Last Updated: [January 1, 2023]

California Employee Privacy Policy

This California Employee Privacy Policy ("Privacy Policy") applies only to California residents. It does not apply to anyone else.

This Privacy Policy describes how Tentamus North America (collectively, "we", "us" or "our") collects information about employees ("you"), the purpose for the collection, to whom we disclose it and the purpose for such disclosure. Your status as a current or prospective employee means that you accept the terms of this Privacy Policy. We reserve the right to change this Privacy Policy at any time. If we change our Privacy Policy, we will post an updated version on this website and send you a notification. Updates to the Privacy Policy will be referenced by the "Last Updated" date shown above. This policy should be read together with any other privacy statement or notice we may provide on specific occasions when we are collecting or processing personal information about you so that you are fully aware of how and why we are using your data.

1. INFORMATION WE COLLECT, HOW WE COLLECT IT AND WHY WE COLLECT IT.

We collect personal information from our employees for a variety of business reasons as indicated in the chart below. Please note the specific pieces of personal information we may collect about you can vary depending on the nature of your interactions with us. We may not collect all of the personal information referenced below regarding you.

The term "personal information" means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. "Personal information" does not include: (1) publicly available information or lawfully obtained, truthful information that is a matter of public concern; or (2) information that is deidentified or aggregate consumer information.

We also collect "sensitive personal information," as set forth below. Sensitive personal information means personal information that reveals information such as: (1) social security, driver's license, state identification card, or passport number; (2) account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account; (3) precise geolocation; (4) racial or ethnic origin, religious or philosophical beliefs, or union membership; (5) the contents of a consumer's mail, email, and text messages unless we are the intended recipient of the communication; and (6) genetic data. Sensitive personal information also includes the processing of biometric information for the purpose of uniquely identifying a consumer, personal information collected and analyzed concerning a consumer's health and personal information collected and analyzed concerning a consumer's sex life or sexual orientation. Sensitive personal information that is publicly available is not considered sensitive personal information or personal information.

Set forth below are the categories of personal information we have collected in the preceding 12 months, the categories of sources from which the personal information was collected and the business purpose for the collection.

Category of Personal Information	**Examples**	**Categories of Sources from which Personal Information Collected**	**Business Purposes for Collection**
PERSONAL INFORMATION			

Category of Personal Information	Examples	Categories of Sources from which Personal Information Collected	Business Purposes for Collection
Personal Identifiers	Name Alias Postal address Phone number Email address Social security number Driver's license number Account name Device identifier Internet Protocol address Cookies, beacons, pixel tags, mobile identifiers, or similar technology	Directly from you Consumer reporting agencies Our service providers Automated means*	To manage workforce activities and personnel To maintain your contact information To assist you in case of emergency To recruit employees and perform background screening To manage wages and other awards To administer healthcare and other benefits To perform identity verification, accounting, security, audit, and other internal functions To monitor, investigate, prevent, and redress potential breaches of applicable policies, regulations, and laws, and/or comply with related investigations To ensure a safe working environment To comply with law or legal process such as tax deductions, reporting, and record-keeping requirements To evaluate or conduct a merger or other transaction in which personal information of our employees is among the assets transferred.
Protected Characteristics	Race Color Sex/gender Gender identity, gender expression* Sexual orientation* Marital status Medical Condition Military or veteran status National origin	Directly from you Consumer reporting agencies Our service providers	To comply with demographic reporting requirement For recruitment purposes To design employee retention programs and diversity initiatives To comply with law or legal process, such as tax deductions, reporting, and record-keeping requirements To determine eligibility for leave of absence or life and

Category of Personal Information	Examples	Categories of Sources from which Personal Information Collected	Business Purposes for Collection
	Disability (mental and physical including HIV/AIDS, cancer, and genetic characteristics) Request for family care leave Request for leave for an employee's own serious health condition Request for pregnancy disability leave Retaliation for reporting patient abuse in tax-supported institutions Age (over 40)		disability insurance and other employee benefits
Biometric Information	Drug screen Vaccine records Certain other information	Directly from you Service providers	Employee credentialling process
Internet Information	Internet Protocol address Cookies**, beacons, pixel tags, mobile ad identifiers, or similar technology	Automated means	To manage workforce activities and personnel To perform identity verification, accounting, security, audit, and other internal functions To operate and manage IT and communications systems and facilities To maintain security on our websites and Internet-connected assets
Audiovisual Information	Camera footage Recordings of meetings	Cameras at our properties Online platforms	To manage workforce activities and personnel As necessary or appropriate to protect or defend the rights, property or safety of us, our employees, our users, or other
Professional and Educational Information	Professional history Employee history Educational history	Directly from you. Consumer reporting agencies Your prior employers Our service providers	To manage workforce activities and personnel To recruit employees and perform background screening To ensure compliance with work-related licensing and credentialing

