

**PRIVACY POLICY**  
Last updated: 9/17/2022

This Privacy Policy covers Velocitos, Inc.'s ("Company", "us", "our", or "we") treatment of personal information and how it may be gathered through our applications ("Platform" or "Product(s)" or "Service Software") and through the use of our services (the "Services") by the customer ("you" or "Customer"). Any information that is provided to us during use of our Service, information that we gather based on use of our Service will only be used in accordance with this Privacy Policy. Please carefully read our Privacy Policy as by using our Service, you consent to our Privacy Policy. If you are not satisfied with our Privacy Policy, please do not use our Platform.

This Privacy Notice does not cover handling of your personal data as an employee, intern, consultant, contractor or applicant of Company and does not cover any information collected by third-party sites or content or applications that may link to or be accessible from communications sent using the Platform.

1. **Definitions.** Capitalized terms not otherwise defined in this Agreement shall have the meanings ascribed to them below.
  - 1.1. **"Authorized Users"** means all users, including but not limited to employees, contractors and Practices, authorized by Customer to access the Services Software and the Platform.
  - 1.2. **"Company Materials"** means the Products, Services Software, Documentation and Company Systems, Company's Confidential Information and any and all other proprietary documents, materials, devices, methods, processes, hardware, software and other technologies and inventions, technical or functional descriptions, requirements, plans or reports of Company, that are provided or used by or on behalf of Company or any Company personnel in connection with the Service Software or relate to the Services or Company Systems.
  - 1.3. **"Company System"** means the information technology infrastructure used by or on behalf of Company in performing the Services or providing the Service Software, including all computers, software, hardware, databases, electronic systems and networks, whether operated directly by Company or through the use of third-party services.
  - 1.4. **"Confidential Information"** means any information disclosed by one Party to the other or accessed by the other under this Agreement, which, (i) if in written, graphic, machine readable or other tangible form is marked "Confidential" or "Proprietary" or which, if disclosed orally or by demonstration, is identified at the time of disclosure as confidential and reduced to a writing marked "Confidential" and delivered to the Receiving Party (as defined below) within thirty (30) days of such disclosure; or (ii) by the nature of the circumstances surrounding the disclosure, ought in good faith to be treated as confidential. Notwithstanding any failure to so identify them, all technology or proprietary information underlying the Platform and the Company System shall be deemed Confidential Information of Company, and the Customer Data, the identity of the Customer Clients, and the existence of this Agreement shall be deemed Confidential Information of Customer.

1.5. “**Customer Data**” means data and other content, in any form or medium that is collected, downloaded or otherwise received, directly or indirectly from Customer or an Authorized User by or through the Service Software.

1.6. “**Customer’s Systems**” means Customer’s information technology infrastructure, including computers, software, hardware, databases, electronic systems (including database management systems) and networks, whether operated directly by the Customer or through the use of third-party services.

1.7. “**Documentation**” means any documentation provided by Company for use with the Platform under this Agreement.

1.8. “**Personally Identifiable Information**” means any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means.

1.9. “**Platform**” means the interface created by Company which allows Customer and Authorized Users to use the Service Software, the Company System and all changes, corrections, bug fixes, enhancements, updates and other modifications thereto.

1.10. “**Product(s)**” means mean any Service Software, Company Materials, platform or other Services provided by Company pursuant to this Agreement, including any interface created by Company where the Customer and Authorized Users view the branded dashboard and data streams, and all changes, corrections, bug fixes, enhancements, updates and other modifications thereto, whether made by or on behalf of Company, Customer, or any third party.

1.11. “**Protected Health Information**” means any data relating to a Customer’s member’s or patient, a member’s healthcare, or the payment for that healthcare that is created, received, stored, or transmitted by HIPAA-covered entities and their business associates.

1.12. “**Services**” means any maintenance, training, configuration, data extraction, data feed, support, hosting, professional, and any other service provided by Company to Customer.

1.13. “**Service Software**” means Company’s proprietary software application or applications and any third party software (and any computer program or module related thereto), including all Documentation, new versions, updates, enhancements, upgrades, revisions, improvements and modifications of the foregoing that Company provides remote access to and use of as part of the Services.

## 2. **What Personal Data Do We Collect**

2.1. **Identifiers**. This includes PII such as the Customer's members' full name, address, email, company name, company website, telephone number, caller ID information, unique personal identifier, online identifier, Internet Protocol (“IP”) address, etc.

2.2. Metadata. This includes information about the communications delivered to the Customer's members' via our platform such as source and destination information, IP address, completion status, time and duration of delivery, etc.

2.3. Health Data. This includes any PHI of the Customer's members including but not limited to diagnosis codes, appointment dates, date of birth, gender, medications data, allergies list, vaccination data, medical conditions, surgeries, etc..

2.4. Events. This includes status information and changes regarding the Customer's members such as member joining the platform, member scheduling an appointment, member leaving the platform, member needing a care management intervention, etc.

2.5. Member Actions. This includes any and all Customer's members' actions on pieces of communications sent to them such as email opened, link clicked, texts responded, etc.

