Privacy Policy

Last updated: June 04, 2020

This Privacy Policy describes Our policies and procedures on the collection, use and disclosure of Your information when You use the Service and tells You about Your privacy rights and how the law protects You.

We use Your Personal data to provide and improve the Service. By using the Service, You agree to the collection and use of information in accordance with this Privacy Policy.

Interpretation and Definitions

Interpretation

The words of which the initial letter is capitalized have meanings defined under the following conditions. The following definitions shall have the same meaning regardless of whether they appear in singular or in plural.

Definitions

For the purposes of this Privacy Policy:

You means the individual accessing or using the Service, or the company, or other legal entity on behalf of which such individual is accessing or using the Service, as applicable.

Under GDPR (General Data Protection Regulation), You can be referred to as the Data Subject or as the User as you are the individual using the Service.

Company (referred to as either "the Company", "We", "Us" or "Our" in this Agreement) refers to Train Centric LLC, 3150 139th AVE SE #4 Bellevue, WA, 98005.

For the purpose of the GDPR, the Company is the Data Controller.

Application means the software program provided by the Company downloaded by You on any electronic device, named Train Centric

Affiliate means an entity that controls, is controlled by or is under common control with a party, where "control" means ownership of 50% or more of the shares, equity interest or other securities entitled to vote for election of directors or other managing authority.

Account means a unique account created for You to access our Service or parts of our Service.

Service refers to the Application.

Country refers to: Washington, United States

Service Provider means any natural or legal person who processes the data on behalf of the Company. It refers to third-party companies or individuals employed by the Company to facilitate the Service, to provide the Service on behalf of the Company, to perform services related to the Service or to assist the Company in analyzing how the Service is used. For the purpose of the GDPR, Service Providers are considered Data Processors.

Third-party Social Media Service refers to any website or any social network website through which a User can log in or create an account to use the Service.

Facebook Fan Page is a public profile named Train Centric specifically created by the Company on the Facebook social network, accessible from https://www.facebook.com/traincentric/

Personal Data is any information that relates to an identified or identifiable individual.

For the purposes for GDPR, Personal Data means any information relating to You such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity.

For the purposes of the CCPA, Personal Data means any information that identifies, relates to, describes or is capable of being associated with, or could reasonably be linked, directly or indirectly, with You.

Device means any device that can access the Service such as a computer, a cellphone or a digital tablet.

Usage Data refers to data collected automatically, either generated by the use of the Service or from the Service infrastructure itself (for example, the duration of a page visit).

Data Controller, for the purposes of the GDPR (General Data Protection Regulation), refers to the Company as the legal person which alone or jointly with others determines the purposes and means of the processing of Personal Data.

Do Not Track (DNT) is a concept that has been promoted by US regulatory authorities, in particular the U.S. Federal Trade Commission (FTC), for the Internet industry to develop and implement a mechanism for allowing internet users to control the tracking of their online activities across websites.

Business, for the purpose of the CCPA (California Consumer Privacy Act), refers to the Company as the legal entity that collects Consumers' personal information and determines the purposes and means of the processing of Consumers' personal information, or on behalf of which such information is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information, that does business in the State of California.

Consumer, for the purpose of the CCPA (California Consumer Privacy Act), means a natural person who is a California resident. A resident, as defined in the law, includes (1) every individual who is in the USA for other than a temporary or transitory purpose, and (2) every individual who is domiciled in the USA who is outside the USA for a temporary or transitory purpose.

Sale, for the purpose of the CCPA (California Consumer Privacy Act), means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a Consumer's Personal information to another business or a third party for monetary or other valuable consideration.

Collecting and Using Your Personal Data

Types of Data Collected

Personal Data

While using Our Service, We may ask You to provide Us with certain personally identifiable information that can be used to contact or identify You. Personally identifiable information may include, but is not limited to:

Email address

First name and last name

Phone number

Address, State, Province, ZIP/Postal code, City

Usage Data

Usage Data

Usage Data is collected automatically when using the Service.

Usage Data may include information such as Your Device's Internet Protocol address (e.g. IP address), browser type, browser version, the pages of our Service that You visit, the time and date of Your visit, the time spent on those pages, unique device identifiers and other diagnostic data.

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

We may also collect information that Your browser sends whenever You visit our Service or when You access the Service by or through a mobile device.

Information from Third-Party Social Media Services

The Company allows You to create an account and log in to use the Service through the following Third-party Social Media Services:

- Google
- Facebook
- Twitter

If You decide to register through or otherwise grant us access to a Third-Party Social Media Service, We may collect Personal data that is already associated with Your Third-Party Social Media Service's account, such as Your name, Your email address, Your activities or Your contact list associated with that account.

You may also have the option of sharing additional information with the Company through Your Third-Party Social Media Service's account. If You choose to provide such information and Personal Data, during registration or otherwise, You are giving the Company permission to use, share, and store it in a manner consistent with this Privacy Policy.

Information Collected while Using the Application

While using Our Application, in order to provide features of Our Application, We may collect, with your prior permission:

- Information regarding your location
- Information from your Device's phone book (contacts list)
- Pictures and other information from your Device's camera and photo library

We use this information to provide features of Our Service, to improve and customize Our Service. The information may be uploaded to the Company's servers and/or a Service Provider's server or it be simply stored on Your device.

