Privacy Statement

1. **Our Commitment to Privacy**

Privacy is highly important to us at Geriatric Practice Management Corp ("GPM"). This Privacy Policy (this "Policy") sets out the key elements of how we address the privacy and security of information entrusted to us by our customers through their access and use of all GPM Corp Services including but not limited to GEHRIMED electronic health record platform and CareTeam (together the "Services"), as well as the privacy of information entrusted to us by business partners, prospects and others who seek information and/or contact us through www.gehrimed.com and www.careteamhub.com (together the "Sites"). The Sites can be used and accessed by the public as a source of general information about GEHRIMED and CareTeam. Our customers and business partners also can access the Services via the Sites.

As privacy laws and practices evolve, we will amend this Policy from time to time. While we will endeavor to give reasonable notice of such changes, we do reserve the right, where necessary, to do so without prior notice.

What is considered private?

Information that is used by a government authority, financial institution or insurance carrier to distinguish a person from other individuals (e.g., social security number, social insurance number, credit card information, or insurance policy number) is private. Such information can be used to identify an individual (e.g., a person who works at a healthcare facility, or a resident or patient in a healthcare facility). Certain information may be used to contact a person directly (e.g., an email address, home mailing address or home telephone number). Depending on the jurisdiction, the above identifiers are considered to be Personal Information ("PI"), Personally Identifiable Information ("PII"), or a similar term, and it is private. An individual's business contact information and business title generally are exempt from privacy laws. Information about an individual's health, including insurance and billing information, is also considered – depending on the jurisdiction – to be PI, Protected Health Information ("PHI"), Personal Health Information (also known as "PHI"), Individually Identifiable Health Information ("IIHI") or a similar term, and it also is private.

For the remainder of this Policy, we will refer to all PI, PII, PHI, IIHI, and "Health Information" as "Personal Information" unless we specifically note otherwise.

This Policy also will apply to non-personal information if such information can be used in combination with other Personal Information or non-personal information to identify an individual.

Please be aware that this Policy only covers information manually submitted to, or automatically collected by, us through use of the Site and/or the Services. If you contact or exchange information with another GPM customer or business partner in person or through a means other than through the Site or Services, such activity is not covered by this Policy. Additionally, if you are ***not*** a customer or a business partner of GPM by way of written agreement, and are contacting us out of interest in the Services, a business partnership or a job opportunity, please be aware that the information that you share with us is not covered by this Policy, unless required by law.

2. **Personal Information Collected by the Services**

There are three ways Personal Information can be submitted to us. The first is through direct submission or what we call 'Manual Submission', the second is by way of 'Automatic Submission' triggered by any interaction with the Sites through a computer, mobile device or tablet, and the third is "Billing and Financial Submission".

Manual Submission

Personal Information can be submitted to us directly when you communicate with us offline (in person or by telephone), via email or via the Sites (by entering data or uploading files) or when you authorize GPM through our Services to access, retrieve and/or import Personal Information from another user or third party on your behalf. Additionally, if you become a customer of GPM, you will be required to register by submitting Personal Information via the Sites, email or offline. This could include name, email address, mailing address, telephone numbers and other contact and billing information.

Automatic Submission

Whenever your computer, mobile device or tablet visits, logs in or otherwise interacts with the Sites, we gather data from your device and the operating software of your device transmits a 'request' to us. That request includes non-

personal information that is necessary to identify and route the information your device is requesting. This communication is necessary for all website and Internet services.

We also use cookies (sometimes referred to as “web beacons” or “server logs”). Cookies are files that web browsers place on a computer’s hard drive that tell us whether customers or visitors have been to the Sites previously. Data collected in this way can include:

- Date and time a ‘request’ is transmitted through the Sites
- The model of the device making the request
- The type and version of the operating software running on the device
- The web browser used on the device and making the request
- IP address
- Geographic location
- Search terms used
- URLs visited

Additionally, we use Google Analytics to track and analyze page usage behavior to improve performance in the use of the Services and the Sites. We use this to track only what page you are clicking on, and do not use it to track any Personal Information.

Financial and Billing Submission

When purchasing the Services or registering for an event, GPM may also require you to provide the Company with financial qualification and billing information, such as billing name and address, credit card number, and the number of employees within the organization that will be using the Services (“Billing Information”). GPM may also ask you to provide additional information, such as company annual revenues, number of employees, or industry (“Optional Information”).