Category of Personal Information	Examples	Categories of Sources from which Personal Information Collected	Business Purposes for Collection
			To facilitate a better, safer, and more efficient working environment To monitor, investigate, prevent, and redress potential breaches of applicable policies, regulations, and laws To carry out our obligations and enforce our rights arising from any contracts entered into between you and us To evaluate or conduct a merger or other transaction in which personal information of our employees is among the assets transferred
SENSITIVE PERSONAL INFORMATION			
Sensitive Personal Identifiers	Social security Driver's license State identification card Passport number	Directly from you	To recruit employees and perform background screening To manage wages and other awards To administer healthcare and other benefits To perform identity verification, accounting, security, audit, and other internal functions To comply with law or legal process such as tax deductions, reporting and record-keeping requirements.
Account Information	Account log-in Username Password Security Information to log-in	Directly from you	To manage wages and other awards. To provide human resources management services. To administer healthcare and other benefits. To perform identity verification, accounting, security, audit, and other internal functions

Category of Personal Information	Examples	Categories of Sources from which Personal Information Collected	Business Purposes for Collection
Sensitive Protected Characteristics	See above under characteristics of protected classifications	See above under characteristics of protected classifications	See above under characteristics of protected classifications
Contents of Writings	Any document or email that is on our servers	Directly from you Automated means	To ensure compliance with our policies To manage workforce activities and personnel To perform identity verification, accounting, security, audit, and other internal functions To operate and manage IT and communications systems and facilities To maintain security on our websites and Internet-connected assets

* We don't actively collect this information in our employee records but may become aware of this if the employee makes statements or conducts themselves in a way to provide this information to us.

** We use cookies and other tracking technologies (such as web beacons, tracking pixels, and HTTP referrers). A cookie is a small file placed on your computer when you visit a site that can be understood by the site that issued the cookie. Web beacons are small bits of code embedded in web pages or in emails. We use web beacons to deliver or communicate with cookies, to count users who have visited a web page, and to understand usage patterns. We also include web beacons in e-mails to learn if messages have been opened, acted on, or forwarded.

Please note that some of our benefits providers may collect personal information from you that is not disclosed to us. For that information, please review the benefit provider's privacy policy and contact them with any questions.

2. INFORMATION WE SELL, SHARE, OR DISCLOSE, AND WHY WE DO SO.

We do not sell or share for cross-context behavioral advertising any personal information that we collect from you, as those terms are defined under the California Consumer Protection Act, as amended by the California Privacy Rights Act, and related regulations (collectively, the "CCPA").

We do, however, disclose personal information to service providers in a manner that does not constitute a sale or sharing of such information. Such disclosures may occur for the following business purposes:

A. **Security and Fraud Detection:** We use personal information for our security and fraud detection services including detecting security incidents, protecting against malicious, deceptive, fraudulent, or illegal activity; and prosecuting those responsible for that activity.

B. **Functionality & Debugging:** We use personal information to engage in debugging to identify and repair errors that impair existing intended functionality.

C. **Services on Our Behalf:** We may disclose personal information in order to receive services performed on our behalf, including maintaining or servicing accounts, providing service for employees, processing or fulfilling requests and transactions, verifying employee information, processing payroll, expenses and payments, providing analytic services, evaluating and responding to requests, providing storage, or providing similar services on our behalf

D. **Research & Development:** We use personal information for our internal research related to technological development and demonstration.

E. **Quality Control & Improvement of Services:** We use personal information to verify, maintain, and improve our services.