You can enable or disable access to this information at any time, through Your Device settings.

Use of Your Personal Data

The Company may use Personal Data for the following purposes:

- **To provide and maintain our Service**, including to monitor the usage of our Service.
- **To manage Your Account:** to manage Your registration as a user of the Service. The Personal Data You provide can give You access to different functionalities of the Service that are available to You as a registered user.
- **For the performance of a contract:** the development, compliance and undertaking of the purchase contract for the products, items or services You have purchased or of any other contract with Us through the Service.

- **To contact You:** To contact You by email, telephone calls, SMS, or other equivalent forms of electronic communication, such as a mobile application's push notifications regarding updates or informative communications related to the functionalities, products or contracted services, including the security updates, when necessary or reasonable for their implementation.
- **To provide You** with news, special offers and general information about other goods, services and events which we offer that are similar to those that you have already purchased or enquired about unless You have opted not to receive such information.
- **To manage Your requests:** To attend and manage Your requests to Us.

We may share your personal information in the following situations:

- **With Service Providers:** We may share Your personal information with Service Providers to monitor and analyze the use of our Service, to advertise on third party websites to You after You visited our Service, to contact You.
- **For Business transfers:** We may share or transfer Your personal information in connection with, or during negotiations of, any merger, sale of Company assets, financing, or acquisition of all or a portion of our business to another company.
- **With Affiliates:** We may share Your information with Our affiliates, in which case we will require those affiliates to honor this Privacy Policy. Affiliates include Our parent company and any other subsidiaries, joint venture partners or other companies that We control or that are under common control with Us.
- **With Business partners:** We may share Your information with Our business partners to offer You certain products, services or promotions.
- **With other users:** when You share personal information or otherwise interact in the public areas with other users, such information may be viewed by all users and may be publicly distributed outside. If You interact with other users or register through a Third-Party Social Media Service, Your contacts on the Third-Party Social Media Service may see Your name, profile, pictures and description of Your activity. Similarly, other users will be able to view descriptions of Your activity, communicate with You and view Your profile.

Retention of Your Personal Data

The Company will retain Your Personal Data only for as long as is necessary for the purposes set out in this Privacy Policy. We will retain and use Your Personal Data to the extent necessary to comply with our legal obligations (for example, if we are required to retain your data to comply with applicable laws), resolve disputes, and enforce our legal agreements and policies.

The Company will also retain Usage Data for internal analysis purposes. Usage Data is generally retained for a shorter period of time, except when this data is used to strengthen the security or to improve the functionality of Our Service, or We are legally obligated to retain this data for longer time periods.

Transfer of Your Personal Data

Your information, including Personal Data, is processed at the Company's operating offices and in any other places where the parties involved in the processing are located. It means that this information may be transferred to — and maintained on — computers located outside of Your state, province, country or other governmental jurisdiction where the data protection laws may differ than those from Your jurisdiction.

Your consent to this Privacy Policy followed by Your submission of such information represents Your agreement to that transfer.

The Company will take all steps reasonably necessary to ensure that Your data is treated securely and in accordance with this Privacy Policy and no transfer of Your Personal Data will take place to an organization or a country unless there are adequate controls in place including the security of Your data and other personal information.

Disclosure of Your Personal Data

Business Transactions

If the Company is involved in a merger, acquisition or asset sale, Your Personal Data may be transferred. We will provide notice before Your Personal Data is transferred and becomes subject to a different Privacy Policy.

Law enforcement

Under certain circumstances, the Company may be required to disclose Your Personal Data if required to do so by law or in response to valid requests by public authorities (e.g. a court or a government agency).

Other legal requirements

The Company may disclose Your Personal Data in the good faith belief that such action is necessary to:

- Comply with a legal obligation
- Protect and defend the rights or property of the Company
- Prevent or investigate possible wrongdoing in connection with the Service
- Protect the personal safety of Users of the Service or the public
- Protect against legal liability

Security of Your Personal Data

The security of Your Personal Data is important to Us, but remember that no method of transmission over the Internet, or method of electronic storage is 100% secure. While We strive to use commercially acceptable means to protect Your Personal Data, We cannot guarantee its absolute security.

Detailed Information on the Processing of Your Personal Data

Service Providers have access to Your Personal Data only to perform their tasks on Our behalf and are obligated not to disclose or use it for any other purpose.

Analytics

We may use third-party Service providers to monitor and analyze the use of our Service.

Google Analytics

Google Analytics is a web analytics service offered by Google that tracks and reports website traffic. Google uses the data collected to track and monitor the use of our Service. This data is shared with other Google services. Google may use the collected data to contextualise and personalise the ads of its own advertising network.

You may opt-out of certain Google Analytics features through your mobile device settings, such as your device advertising settings or by following the instructions provided by Google in their Privacy Policy: https://policies.google.com/privacy

For more information on the privacy practices of Google, please visit the Google Privacy & Terms web page: https://policies.google.com/privacy

Firebase

Firebase is an analytics service provided by Google Inc.