3. **Purpose**

GEHRIMED is a cloud-based Software-as-a-Service (SaaS) platform designed to help long-term, post-acute care providers manage both clinical and financial aspects of residents and patients in their care and to connect GEHRIMED customers with a variety of related healthcare networks and service providers. We promise to collect Personal Information only as necessary to communicate with you and/or to provide the Services.

CareTeamTM is the only collaboration platform that connects Long-Term Care/Post-Acute Care (LTPAC) practitioners with Senior Care Facilities by enabling real-time information exchange. CareTeam provides better patient population insights for Nurses, MDS Coordinators, and Medical Directors through episodic documentation, MDS analysis and reporting:

- Immediately view the physician's encounters
- Quickly review and audit ICD-10 diagnosis codes to increase billing accuracy
- Communicate with mobile practitioners via CareNote™, a HIPAA-compliant messaging solution
- Establish visit priorities for new and high-risk patients
- View CareInsights: Rehospitalization Rates, Frailty Indices, Patients at Risk, Medicare vs. Medicaid Patient View

Personal Information and non-personal information may be used for the following reasons:

- to register customer accounts
- to contact customers to discuss their experience with the Services, current and future needs as a customer, or to communicate future promotions or special events which might benefit them
- to contact a prospective customer
- to provide our cloud-hosted SaaS Services
- to operate, maintain, manage and administer the Services, including processing registrations and payments, and diagnosing technical problems
- to respond to questions and communications
- to make service or administrative announcements to customers about unscheduled downtime or new features, services, products, functionality, terms, or other aspects of the Services
- to perform audits, research, measurements and analyses in an effort to maintain, administer, support, enhance and protect the Services, including determining usage trends and patterns and measuring the effectiveness of content, advertising, features or services
- to create new features, products or services
- to contribute to certain health and medical research
- to provide benchmarking and performance tracking solutions

We may track and analyze non-identifying, aggregate usage, and volume statistical information from our visitors and customers and may provide such

information to third parties. We are committed to ensuring privacy and protecting Personal Information. We also are committed to providing valuable insights and analytics to enable better performance and quality.

We use cookies to enhance the quality of the Services by, for example:

- saving user preferences
- preserving session settings and activities
- providing limited auto-fill functionality for those who use the Services frequently
- analyzing various features and content of the Services

GPM uses a persistent cookie to help save and retrieve org codes for a user who has accessed the Services. We issue a session cookie only to record encrypted authentication information for the duration of a specific session. The session cookie does not include the username or password of a customer. For user convenience, in relation to touchscreen logins, we also use a non-session-based cookie to store a user's ID; however, this is configurable. We do not store passwords in session cookies, persistent cookies or headers. If a cookie is rejected, access to and usage of the Services will be denied.

Support, Education Services and Purchase Orders

Personal Information collected through the Sites may be accessed and used by GPM to respond to customer requests for support, to provide education or consulting services and/or to confirm customer compliance with the terms of its purchase (as set forth in signed orders). This may include testing and applying new product or system versions, patches, updates and upgrades; monitoring and testing system usage and performance; and resolving bugs and other issues which a customer reports to GPM. Personal Information collected for these purposes is only used for time periods relevant to fulfill such purposes.

Provider Directories and Communication Services

As a customer of GPM, and depending on the Services you subscribe to or enroll in, your contact and directory information may be listed in one or more public or professional directories. These directories may include profile information such as contact information or name.
We also offer services that facilitate communications, including secure and encrypted transmission of data between users and non-users through in-product instant messaging services, service-branded emails, short message

service (“SMS”) and other electronic communication channels. The identity of the sender and the receiver always will be evident with every communication transmitted via the Services. The information you choose to share with such parties is not the responsibility of GPM. We cannot take responsibility for the actions of other users or persons with whom you share information, including Personal Information.

GPM Events, Community Forums and Surveys

Many GPM customers share their experiences of the Services, either at our GPM Events or online via customer-driven Community Forums. During our GPM Events, we may solicit testimonies of the Services or your relationship with GPM, either as a customer or business partner. We will never use any such testimony, or video or audio footage, in conjunction with information that identifies you (or the organization you represent) without your express consent. Community Forums are public and allow customers to communicate between each other and, possibly, with the general public. Any information posted within Community Forums is public and we recommend against any disclosure of Personal Information or other sensitive information that could be traced, directly or indirectly, to an individual.
From time to time, we may ask customers to complete surveys or ratings about the provision of the Services or of their own health care practices and operations. You should assume that the content of any Personal Information you provide would not be maintained in confidence. We will, however, tell you why we are collecting your responses and how they will be used. In completing such surveys, be mindful of what Personal Information is disclosed. We recommend against sharing any PI, PHI or other sensitive information that could be traced, directly or indirectly, to any individual.

