature of foreseeable risks to the personal information we collect. We further periodically review and update our Security Program, including as required by applicable law.

Our Incident Response and Management Plan

Despite the significant investment we've made in, and our commitment to, the Security Program including enforcement of our third party oversight procedures, described above, we cannot guarantee that your personal information, whether during transmission or while stored on our systems, otherwise in our care, or the care of our vendors and business partners, will be free from either failed or successful attempts at unauthorized access or that loss or accidental destruction will never occur. Except for our duty under applicable law to maintain the Security Program, we necessarily disclaim, to the maximum extent the law allows, any other liability for any such theft or loss of, unauthorized access or damage to, or interception of any data or communications including personal information.

All that said, as part of our Security Program, we have specific incident response and management procedures that are activated whenever we become aware that your personal

information was likely to have been compromised. Those procedures include mechanisms to provide, when circumstances and/or our legal obligations warrant, notice to all affected data subjects within the timeframes required by law, as well as to give them such other mitigation and protection services (such as the credit monitoring and identity theft insurance) as may be required by applicable law. We further require, as part of our vendor and business partner oversight procedures, that such parties notify us within the timeframes required by law if they have any reason to believe that an incident adversely affecting personal information, we provided to them has occurred.

YOUR RIGHTS AND OPTIONS

If we are using your personal information to send you marketing materials, such as newsletters or product alerts via text or email, you may opt out by following the opt-out instructions in the email or other communication (e.g., by responding to the text with “STOP”). In addition, certain of our online and mobile resources will provide a centralized opt-out link allowing you to opt out of any programs in which you may have enrolled using that particular online and mobile resource. When we receive your request, we will take reasonable steps to remove your name from our distribution lists, but it may take time to do so. You may still receive materials for a period of time after you opt out. In addition to opting out, you have the ability to access, amend and delete your personal information by contacting us using the contact information below. Opting out of or changing affinity actions or other submissions or requests made on our external social media presence, will likely require that you do so directly on that applicable platform as we do not control their procedures.

Your email information (email address, first name) is stored at the list server. Your information can only be accessed by those who help manage those lists in order to deliver e-mail to those who would like to receive Trauma Reprocessing Institute information. You can remove yourself at any time from our emails by unsubscribing via a message on our Contact page at traumareprocessing.com. If you have purchased any of my programs, you will continue to receive mailings related to your purchase. If you are an affiliate partner, then you will continue to receive mailings related to our affiliate program. If you would like to be removed from any of these mailings, please contact us at [Trauma Reprocessing.com](http://TraumaReprocessing.com).

Some browsers have a “do not track” feature that lets you tell websites that you do not want to have your online activities tracked. At this time, we do not specifically respond to browser “do not track” signals.

CHILDREN’S PRIVACY

You may not make any use of our websites or services if you are a minor or are not authorized to make binding legal decisions for yourself. Federal law imposes special restrictions and obligations on commercial website operators who direct their operations toward, and collect and use information from children under the age of 13. We take those age-related requirements very seriously, and, consistent with them, do not intend for our online and mobile resources to be used

by children under the age of 18, and certainly not by those under the age of 13. Moreover, we do not knowingly collect personal information from minors under the age of 18. If we become aware that anyone under the age of 18 has submitted personal information to us via our online and mobile resources, we will delete that information and not use it for any purpose whatsoever. Because we do not collect any personally identifiable information from children under the age of thirteen as part of the Site, we also do NOT knowingly distribute such information to third parties. We do NOT knowingly allow children under the age of thirteen to publicly post or otherwise distribute personally identifiable contact information through the Site. We encourage parents and legal guardians to talk with their children about the potential risks of providing personal information over the Internet.

THE CALIFORNIA CONSUMER PRIVACY ACT

When we collect personal information from California residents, we become subject to, and those residents have rights under, the California Consumer Privacy Act or “**CCPA**”. This section of our statement is used to allow us to fulfill our CCPA obligations and explain your CCPA rights. For purposes of this section, the words “**you**” and “**your**” mean only such California residents.

What did we collect from California Residents? [GMM to verify categories below]

We collected the following categories of personal information within the last 12 months:

- **identifiers** such as name, address, IP address, and other similar identifiers
- **personal information under the Customer Records provision of the California Civil Code** such as a name, address, telephone number, credit card number
- **commercial information** such as products or services purchased
- **internet/electronic activity** such as browsing history and search history
- **geolocation data** including geographic coordinates/physical location
- **audio, video, electronic** or other similar information
- **inferences drawn from the foregoing** to create a profile about a consumer reflecting the consumer’s preferences, characteristics, psychological traits, predispositions, behavior, attitudes, intelligence abilities and aptitudes.