You may opt-out of certain Firebase features through your mobile device settings, such as your device advertising settings or by following the instructions provided by Google in their Privacy Policy: https://policies.google.com/privacy

We also encourage you to review the Google's policy for safeguarding your data: https://support.google.com/analytics/answer/6004245

For more information on what type of information Firebase collects, please visit the Google Privacy & Terms web page: https://policies.google.com/privacy

Matomo

Matomo is a web analytics service. You can visit their Privacy Policy page here: https://matomo.org/privacy-policy

Clicky

Clicky is a web analytics service. Read the Privacy Policy for Clicky here: https://clicky.com/terms

Statcounter

Statcounter is a web traffic analysis tool. You can read the Privacy Policy for Statcounter here: https://statcounter.com/about/legal/

Flurry Analytics

Flurry Analytics service is provided by Yahoo! Inc.

You can opt-out from Flurry Analytics service to prevent Flurry Analytics from using and sharing your information by visiting the Flurry's Opt-out page: https://developer.yahoo.com/flurry/end-user-opt-out/

For more information on the privacy practices and policies of Yahoo!, please visit their Privacy Policy page: https://policies.yahoo.com/xa/en/yahoo/privacy/index.htm

Mixpanel

Mixpanel is provided by Mixpanel Inc.

You can prevent Mixpanel from using your information for analytics purposes by opting-out. To opt-out of Mixpanel service, please visit this page: https://mixpanel.com/optout/

For more information on what type of information Mixpanel collects, please visit the Terms of Use page of Mixpanel: https://mixpanel.com/terms/

Unity Analytics

Unity Analytics is provided by Unity Technologies.

For more information on what type of information Unity Analytics collects, please visit their Privacy Policy page: https://unity3d.com/legal/privacy-policy

Email Marketing

We may use Your Personal Data to contact You with newsletters, marketing or promotional materials and other information that may be of interest to You. You may opt-out of receiving any, or all, of these communications from Us by following the unsubscribe link or instructions provided in any email We send or by contacting Us.

We may use Email Marketing Service Providers to manage and send emails to You.

Mailchimp

Mailchimp is an email marketing sending service provided by The Rocket Science Group LLC.

For more information on the privacy practices of Mailchimp, please visit their Privacy policy: https://mailchimp.com/legal/privacy/

AWeber

AWeber is an email marketing sending service provided by AWeber Communications.

For more information on the privacy practices of AWeber, please visit their Privacy policy: https://www.aweber.com/privacy.htm

GetResponse

GetResponse is an email marketing sending service provided by GetResponse.

For more information on the privacy practices of GetResponse, please visit their Privacy policy: https://www.getresponse.com/legal/privacy.html

Omnisend

Their Privacy Policy can be viewed at https://www.omnisend.com/privacy/

Behavioral Remarketing

The Company uses remarketing services to advertise on third party websites to You after You visited our Service. We and Our third-party vendors use cookies to inform, optimize and serve ads based on Your past visits to our Service.

Google Ads (AdWords)

Google Ads (AdWords) remarketing service is provided by Google Inc.

You can opt-out of Google Analytics for Display Advertising and customise the Google Display Network ads by visiting the Google Ads Settings page: http://www.google.com/settings/ads

Google also recommends installing the Google Analytics Opt-out Browser Add-on - https://tools.google.com/dlpage/gaoptout - for your web browser. Google Analytics Opt-out Browser Add-on provides visitors with the ability to prevent their data from being collected and used by Google Analytics.

For more information on the privacy practices of Google, please visit the Google Privacy & Terms web page: https://policies.google.com/privacy

Bing Ads Remarketing

Bing Ads remarketing service is provided by Microsoft Inc.

You can opt-out of Bing Ads interest-based ads by following their instructions: https://advertise.bingads.microsoft.com/en-us/resources/policies/personalized-ads

You can learn more about the privacy practices and policies of Microsoft by visiting their Privacy Policy page: https://privacy.microsoft.com/en-us/PrivacyStatement

Twitter

Twitter remarketing service is provided by Twitter Inc.

You can opt-out from Twitter's interest-based ads by following their instructions: https://support.twitter.com/articles/20170405

You can learn more about the privacy practices and policies of Twitter by visiting their Privacy Policy page: https://twitter.com/privacy

Facebook

Facebook remarketing service is provided by Facebook Inc.

You can learn more about interest-based advertising from Facebook by visiting this page: https://www.facebook.com/help/164968693837950

To opt-out from Facebook's interest-based ads, follow these instructions from Facebook: https://www.facebook.com/help/568137493302217

Facebook adheres to the Self-Regulatory Principles for Online Behavioural Advertising established by the Digital Advertising Alliance. You can also opt-out from Facebook and other participating companies through the Digital Advertising Alliance in the USA http://www.aboutads.info/choices/, the Digital Advertising Alliance of Canada in Canada http://youradchoices.ca/ or the European Interactive Digital Advertising Alliance in Europe http://www.youronlinechoices.eu/, or opt-out using your mobile device settings.

For more information on the privacy practices of Facebook, please visit Facebook's Data Policy: https://www.facebook.com/privacy/explanation

Pinterest

Pinterest remarketing service is provided by Pinterest Inc.

You can opt-out from Pinterest's interest-based ads by enabling the "Do Not Track" functionality of your web browser or by following Pinterest instructions: http://help.pinterest.com/en/articles/personalization-and-data

You can learn more about the privacy practices and policies of Pinterest by visiting their Privacy Policy page: https://about.pinterest.com/en/privacy-policy

AdRoll

AdRoll remarketing service is provided by Semantic Sugar, Inc.