4. **Consent and Authorization**

By visiting the Sites, you are consenting to the use of your Personal Information for the aforementioned purposes. On occasion, we may request additional consent in connection with the use or sharing of Personal Information for a purpose not stated in this Policy or because the law requires such consent.
If you are a customer or business partner of GPM, we will never use your Personal Information in a manner not otherwise provided for in our written contracts with you, authorization forms you provide to us, or this Policy.

5. **Protecting Health Information**

As a provider of hosted, electronic health record solutions, GPM customers are health care providers and subject to laws and regulations governing the use and disclosure of PHI. In the United States, the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”), the Health Information Technology for Economic and Clinical Health of 2009 (“HITECH”), along with the regulations adopted under those statutes, and similar state laws (where those laws are more stringent than HIPAA) govern the handling of PHI. Health care providers are considered to be Covered Entities under HIPAA and are subject to its rules regarding PHI. If a provider delegates some of its work to a third party, and that party must access PHI in order to perform the work, then such party is considered by HIPAA to be a Business Associate and is subject to the same rules regarding the protection of PHI as the Covered Entity. To enforce protection, HIPAA requires Covered Entities to execute a “Business Associate Agreement” or ”BAA” with each of its Business Associates. Our customers are required to sign a BAA with us. As a Business Associate, we are required to use reasonable and appropriate measures to safeguard the confidentiality, integrity and accessibility of PHI that is stored and processed on behalf of Covered Entities. From time to time, the terms of GPM’s standard BAA may be posted on the Sites.

6. **Sharing Your Personal Information**

Third-Party Websites, Software and Services

Our Sites contain links to third-party websites, software and services. Customers and visitors who access a linked website via the Sites may be disclosing Personal Information. It is the responsibility of the user to keep Personal Information private and confidential. Additionally, we allow third-parties to offer services to our customers through integration with the our platforms (“3rdParty Services”). Customers’ use of 3rd Party Services are optional. Customers that choose to use a 3rd Party Service acknowledge and authorize the transmission of Personal Information to a third party. We are not responsible for, nor can we control, the privacy practices of third parties. A third party’s use, storage and sharing of your Personal Information is subject to its own privacy policies and not this Policy.

Business Reorganizations or New Management

There are two situations where we will need to share your Personal Information with a third party as a result of a business reorganization. The first situation concerns the acquisition of GPM by a third party, and the second concerns the acquisition of our customers. A reorganization involves a sale,

merger, transfer, exchange or other disposition of all or part of a business. If such a transaction occurs, be aware that your Personal Information may be made available to the acquiring party. If the reorganization concerns one of our customers, GPM requires the parties participating in the sale to show written evidence of the completed transaction, or some alternate form of written authorization (by both the buyer and the seller), to transfer Personal Information hosted by the Sites from the seller to the buyer. A change in management of a customer facility could involve similar authorization requirements, if data must be transferred from the prior management company to the new management company (or to the owner). We will not disclose your Personal Information to a party without sufficient and proper authorization from you, unless required by law.

Legal Procedures

We may need to preserve, use or disclose your Personal Information in response to a court order, subpoena, search warrant, judicial proceeding or other legal process, if we have a good faith belief that the law requires us to do so. Some legal procedures may prohibit or prevent us from notifying users, other individuals or entities identified in such procedure or may compel us to take measures otherwise in violation of this Policy or a written agreement you have with us. Personal Information preserved as a result of legal procedures can be maintained for an indefinite period of time and for as long as we have a good faith belief that it is necessary and appropriate under the circumstances. These procedures may even involve your information if your contractual relationship with us has been terminated or disabled.