What Personal Information did we disclose for a business purpose?

We may have disclosed the categories of personal information listed above for one or more business purposes permitted by the CCPA during the last 12 months.

What Personal Information did we sell?

We do not sell, and within the last 12 months have not sold, personal information to third parties.

What sources did we obtain Personal Information from and why did we collect it?

Please re-review the section of this of this privacy statement titled “Who Do We Collect Personal Information From?” to understand the scope of purposes and the sources from which we collect it. Similarly, we urge you to re-read the section of this statement titled “With Whom Do We Share Personal Information?” where we describe the categories of third parties with which we may share your personal information and why.

Rights of California Residents

You have the following rights under the CCPA. It’s important to us that you know that if you exercise these rights, we will not discriminate against you by treating you differently from other California residents who use our sites and mobile resources or purchase our services but did not exercise their rights.

- **Know** – the right to request that we disclose to you, specifically beyond the general statement immediately above, the categories and specific elements of personal information collected including the source of the information, our use of it and, if the information was disclosed or sold to third parties, the categories so disclosed or sold as well as the categories of third party who received or purchased it.
- **Access** – the right to receive a copy of the categories and specific elements of personal information we collected about you in the preceding 12 months.
- **Delete** – the right to request that we delete the personal information we collected about you under certain circumstances.
- **Opt-Out** – the right to direct a business that sells personal information about the consumer to third parties not to sell the consumer’s personal information.

You, or an authorized agent acting on your behalf, can exercise the Right to Know up to two different times every 12 months. To exercise these rights, contact us [Trauma Reprocessing.com](http://TraumaReprocessing.com). We may ask you to fill out a request form. The CCPA only allows us to act on your request if we can verify your identity and/or your agent’s authority to make the request, so you will also need to follow our instructions for identity verification.

If you make a verifiable request per the above, we will confirm our receipt and respond in the time frames prescribed by the CCPA.

New Jersey Public Servicemembers

We value the privacy of public service members and do not publish or otherwise make available the information related to the same to the public. If you are a public servicemember in New Jersey, including for example a current or retired New Jersey judge, prosecutor or police officer, ***do not submit any private, non-public contact information to us***. If you do, you agree that, to the extent your non-public contact information is protected by New Jersey’s “Daniels law,” you will exercise your right to opt-out (a non-disclosure request) only by emailing your request to through the contact page at [Trauma Reprocessing.com](http://TraumaReprocessing.com), and you will allow us a reasonable period

to recognize and honor your request.

CHANGES TO THIS PRIVACY STATEMENT

We reserve the right to change or update this statement from time to time. Please check our online and mobile resources periodically for such changes since all information collected is subject to the statement in place at the time of collection. Typically, we will indicate the effective/amendment date at the beginning of this statement. If we feel it is appropriate, or if the law requires, we'll also provide a summary of changes we've made near the end of the new statement.

This policy may be changed at any time. If we should update this policy, we will post the updates to this page on our Website. This policy was revised January 15, 2026. If you have any questions or concerns regarding our privacy policy please send us your question to Trauma Reprocessin.com.

CONTACTING US

If you have questions about our privacy statement or privacy practices, please contact our Privacy Office:

Trauma Reprocessing Institute, LLC
5441 S. Macadam Ave., Suite N
Portland, OR 97239

Email: Warriorrenew@yahoo.com

General Data Privacy Regulation (GDPR): The GDPR takes effect on May 25, 2018, and is intended to protect the data of European Union citizens. As a company that markets its site. Content, products and/or services on line we do not specifically target our marketing to the EU or conduct business in or to the EU in any meaningful way. If the data that you provide to us in the course of your use of our site or services or products is governed by GDPR, we will abide by the relevant portions of the regulation. If you are a resident of the European Economic Area (EEA), or are accessing this site from within the EEA, you may have the right to request: access to, correction of, deletion of; portability of; and restriction or objection to processing, of your personal data, from us. This includes the “right to be forgotten.” To make any of these requests, please contact our GDPR contact at warriorrenew@yahoo.com

You, or an authorized agent acting on your behalf, can exercise the Right to Know up to two different times every 12 months. To exercise these rights, contact us at warriorrenew@yahoo.com. We may ask you to fill out a request form. The CCPA only allows us to act on your request if we can verify your identity and/or your agent's authority to make the request, so you will also need to follow our instructions for identity verification.

If you make a verifiable request per the above, we will confirm our receipt and respond in the time frames prescribed by the CCPA.