The following chart sets forth the categories of personal information we may disclose, and the business purposes for such disclosure:

Categories of Personal Information that We Disclose	**Business Purposes for the Disclosure of Personal Information**
PERSONAL INFORMATION	
Personal Identifiers	Security and Fraud Detection Functionality & Debugging Services on Our Behalf Research & Development Quality Control & Improvement of Services
Protected Characteristics	Security and Fraud Detection Functionality & Debugging Services on Our Behalf
Biometric Information	Security and Fraud Detection Functionality & Debugging Services on Our Behalf Research & Development Quality Control & Improvement of Services
Internet Information	Security and Fraud Detection Functionality & Debugging Services on Our Behalf Research & Development Quality Control & Improvement of Services
Audiovisual Information	Security and Fraud Detection Functionality & Debugging Services on Our Behalf Research & Development Quality Control & Improvement of Services
Professional and Educational Information	Security and Fraud Detection Functionality & Debugging

Categories of Personal Information that We Disclose	Business Purposes for the Disclosure of Personal Information
	Services on Our Behalf Research & Development Quality Control & Improvement of Services
SENSITIVE PERSONAL INFORMATION	
Sensitive Personal Identifiers	Security and Fraud Detection Functionality & Debugging Services on Our Behalf Quality Control & Improvement of Services
Account Information	Security and Fraud Detection Functionality & Debugging Services on Our Behalf Quality Control & Improvement of Services
Sensitive Protected Characteristics"	Security and Fraud Detection Functionality & Debugging Services on Our Behalf Quality Control & Improvement of Services
Contents of Communications	Security and Fraud Detection Functionality & Debugging Services on Our Behalf Quality Control & Improvement of Services

As Necessary: We may also disclose personal information, as necessary: (1) to our insurers and professional advisers for the purposes of managing risks, obtaining professional advice, exercising or defending against legal claims, etc.; (2) to comply with any legal process; (3) to respond to requests from public and government authorities; (4) to enforce our terms and conditions and policies; (5) to protect our operations and protect our rights, privacy, safety or property, and/or that of you or others; and (6) to allow us to pursue available remedies or limit the damages that we may sustain. As we develop our business, we might sell or buy businesses or assets. In the event of a corporate sale, merger, reorganization, dissolution, or similar event, personal information may be part of the transferred assets. Any successor to or acquirer will continue to have the right to use your personal information and other information in accordance with the terms of this Privacy Policy.

We only use sensitive personal information for purposes disclosed herein. We do not use or disclose sensitive personal information for purposes other than those specified herein.

3. HOW LONG WE KEEP YOUR PERSONAL INFORMATION.

We will retain your personal information for as long as necessary to fulfil the purposes we collected it. To determine the appropriate retention period for personal information, we consider the amount, nature, and sensitivity of the personal information, the potential risk of harm from unauthorized use or disclosure of your

personal information, the purposes for which we process your personal information and whether we can achieve those purposes through other means, and the applicable legal requirements.

Record retention for employee records is generally during the period of employment and for 6 years thereafter. However, for workers comp records, the period is during the period that the employee receives workers' compensation benefits plus 10 years. For employee benefit claim records, the period is the period until final resolution of the claim plus 10 years. Please contact us for more detailed information.

4. YOUR RIGHTS IF YOU ARE A RESIDENT OF CALIFORNIA.

In accordance with the CCPA, residents of the State of California are entitled to the following rights with respect to their personal information. Please note that these rights are subject to certain exceptions and certain of these rights are subject to verification mechanisms under the CCPA.

Rights to Know, Correct and Delete

Right to Know Personal Information Collected About You.

You have the right to know: (1) the categories of personal information we have collected about you; (2) the categories of sources from which the personal information is collected; (2) the business or commercial purpose for collecting personal information; (3) the categories of third parties to whom we disclose personal information; and (4) the specific pieces of personal information we have collected about you.

Right to Know Personal Information Disclosed and to Whom.

Since disclose your personal information, as described above, you have the right to request that we disclose to you: (1) the categories of personal information that we collected about you; and (2) the categories of personal information that we disclosed about you for a business purpose and the categories of persons to whom it was disclosed for a business purpose.

Right to Correct Inaccurate Information.

If you believe that any of the personal information we maintain about you is inaccurate, you have the right to submit a request for us to correct that information. Upon receipt of a request, we will use commercially reasonable efforts to correct the information as you direct.

Right to Request Deletion of Your Personal Information.