7. **Security, Threats and Breach Notification**

Our Services have physical, administrative and technical security measures in place to protect against the loss, misuse, unauthorized access and alteration of data and Personal Information under our direct control. When the Services are accessed using current browser technology, Secure Socket Layer (“SSL”) technology protects information using both server authentication and data encryption to help ensure that data is safe, secure, and available only to you. GPM also implements an advanced security methodology based on dynamic data and encoded session identifications, and hosts the Services in a secure server environment which uses a firewall and other advanced technology to prevent interference or access from outside intruders. Unique user names and passwords also are required and must be entered each time a customer logs into the Services. We are committed to educating our staff about the protection of Personal Information, and the importance of compliance with

relevant privacy legislation and company policies. Employees and contractors are required to sign confidentiality agreements.

These safeguards help prevent unauthorized access, maintain data accuracy, and ensure the appropriate use of Personal Information; however, it is important to remember that no system can guarantee 100% security at all times. In the event that we detect a threat to security or a security vulnerability, we may attempt to contact you to recommend protective measures. Additionally, incidents of suspected or actual unauthorized handling of Personal Information are always directed to GPM's Legal and Compliance team, which is responsible for determining escalation and response procedures, depending on the severity and nature of the incident. Incidents involving unauthorized handling of PHI will be governed by relevant legislation and, where applicable, the provisions of a BAA or IMA with a customer. If GPM determines that Personal Information has been misappropriated or otherwise wrongly acquired, GPM will report such misappropriation or acquisition to you promptly.

For customers who purchase Connected Services, it is important to note that the third-party vendors that provide Connected Services to you may have different procedures in place to protect your Personal Information than the standards GPM has implemented. We cannot be responsible for their policies or their compliance with them, regardless of whether we have integrated their solutions with our Services and/or made them available to you.

8. **Openness, Transparency and Access to Personal Information**

Upon written request by an authorized individual, GPM will allow access to any Personal Information collected and stored about such individual, unless providing access could reasonably be expected to interfere with the administration or enforcement of the law or it is impracticable or impossible for GPM to retrieve the Personal Information. When provided with reliable evidence of an error, GPM will correct any inaccurate Personal Information, unless to do so would interfere with the administration or enforcement of the law. Unless otherwise prohibited or restricted by you, GPM may transmit any corrected Personal Information to third parties that have had access to the erroneous Personal Information. Please note that any deletions performed by GPM will only be "soft" deletes (i.e., the data will no longer be viewable from the front end of the platform). In order to be able to address any concerns about fraud which may be raised in the future by, for example, a resident or a government agency, we will retain evidence of: (i) the deletion; (ii) your authorization to make the deletion; and, (iii) the prior version of the data.

If customers need to update or change their Personal Information stored by us, they may do so by editing the user or organization record via the Sites.

9. **Retention and Deletion**

GPM will retain Personal Information: as necessary for the purposes outlined in this Policy; for as long as a customer account remains active; as required to manage and administer the Services; as required to carry out legal responsibilities (e.g., legal holds and other legal procedures); to resolve a dispute (including enforcement of a contract); or, as communicated to you at the time of collection. After all applicable retention periods have expired, we will delete or destroy your Personal Information in a manner designed to ensure that it cannot be reconstructed or read. If, at any time, it is not feasible for us to delete or destroy your Personal Information, we will continue using the same safeguards of protection and security outlined in this Policy and related subordinate policies, for as long as it cannot be destroyed.

10. **Cross-Border Transfers**

Unless otherwise specified, GPM provides the Services from its headquarters in Asheville, North Carolina and hosts customer data in the customer's country of residence.

11. **Opt-Out Policy**

We offer visitors to the Sites and our customers a means to choose how we may use the information they provide to us. If, at any time, you change your mind about:

1.
    1. our use of Personal Information submitted to the Sites;
    2. our use of Personal Information submitted via the Services;
    3. receiving notices from us (including automatic notifications about updates to the Services and the frequency with which we send you such messages); or
    4. sharing your non-personal information with third parties (as described in this Policy),

send us a request specifying your choice or change of permission by contacting us. Please note that, if you choose to impose certain restrictions on our use of your Personal Information – e.g., if we may no longer access your database to perform any necessary quality testing or disaster recovery testing

– you may no longer be able to use the Services. If complying with your request would result in termination of the Services, we will make that clear to you and confirm that this is what you want before proceeding.

12. Contact Us

If you believe your Personal Information has been used in a way that is inconsistent with this Policy or your specified preferences, or if you have further questions related to our privacy practices, please contact us at (828) 348-2888.

13. Do-Not-Track Signals

Our website includes third-party applications that track visitors. These applications respond to Do-Not-Track (“DNT”) requests by not dropping cookies into visitors’ browsers.