Otegrity, Inc. Privacy Policy

In this age of the Internet where privacy has become an increasing concern, we take your privacy very seriously. The privacy and security of your personal data (the "Personal Information") which we collect from you is important to us. It is equally important that you understand how we handle this data.

By entering into an agreement with or providing Personal Information to Otegrity, you expressly acknowledge that you have read, understand and agree to all of the terms of this Privacy Policy as outlined below and as it may be modified by us from time to time with or without prior notice.

Collection of Information

In the course of conducting our business and complying with federal, state, and local government regulations governing such matters as employment, tax, insurance, etc., we must collect Personal Information from you. The nature of the Information collected varies somewhat for each employee, depending on your employment responsibilities, your citizenship, the location of the facility where you work, and other factors. We collect Personal Information from you solely for business purposes, including those related directly to your agreement with Otegrity, and those required by governmental agencies. Personal Information may also be used to contact you regarding promotions, marketing efforts, and any other matters relating to Otegrity's business development.

Data collected may include, without limitation, such things as:

- Your name
- User ID(s)
- Phone numbers
- Email address(es)
- Mailing addresses
- Banking and other financial data
- Government identification numbers, e.g., Social Security number, driver's license number
- Date of birth
- Gender, race, and ethnicity
- Health and disability data
- Family-related data, e.g., marital status,
- Personal and health -related data for you and your family
- Trade union data

Anyone who sends Personal Information to the Company by any means, e.g., mail, email, fax, expressly consents to the storage, destruction, processing, or disclosure of the data, as well as any other reasonable business-related use by the Company or any government agency of the unsolicited data.

The Company will not knowingly collect or use Personal Data in any manner not consistent with this Policy, as it may be amended from time to time, and applicable laws.

Because Personal Information collected by Otegrity or affiliated third-party providers is necessary for business purposes, you are required to provide it. Your refusal or failure to

provide the requested Personal Information may, therefore, disqualify you from receipt or enjoyment of certain benefits.

Use of the Information We Collect

The primary purposes for collection, storage and/or use of your Personal Information include, but are not limited to:

- **Human Resources Management.** We collect, store, analyze, and share (internally) Personal Information in order to attract, retain and motivate a highly qualified workforce. This includes recruiting, compensation planning, succession planning, reorganization needs, performance assessment, training, employee benefit administration, compliance with applicable legal requirements, and communication with employees and/or their representatives.
- **Safety and Security Management.** We use such Information as appropriate to ensure the safety and protection of our clients, their employees, assets, resources, and communities.
- **Communication and Identification.** We use your Personal Information to identify you and to communicate with you.

Disclosure of Data

Otegrity acts to protect your Personal Information and ensure that unauthorized individuals do not have access to your Information by using security measures to protect Personal Information. We will not knowingly disclose, sell or otherwise distribute your Personal Information to any third party without your knowledge and, where appropriate, your express written permission, except under the following circumstances.

- **Legal requests and investigations.** We may disclose your Personal Information when such disclosure is reasonably necessary (i) to prevent fraud; (ii) to comply with any applicable statute, law, rule or regulation; or (iii) to comply with a court order.
- **Third-party vendors and service providers.** We may, from time to time, outsource services, functions, or operations of our business to third -party service providers. When engaging in such outsourcing, it may be necessary for us to disclose your Personal Information to those service providers, e.g., a benefits provider. In some cases, the service providers may collect Personal Information directly from you on our behalf. We will work with any such providers to restrict how the providers may access, use and disclose your Information.

  When using a third party provider to whom we must furnish your Personal Information, we will select reliable third parties and we will require them to enter into written agreements with the Company which will (i) specify the rights and obligations of each party; (ii) provide that the third party has adequate security measures in place to protect the Personal Information; and (iii) the provider will only process Personal Information on the specific written instructions of the Company.

- **Business Transfers**: During the term of your agreement we may buy other companies, create new subsidiaries or business units or sell part or all of Otegrity or its assets. It is likely that some or all of your Personal Information will be transferred to another company as part of any such the transaction. However, your Personal Information will remain subject to protection outlined in the then current Privacy Policy.
- **Protection of Otegrity and Others.** We may release Personal Information when we believe release is necessary to comply with the law; enforce or apply our policies and other agreements; or protect the rights, property, or safety of Otegrity, our employees, our clients or others. This disclosure will never, however, include selling, renting, sharing or otherwise disclosing your Personal Information for commercial purposes in violation of the commitments set forth in this Privacy Policy.