You can opt-out of AdRoll remarketing by visiting this AdRoll Advertising Preferences web page: http://info.evidon.com/pub_info/573?v=1&nt=1&nw=false

For more information on the privacy practices of AdRoll, please visit the AdRoll Privacy Policy web page: http://www.adroll.com/about/privacy

Perfect Audience

Perfect Audience remarketing service is provided by NowSpots Inc.

You can opt-out of Perfect Audience remarketing by visiting these pages: Platform Opt-out (http://pixel.prfct.co/coo) and Partner Opt-out (http://ib.adnxs.com/optout).

For more information on the privacy practices of Perfect Audience, please visit the Perfect Audience Privacy Policy & Opt-out web page: https://www.perfectaudience.com/privacy/

AppNexus

AppNexus remarketing service is provided by AppNexus Inc.

You can opt-out of AppNexus remarketing by visiting the Privacy & the AppNexus Platform web page: https://www.appnexus.com/platform-privacy-policy

For more information on the privacy practices of AppNexus, please visit the AppNexus Platform Privacy Policy web page: https://www.appnexus.com/platform-privacy-policy

Usage, Performance and Miscellaneous

We may use third-party Service Providers to provide better improvement of our Service.

Invisible reCAPTCHA

We use an invisible captcha service named reCAPTCHA. reCAPTCHA is operated by Google.

The reCAPTCHA service may collect information from You and from Your Device for security purposes.

The information gathered by reCAPTCHA is held in accordance with the Privacy Policy of Google: https://www.google.com/intl/en/policies/privacy/

Mouseflow

Mouseflow is a session replay and heatmap tool that shows how visitors click, move, scroll, browse, and pay attention on websites. The service is operated by ApS.

Mouseflow service may collect information from Your device.

The information gathered by Mouseflow is held in accordance with its Privacy Policy: https://mouseflow.com/privacy/

FreshDesk

FreshDesk is a customer support software. The service is operated by Freshworks, Inc.

FreshDesk service may collect information from Your Device.

The information gathered by FreshDesk is held in accordance with its Privacy Policy: https://www.freshworks.com/privacy/

Google Places

Google Places is a service that returns information about places using HTTP requests. It is operated by Google

Google Places service may collect information from You and from Your Device for security purposes.

The information gathered by Google Places is held in accordance with the Privacy Policy of Google: https://www.google.com/intl/en/policies/privacy/

GDPR Privacy

Legal Basis for Processing Personal Data under GDPR

We may process Personal Data under the following conditions:

- **Consent:** You have given Your consent for processing Personal Data for one or more specific purposes.
- **Performance of a contract:** Provision of Personal Data is necessary for the performance of an agreement with You and/or for any pre-contractual obligations thereof.
- **Legal obligations:** Processing Personal Data is necessary for compliance with a legal obligation to which the Company is subject.
- **Vital interests:** Processing Personal Data is necessary in order to protect Your vital interests or of another natural person.
- **Public interests:** Processing Personal Data is related to a task that is carried out in the public interest or in the exercise of official authority vested in the Company.
- **Legitimate interests:** Processing Personal Data is necessary for the purposes of the legitimate interests pursued by the Company.

In any case, the Company will gladly help to clarify the specific legal basis that applies to the processing, and in particular whether the provision of Personal Data is a statutory or contractual requirement, or a requirement necessary to enter into a contract.

Your Rights under the GDPR

The Company undertakes to respect the confidentiality of Your Personal Data and to guarantee You can exercise Your rights.

You have the right under this Privacy Policy, and by law if You are within the EU, to:

- **Request access to Your Personal Data.** The right to access, update or delete the information We have on You. Whenever made possible, you can access, update or request deletion of Your Personal Data directly within Your account settings section. If you are unable to perform these actions yourself, please contact Us to assist You. This also enables You to receive a copy of the Personal Data We hold about You.
- **Request correction of the Personal Data that We hold about You.** You have the right to to have any incomplete or inaccurate information We hold about You corrected.
- **Object to processing of Your Personal Data.** This right exists where We are relying on a legitimate interest as the legal basis for Our processing and there is something about Your particular situation, which makes You want to object to our processing of Your Personal Data on this ground. You also have the right to object where We are processing Your Personal Data for direct marketing purposes.
- **Request erasure of Your Personal Data.** You have the right to ask Us to delete or remove Personal Data when there is no good reason for Us to continue processing it.
- **Request the transfer of Your Personal Data.** We will provide to You, or to a third-party You have chosen, Your Personal Data in a structured, commonly used, machine-readable format. Please note that this right only applies to automated information which You initially provided consent for Us to use or where We used the information to perform a contract with You.
- **Withdraw Your consent.** You have the right to withdraw Your consent on using your Personal Data. If You withdraw Your consent, We may not be able to provide You with access to certain specific functionalities of the Service.

Exercising of Your GDPR Data Protection Rights

You may exercise Your rights of access, rectification, cancellation and opposition by contacting Us. Please note that we may ask You to verify Your identity before responding to such requests. If You make a request, We will try our best to respond to You as soon as possible.

You have the right to complain to a Data Protection Authority about Our collection and use of Your Personal Data. For more information, if You are in the European Economic Area (EEA), please contact Your local data protection authority in the EEA.