You have the right to request that we delete your personal information. There may be circumstances where we or our service providers cannot delete your personal information. Following receipt of a request, we will let you know what, if any, personal information we can delete from our records. If we cannot delete all of your personal information, we will let you know the reason.

Exercising Rights to Know, Correct and Delete, and Related Verification Measures

You may submit a request regarding your rights to know, correct and/or delete via by emailing us at **privacy@tentamus.com** or by calling us at **1-833-865-9499.**

Upon submission of a request to know, correct or delete, we will take reasonable steps to confirm that the person submitting the request to know or request to delete is the person to whom the information relates (or his or her authorized agent), and to prevent unauthorized access or deletion of information. The specific steps taken to verify the identity of the requesting person may vary based on the nature of the request, including the type, sensitivity, and value of the information requested, the risk of harm posed by unauthorized access or deletion, the likelihood that fraudulent or malicious actors may seek the information, the robustness

of personal information provided to verify your identity, the nature of our relationship with you, and available technology for verification.

We will generally try to avoid requesting additional information from you for the purpose of verification, but we may need to do so if we cannot verify your identity based on the information already maintained by us. If we request additional information to verify your identity, it will be for that purpose only and will be deleted as soon as practical after processing the request, except as otherwise provided by law.

The following generally describes the verification processes we use:

- **Password Protected Accounts**. If you have a password-protected account with us, we may use existing authentication practices to verify your identity but will require re-authentication before disclosing, correcting or deleting data. If we suspect fraudulent or malicious activity relating to your account, we will require further verification (as described below) before complying with a request to know or delete.

- **Verification for Non-Accountholders**. If you do not have, or cannot access, a password-protected account with us, we will generally verify your identity as follows:

    - For *requests to know categories of personal information*, we will verify your identity to a reasonable degree of certainty by matching at least two data points provided by you with reliable data points maintained by us.

    - For *requests to know specific pieces of personal information*, we will verify your identity to a reasonably high degree of certainty by matching at least three data points provided by you with reliable data points maintained by us. We will also require a declaration, signed under penalty of perjury, that the person requesting the information is the person whose information is the subject of the request or that person's authorized representative. We will maintain all signed declarations as part of our records.

    - For *requests to correct or delete personal information*, we will verify your identity to a reasonable degree or a reasonably high degree of certainty depending on the sensitivity of the personal information and the risk of harm posed by unauthorized deletion. We will act in good faith when determining the appropriate standard to apply.

If there is no reasonable method by which we can verify your identity, we will state so in response to a request to know or delete personal information, including an explanation of why we have no reasonable method to verify your identity.

If you use an authorized agent to submit a request to know, delete or correct, we may require the authorized agent to provide proof that you gave the agent signed permission to submit the request. We may also require you to do either of the following: (a) verify your own identity directly with us; or (b) directly confirm with us that you provided the authorized agent permission to submit the request. This requirement does not apply if you have provided the authorized agent with power of attorney pursuant to Probate Code sections 4121 to 4130.

We will respond to requests to know, requests to delete and / or delete no later than 45 calendar days. If we cannot verify your request within 45 days, we may deny your request. If necessary, we may take up to an additional 45 days to respond to your request but in such an event will provide you a notice and an explanation of the reason that we will take more than 45 days to respond to your request.

Right to Opt-Out of the Sale and Sharing of Your Personal Information. As noted above, we do not sell or share your personal information. As such, you do not have this right.

Right to Limit the Use of Your Sensitive Personal Information. We only use your sensitive personal information for the following purposes: (1) to that use which is necessary to perform the services reasonably expected by you; (2) to help to ensure security and integrity; (3) to perform services on our behalf; (4) to undertake activities to verify or maintain the quality or safety of a service or device that is owned, manufactured, manufactured for, or controlled by us; and (5) to improve, upgrade, or enhance the service or device that is owned, manufactured, manufactured for, or controlled by us. Given the nature of our use of your sensitive personal information, you do not have the right to request that we limit the use of your sensitive personal information.

Right to Non-Discrimination for Exercising Your Rights. If you choose to exercise any of your rights, you have the right to not receive discriminatory treatment by us. This includes the right not to be retaliated against for the exercise of your rights

5. CONTACT INFORMATION.

If you have any questions or concerns about our privacy policies and practices, please feel free to contact us by emailing us at **privacy@tentamus.com** or by calling us at **1-833-865-9499.**