2.6. Usage Information. We collect certain information automatically when a Authorized User uses our Product(s), such as the Internet protocol (IP) address, device identifiers, browser type, operating system, Internet service provider, pages that you visit, the date and time of the visit, information about the links clicked, the pages viewed, the general manner in which navigation between pages is done, and other standard server log information.

### **3. What Personal Data We Do Not Collect**

We do not intentionally collect data that might reveal a Customer's members' religious or philosophical beliefs, political opinions, sexual preferences, precise geographical location, credit card numbers or financial data. If we find out that our servers have inadvertently collected this data, and that this data may be linked to a specific member (through reasonably available means), we will promptly delete the data or make it inaccessible by third parties, as applicable.

### **4. How Do We Collect Personal Data**

4.1. Direct Interactions. When Customer's members' interact with communications sent to them, these interactions are automatically tracked, collected, aggregated and collated within the Platform's database systems.

4.2. Automated Technologies. We may automatically collect technical data about equipment, browsing actions, click actions and patterns.

4.3. Indirectly. We may automatically collect information as a service provider in the course of providing communications services.

4.4. APIs. We collect the information you provide directly to us about your members using our APIs. This could potentially include both PII and PHI data of your members.

4.5. SDKs embedded within Customer's Digital Portals. We collect information that is directly pushed into our SDKs that are embedded within your mobile apps and web portals. Such information collected could potentially include both PII and PHI data of your members.

4.6. File Uploads. We collect the information you upload into our Platform about your members. This could potentially include both PII and PHI data of your members.

## 5. How We Use The Collected Personal Data

5.1. To fulfill or meet the reason you provided the information to our Products and Services.

- a. To enable our Customers and their Authorized Users to send and receive communications via our Platform to their members
- b. To allow you to interact with our systems
- c. To create, maintain, customize and secure your account with us.
- d. To process your requests, workflows and other executable items on the Platform
- e. To view member actions on various pieces of communications that have been sent to them
- f. To maintain the safety, security and integrity of our website, services, databases and other technology assets and business.
- g. For testing, research, development, and analysis; mitigation of fraud and spam (as applicable per specific product offering), unlawful or abusive activity, or violations of our Terms of Service; perform quality control; gauge routing effectiveness and deliverability and product development, including developing and improving our websites and Products and Services.
- h. As described to you when collecting your personal data.

5.2. Law Enforcement & Government Officials.

- a. To respond to law enforcement requests and as required by applicable law, court order, governmental regulations, or other legal process where we believe in good faith that disclosure protects your safety and/or the safety of others, or where we need to protect a legitimate business interest such as fighting against fraud that harms our rights.

The legal basis for collecting and using the personal data described above will depend on the personal data concerned and the specific context in which we collect it, including but not limited to: (a) performance of a contract; (b) legitimate interest; (c) necessary for compliance with a legal obligation; or (d) consent to collect and process your personal data.

Company will not use the personal data we collected for materially different, unrelated, or incompatible purposes without providing you notice. We may use non-personal data for any business purpose. To improve our products and services, we commonly will de-identify/anonymize or aggregate your personal data (so that it can no longer be associated with you), in which case we may use this information indefinitely without further notice to you.

## 6. **How we Share Your Personal Data**

We may disclose your personal data to a third party for a business purpose. Company may share your personal data in the following ways:

- a) To companies that perform services on our behalf only as needed for them to perform those services, including other communications providers in order to route communications over the Company network.
- b) To any member of our corporate group, which means our subsidiaries, our ultimate holding company and its subsidiaries.
- c) To data analytic providers.
- d) To other companies and entities, to:
  - i. Respond to emergencies or exigencies;
  - ii. Comply with court orders, law, and other legal process, including responding to any government or regulatory request;
  - iii. Assist with identity verification, preventing fraud, and identity theft;
- e) For any other purpose that we disclose in writing when you provide the personal data, with your consent.
- f) To sell, transfer, merge, divest, restructure, reorganize, or dissolve all or a portion of our business or assets.
- g) To enforce our Terms of Service and other related agreements.

## 7. **Security**

We are extremely sensitive to maintaining the security of the information that you as a Customer have entrusted us with, regarding your members. We use reasonable measures to help protect information from loss, theft, misuse and unauthorized access, disclosure, alteration and destruction. In order to prevent unauthorized access or disclosure, we have put in place suitable physical, electronic and managerial procedures to safeguard and secure the information that is entered into our Service.

As part of Company's protected health information ("PHI") privacy policy and its Confidential Information privacy compliance program, and in connection with its desire to uniformly protect PHI and other sensitive data, Company maintains a HIPAA Data Management Policy, Data Integrity Policy and Risk Management Policy that, to the best of Company's knowledge, comply with all applicable federal and state statutes and regulations.

## 8. **International Customers**

If you are located outside of the United States, you should know that the information you provide to us is being transmitted to us and processed in the United States and will be protected subject to this Privacy Policy and United States laws, which may not be as protective as the laws in your country.

9. **How to Contact Us**

If you have questions about this Privacy Notice, concerns, or questions, please contact [support@velocitos.com](mailto:support@velocitos.com). To contact us in writing, please use:

Velocitos Inc.  
39899, Balentine Dr., Suite 200  
Newark, CA 94560.