Facebook Fan Page

Data Controller for the Facebook Fan Page

The Company is the Data Controller of Your Personal Data collected while using the Service. As operator of the Facebook Fan Page https://www.facebook.com/traincentric/, the Company and the operator of the social network Facebook are Joint Controllers.

The Company has entered into agreements with Facebook that define the terms for use of the Facebook Fan Page, among other things. These terms are mostly based on the Facebook Terms of Service: https://www.facebook.com/terms.php

Visit the Facebook Privacy Policy https://www.facebook.com/policy.php for more information about how Facebook manages Personal data or contact Facebook online, or by mail: Facebook, Inc. ATTN, Privacy Operations, 1601 Willow Road, Menlo Park, CA 94025, United States.

Facebook Insights

We use the Facebook Insights function in connection with the operation of the Facebook Fan Page and on the basis of the GDPR, in order to obtain anonymized statistical data about Our users.

For this purpose, Facebook places a Cookie on the device of the user visiting Our Facebook Fan Page. Each Cookie contains a unique identifier code and remains active for a period of two years, except when it is deleted before the end of this period.

Facebook receives, records and processes the information stored in the Cookie, especially when the user visits the Facebook services, services that are provided by other members of the Facebook Fan Page and services by other companies that use Facebook services.

For more information on the privacy practices of Facebook, please visit Facebook Privacy Policy here: https://www.facebook.com/full_data_use_policy

CCPA Privacy

Your Rights under the CCPA

Under this Privacy Policy, and by law if You are a resident of California, You have the following rights:

- **The right to notice.** You must be properly notified which categories of Personal Data are being collected and the purposes for which the Personal Data is being used.
- **The right to access / the right to request.** The CCPA permits You to request and obtain from the Company information regarding the disclosure of Your Personal Data that has been collected in the past 12 months by the Company or its subsidiaries to a third-party for the third party's direct marketing purposes.
- **The right to say no to the sale of Personal Data.** You also have the right to ask the Company not to sell Your Personal Data to third parties. You can submit such a request by visiting our "Do Not Sell My Personal Information" section or web page.
- **The right to know about Your Personal Data.** You have the right to request and obtain from the Company information regarding the disclosure of the following:
    - The categories of Personal Data collected
    - The sources from which the Personal Data was collected
    - The business or commercial purpose for collecting or selling the Personal Data

- Categories of third parties with whom We share Personal Data
- The specific pieces of Personal Data we collected about You

- **The right to delete Personal Data.** You also have the right to request the deletion of Your Personal Data that have been collected in the past 12 months.
- **The right not to be discriminated against.** You have the right not to be discriminated against for exercising any of Your Consumer's rights, including by:
  - Denying goods or services to You
  - Charging different prices or rates for goods or services, including the use of discounts or other benefits or imposing penalties
  - Providing a different level or quality of goods or services to You
  - Suggesting that You will receive a different price or rate for goods or services or a different level or quality of goods or services.

Exercising Your CCPA Data Protection Rights

In order to exercise any of Your rights under the CCPA, and if you are a California resident, You can email or call us or visit our "Do Not Sell My Personal Information" section or web page.

The Company will disclose and deliver the required information free of charge within 45 days of receiving Your verifiable request. The time period to provide the required information may be extended once by an additional 45 days when reasonable necessary and with prior notice.

Do Not Sell My Personal Information

We do not sell personal information. However, the Service Providers we partner with (for example, our advertising partners) may use technology on the Service that "sells" personal information as defined by the CCPA law.

If you wish to opt out of the use of your personal information for interest-based advertising purposes and these potential sales as defined under CCPA law, you may do so by following the instructions below.

Please note that any opt out is specific to the browser You use. You may need to opt out on every browser that you use.

Website

You can opt out of receiving ads that are personalized as served by our Service Providers by following our instructions presented on the Service:

- From Our "Cookie Consent" notice banner
- Or from Our "CCPA Opt-out" notice banner

- Or from Our "Do Not Sell My Personal Information" notice banner
- Or from Our "Do Not Sell My Personal Information" link

The opt out will place a cookie on Your computer that is unique to the browser You use to opt out. If you change browsers or delete the cookies saved by your browser, you will need to opt out again.

Mobile Devices

Your mobile device may give you the ability to opt out of the use of information about the apps you use in order to serve you ads that are targeted to your interests:

- "Opt out of Interest-Based Ads" or "Opt out of Ads Personalization" on Android devices
- "Limit Ad Tracking" on iOS devices

You can also stop the collection of location information from Your mobile device by changing the preferences on your mobile device.

"Do Not Track" Policy as Required by California Online Privacy Protection Act (CalOPPA)

Our Service does not respond to Do Not Track signals.

However, some third party websites do keep track of Your browsing activities. If You are visiting such websites, You can set Your preferences in Your web browser to inform websites that You do not want to be tracked. You can enable or disable DNT by visiting the preferences or settings page of Your web browser.

Children's Privacy

The Service may contain content appropriate for children under the age of 13. As a parent, you should know that through the Service children under the age of 13 may participate in activities that involve the collection or use of personal information. We use reasonable efforts to ensure that before we collect any personal information from a child, the child's parent receives notice of and consents to our personal information practices.

We also may limit how We collect, use, and store some of the information of Users between 13 and 18 years old. In some cases, this means We will be unable to provide certain functionality of the Service to these Users. If We need to rely on consent as a legal basis for processing Your information and Your country requires consent from a parent, We may require Your parent's consent before We collect and use that information.

We may ask a User to verify its date of birth before collecting any personal information from them. If the User is under the age of 13, the Service will be either blocked or redirected to a parental consent process.

Information Collected from Children Under the Age of 13

The Company may collect and store persistent identifiers such as cookies or IP addresses from Children without parental consent for the purpose of supporting the internal operation of the Service.

We may collect and store other personal information about children if this information is submitted by a child with prior parent consent or by the parent or guardian of the child.

The Company may collect and store the following types of personal information about a child when submitted by a child with prior parental consent or by the parent or guardian of the child:

- First and/or last name
- Date of birth
- Gender
- Grade level
- Email address
- Telephone number
- Parent's or guardian's name
- Parent's or guardian's email address

For further details on the information We might collect, You can refer to the "Types of Data Collected" section of this Privacy Policy. We follow our standard Privacy Policy for the disclosure of personal information collected from and about children.

Parental Access

A parent who has already given the Company permission to collect and use his child personal information can, at any time:

- Review, correct or delete the child's personal information
- Discontinue further collection or use of the child's personal information

To make such a request, You can write to Us using the contact information provided in this Privacy Policy.

Your California Privacy Rights (California's Shine the Light law)

Under California Civil Code Section 1798 (California's Shine the Light law), California residents with an established business relationship with us can request information once a year about sharing their Personal Data with third parties for the third parties' direct marketing purposes.

If you'd like to request more information under the California Shine the Light law, and if you are a California resident, You can contact Us using the contact information provided below.

California Privacy Rights for Minor Users (California Business and Professions Code Section 22581)

California Business and Professions Code section 22581 allow California residents under the age of 18 who are registered users of online sites, services or applications to request and obtain removal of content or information they have publicly posted.

To request removal of such data, and if you are a California resident, You can contact Us using the contact information provided below, and include the email address associated with Your account.

Be aware that Your request does not guarantee complete or comprehensive removal of content or information posted online and that the law may not permit or require removal in certain circumstances.

Links to Other Websites

Our Service may contain links to other websites that are not operated by Us. If You click on a third party link, You will be directed to that third party's site. We strongly advise You to review the Privacy Policy of every site You visit.

We have no control over and assume no responsibility for the content, privacy policies or practices of any third party sites or services.

Changes to this Privacy Policy

We may update our Privacy Policy from time to time. We will notify You of any changes by posting the new Privacy Policy on this page.

We will let You know via email and/or a prominent notice on Our Service, prior to the change becoming effective and update the "Last updated" date at the top of this Privacy Policy.

You are advised to review this Privacy Policy periodically for any changes. Changes to this Privacy Policy are effective when they are posted on this page.

Contact Us

If you have any questions about this Privacy Policy, You can contact us:

By email: info@traincentricapp.com

By visiting this page on our website: https://www.traincentricapp.com

BUSINESS ASSOCIATE AGREEMENT

This Business Associate Agreement is entered into by and between Train Centric, ("Business Associate") and you ("Covered Entity") to permit Business Associate to create, receive, maintain, and transmit Protected Health Information (including Electronic Protected Health Information) for or on behalf of Covered Entity, so that Business Associate may render services, advice, and consultation ("Services") to Covered Entity under the terms of an agreement between Business Associate and Covered Entity (the "Services Agreement"). This Agreement shall be considered part of the Services Agreement between Business Associate and Covered Entity.

I. Definitions

Capitalized terms used but not otherwise defined in this Agreement shall have the same meaning as those terms in final regulations relating to privacy and security of individually identifiable health information at 45 CFR parts 160, 162, and 164 implementing the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH), as amended from time to time.

(A) "Breach Notification Rule" means the final regulatory provisions set forth at 45 CFR Subtitle A, Subchapter C, Parts 160 and 164, Subparts A and D.

(B) "Compliance Date" means the later of (1) the date that compliance is required under the relevant provision of the HIPAA Rules, and (2) the date this Agreement takes effect between the Parties.

(C) "HIPAA Rules" means, collectively, the Breach Notification Rule, Privacy Rule, and Security Rule.

(D) "Individual" has the same meaning as in the HIPAA Rules, as well as a person who qualifies as a personal representative in accordance with the HIPAA Rules.

(E) "Internal Material" means Business Associate's documented internal practices, books, and records, including policies and procedures relating to the use and disclosure of PHI created, received, maintained, or transmitted by, Business Associate for or on behalf of Covered Entity.

(F) "Privacy Rule" means final regulatory provisions set forth at 45 CFR Subtitle A, Subchapter C, Parts 160 and 164, Subparts A and E.

(G) "Protected Health Information" or "PHI", "Electronic Protected Health Information" or "ePHI" have the same meaning as "protected health information" and "electronic protected health information" in the HIPAA Rules, but limited to the information created, received, maintained, or transmitted by Business Associate for or on behalf of Covered Entity.

(H) "Security Rule" means final regulatory provisions set forth at 45 CFR Subtitle A, Subchapter C, Parts 160 and 164, Subparts A and C.

II. **Obligations and Activities of Business Associate**

(A) Business Associate agrees not to use or disclose PHI other than as necessary to render Services pursuant to the Services Agreement, as permitted or required by this Agreement, or as Required by Law.

(B) Business Associate agrees to use appropriate safeguards and comply, where applicable, with the Security Rule with respect to ePHI to prevent use or disclosure of the information other than as provided for by this Agreement.

(C) Business Associate agrees to report to Covered Entity any use or disclosure of PHI of which it becomes aware that is not permitted by this Agreement, including but not limited to any Breach of Unsecured PHI.

(D) Business Associate agrees to report to Covered Entity in a reasonable manner and upon request by Covered Entity, but not more than once in any 12-month period, aggregate information on unsuccessful Security Incidents.

(E) Business Associate agrees to ensure that any subcontractor that creates, receives, maintains or transmits PHI for or on behalf of Business Associate agrees to the same restrictions and conditions that apply through this Agreement to Business Associate with respect to such information, including the use and implementation of safeguards as required by Section II.(B) of this Agreement.

(F) Upon request by the Secretary, and subject to Business Associate's obligations under all other applicable laws, regulations, or orders of a court or other tribunal, Business Associate agrees to make available to the Secretary Business Associate's Internal Material for use by the Secretary in determining whether Covered Entity or Business Associate is in compliance with the HIPAA Rules. Business Associate may delay complying with a request of the Secretary as to this provision while Business Associate makes reasonable efforts to ascertain its applicable obligations with respect to this Section II.(F).

(G) Subject to Business Associate's obligations and rights relating to all other applicable laws, regulations, or orders of a court or other tribunal, and all other applicable privacy and confidentiality laws and regulations, Business Associate agrees to document any disclosures of PHI and to provide to Covered Entity upon written request, within a reasonable time and in a reasonable manner, information related to such disclosures as necessary for Covered Entity to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 CFR § 164.528. Notwithstanding the foregoing, Business Associate shall not be obligated to respond to an Individual's request for an accounting of disclosures of PHI that is made by the Individual directly to Business Associate.

(H) Business Associate agrees to provide to Covered Entity upon written request all PHI that has been identified by Covered Entity as part of a Designated Record Set, is not otherwise available to Covered Entity from any other source, is not subject to any legally enforceable nondisclosure or confidentiality order, and is necessary for Covered Entity to respond to an Individual's request for access to, or amendment of, PHI pursuant to 45 CFR §§ 164.524 or 164.526. If PHI subject to this paragraph is maintained electronically, Business Associate will provide the PHI in the requested electronic form and format, if it

is readily producible in such form and format; if the PHI is not readily producible by Business Associate in the requested form and format, Business Associate will provide the PHI to Covered Entity in a readable electronic form as agreed by Covered Entity and Business Associate. Notwithstanding the foregoing, Business Associate shall not be obligated to respond to an Individual's request for access to PHI maintained in a Designated Record Set that is made by the Individual directly to Business Associate.

(I) Upon written instructions from Covered Entity, and subject to Business Associate's needs in order to provide Services, any professional obligation, or any legally enforceable requirement to maintain PHI without amendment, revision, or other changes, Business Associate agrees to incorporate any amendment to PHI agreed to by Covered Entity pursuant to 45 CFR § 164.526.

(J) Subject to Business Associate's needs in order to provide Services, any professional obligation, or any legally enforceable requirement to use or disclose PHI, and upon receipt of written instructions from Covered Entity, Business Associate agrees to honor any restriction on use or disclosure of PHI or request for confidential communications as agreed to by Covered Entity pursuant to 45 CFR § 164.522.

(K) Business Associate agrees to report to Covered Entity any Breach of Unsecured PHI as required by the Breach Notification Rule. Notwithstanding the foregoing, Business Associate is under no other obligation to make any report of a Breach of Unsecured PHI to any individual, government agency, or the media.

(L) Business Associate agrees that as of the Compliance Date of any amendments to the HIPAA Rules, it will conform its practices to comply with amended requirements applicable to Business Associate; provided, however, that Business Associate may instead terminate this Agreement and the Services Agreement as provided by Section VI.(C).

(M) To the extent that Business Associate is to carry out any of Covered Entity's obligations under the Privacy Rule, Business Associate will comply with the requirements of the Privacy Rule that would apply to Covered Entity in the performance of such obligations.

III. Permitted Uses and Disclosures by Business Associate

(A) Except as otherwise permitted or limited by this Agreement, Business Associate may use or disclose PHI to render Services to or on behalf of Covered Entity, provided that such use or disclosure would not violate (1) the HIPAA Rules if such use or disclosure was made by Covered Entity, or (2) the minimum necessary policies and procedures of Covered Entity if those policies and procedures have been disclosed to Business Associate.

(B) Business Associate may use PHI for the proper management and administration of Business Associate and to carry out the legal responsibilities of Business Associate.

(C) Business Associate may disclose PHI for the proper management and administration of Business Associate or to carry out Business Associate's legal responsibilities, provided that (1) such disclosures are Required by Law, or (2) Business Associate obtains reasonable assurances from the recipient of the PHI that the PHI will remain confidential

and will be used or further disclosed only as Required by Law or for the purpose for which it was disclosed to the recipient, and that the recipient will notify Business Associate of any instances of which the recipient is aware in which the confidentiality of the PHI has been breached.

(D) Business associate may provide data aggregation services related to the health care operations of the Covered Entity.

IV. Obligations of Covered Entity

(A) Covered Entity shall notify Business Associate of any limitations in the Covered Entity's Notice of Privacy Practices, to the extent such limitations may affect Business Associate's use or disclosure of PHI.

(B) Covered Entity shall notify Business Associate of any changes in, or revocation of, permission granted by any Individual to use or disclose PHI, to the extent such changes or revocations may affect Business Associate's use or disclosure of PHI.

(C) Covered Entity shall notify Business Associate of any restrictions on the use or disclosure of PHI to which Covered Entity has agreed in accordance with 45 CFR § 164.522, to the extent such restrictions may affect Business Associate's use or disclosure of PHI.

V. Permissible Requests by Covered Entity

Except as provided in Section III of this Agreement, Covered Entity shall not request Business Associate to use or disclose PHI in any manner that would not be permissible under the HIPAA Rules if such use or disclosure was made by Covered Entity.

VI. Term and Termination

(A) Term: This Agreement shall become effective the day the Covered Entity signs up sand shall terminate when all of the PHI is destroyed or returned to Covered entity or, if it is infeasible to return or destroy such PHI , when protections are extended to such PHI in accordance with the termination provisions in Section VI. (D) of this Agreement.

(B) Termination for Cause: Upon Covered Entity's knowledge of a breach of a material term of this Agreement by Business Associate, Covered Entity shall:

(1) Provide an opportunity for Business Associate to cure the breach and, if Business Associate does not cure the breach within a reasonable time, terminate this Agreement;

(2) Immediately terminate this Agreement if Business Associate has breached a material term of this Agreement and cure is not possible; or

(3) If neither termination nor cure is feasible, report the violation to the Secretary.

(C) Termination by Business Associate in Lieu of Amendment: If Business Associate determines that it is not reasonably able to comply with any final new or amended provision of the HIPAA Rules, Business Associate may terminate this Agreement (and the Services Agreement) upon notice to Covered Entity.

(D) Effect of Termination:

(1) Except as provided in Section VI.(D)(2) of this Agreement, upon termination of the Agreement for any reason, Business Associate shall return or destroy all PHI or ePHI. This provision shall also apply to PHI that is in the possession of subcontractors of Business Associate. Business Associate shall retain no copies of the PHI.

(2) If Business Associate determines that returning or destroying the PHI is infeasible, Business Associate shall provide to Covered Entity notification of the conditions that make return or destruction infeasible and extend the protections of this Agreement to such PHI and limit further uses and disclosures of such PHI to those purposes that make return or destruction infeasible, for so long as Business Associate retains such PHI.

VII. **Miscellaneous**

(A) Regulatory References: A reference in this Agreement to a section in the HIPAA Rules means the section as in effect or amended, if such amendment is final and the Compliance Date for such amendment has passed.

(B) Amendment: The Parties agree to negotiate in good faith to amend this Agreement from time to time as is necessary for Covered Entity to comply with any new or revised final requirements of the HIPAA Rules, HIPAA, and HITECH. This Agreement may be amended only by a writing signed by both Business Associate and Covered Entity.

(C) Survival: The rights and obligations of Business Associate under Sections II, III. (B), (C), and (D), and VI.(D) of this Agreement shall survive the termination of this Agreement.

(D) Interpretation: If Covered Entity or Business Associate determines that there is any ambiguity in this Agreement, they shall discuss the provision(s) in question and shall attempt, in good faith, to resolve the ambiguity in a manner that permits Covered Entity to comply with the HIPAA Rules and that permits Business Associate to comply with the terms of this Agreement and to render Services.

(E) No Third-Party Beneficiaries: Nothing in this Agreement confers on any person other than Business Associate and Covered Entity any rights, remedies, obligations, or liabilities.

(F) Severability: If any provision of this Agreement is held by a court of competent jurisdiction to be illegal, invalid, or unenforceable, the remaining provisions of this Agreement shall not be affected.

(G) Counterparts: This Agreement may be executed in counterparts, all of which together shall constitute a single agreement and any one of which shall be deemed an original. A facsimile copy of a signed counterpart shall be treated as an original.

(H) Waiver: A waiver by Business Associate or Covered Entity of any requirement of this Agreement shall not be construed as a continuing waiver, a waiver of any other requirement, or a waiver of any right or remedy otherwise available.

(I) Notices: Any notice required by this Agreement shall be provided to the address below, using a national courier service for next business day delivery. In addition, and not in lieu of such notice, an e-mail with a copy of the notice shall also be provided and sent to the email address below, not later than the date such notice is deposited with the national courier service. An address for notice may be changed by giving notice as required by this paragraph.

(J) Notwithstanding anything to the contrary in this Agreement, the following shall apply:

(1) No provision herein shall be construed to require Business Associate to engage in any conduct that would be a violation of federal, state, local, or other applicable law including any lawful administrative or judicial order, or all other applicable privacy and confidentiality laws and regulations.

(2) To the maximum extent permitted by applicable law and without intending to give rise to any violation of the HIPAA Rules, each party reserves and retains any and all lawfully applicable self-incrimination and other privileges and immunities including, but not limited to, the attorney-client privilege and the attorney work-product protections.