Security of Your Personal Information

We employ reasonable security measures and technologies, such as password protection, encryption, physical locks, etc., to protect the confidentiality of your Personal Information Only authorized employees have access to Personal Information.

Otegrity will make reasonable efforts to secure Personal Information stored or transmitted electronically secure from hackers or other persons who are not authorized to access such Information.

Compliance with this Privacy Policy is important to Otegrity. Any violation or potential violation of this Policy should be reported to info@otegrity.com. The failure by any employee to follow these privacy policies may result in discipline up to and including discharge of the employee. Any questions or suggestions regarding this policy may also be directed to info@otegrity.com.

HIPAA Policy and Procedures

Purpose for Policy

Otegrity, Inc. places a high value on the privacy of its clients ("Clients") and the expectation that information regarding Clients remains confidential and is made available only to persons who have a legitimate right to know. In addition, Otegrity, Inc. is contractually obligated to comply with the privacy and security provisions of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). Otegrity, Inc. recognizes that all employees and temporary workers ("Employees"), as well as outside contractors, have an ethical and legal obligation to keep certain information about Clients confidential and to protect and safeguard this information against unauthorized use or disclosure.

Overview

This privacy policy concerns protected health information ("PHI"). PHI, as defined by federal law, means any individually identifiable health information of a Client, including, but not limited to: social security number, name, address, birth date, age, telephone number, subscriber number, policy number, e-mail address, fax number, medical records and genetic information. PHI is not confined to written materials, facsimiles or hard copy. It also includes information derived from any source, including, but not limited to: e-mail, computer data, data stored on electronic media, disks or handheld computing devices (such as smartphones), verbal communications or recordings and visual observation.

Procedures

The following section outlines the basic procedures necessary to comply with this policy.

Disclosure of Information

- An Employee may access, discuss, use and disclose PHI only for Otegrity, Inc. business as it relates to that employee's specific job functions and/or responsibilities.
- Employees may disclose PHI only to those who have a legitimate, Otegrity, Inc.-related business need to know or who have prior written authorization. PHI about a Client may only be shared for purposes of claims payment or healthcare operations.
- PHI must never be the subject of casual conversation either inside or outside of the workplace. PHI must not be discussed in lobbies, stairwells, elevators, restrooms, hallways, or any other public area where conversation could be easily overheard by visitors and Employees who do not have a need to know.
- Only "Minimally Necessary" PHI may be disclosed. "Minimally Necessary" means only that amount of PHI necessary to accomplish the intended purpose of the use or disclosure.

Access to Information

- PHI may only be accessed if related to specific job functions and responsibilities.
- Casual reading of PHI is not permitted.
- Employees with legitimate access to PHI will protect this information from casual or unauthorized access.

Security of PHI

- Employees may remove PHI from the facility only as it relates to specific job functions and/or responsibilities. Approval from an employee's direct manager is necessary to remove PHI from the facility. It is the responsibility of each Employee to protect and safeguard all such information.
- Employees are encouraged to review PHI in a secure area and are responsible for records that are checked out to them. It is the responsibility of the Employee to protect and safeguard all records that are removed from the secure areas.
- Technical security safeguards are used to store, process and transmit electronic PHI. Our IT staff has primary responsibility for the security oversight of electronic PHI. Employees are responsible for complying with these security safeguards. All workstations that store, process or otherwise access electronic PHI must be protected with a strong password. Open sessions will be disconnected after a period of inactivity.

Breach of Confidentiality

- Any Employee who believes he/she has observed a breach of security or confidentiality should promptly notify his or her direct manager or the Chief Privacy Officer.
- Employees found to be in violation of this policy may be subject to disciplinary action, up to, and including termination and/or legal action. PHI is protected by federal and state laws and regulations that define civil and criminal penalties for violations of confidentiality.
- Otegrity, Inc. will periodically conduct unscheduled audits to ensure compliance with this policy.

Safeguarding PHI

- In order to maintain confidentiality, any item containing PHI must be discarded according to the standards identified below:

Item	Examples	Where/How Discarded
Paper	Medical records, applications, census files, or any other paper-based document containing PHI	Paper-based PHI should be placed in a sealed recycle bin for destruction or destroyed by shredding. Electronic copies stored in the Otegrity, Inc. Document Management System will be password protected using encryption procedures.
Electronic	Computer hard drives, disks, e-mails and electronic files	The IT staff will remove the hard drive from each computer or laptop that is scheduled for disposal. These hard drives will be physically secured until they are destroyed or recycled. Computers that will be reused must cleared or purged to remove PHI. Disks should be destroyed or re-formatted. E-mails and electronic files should be purged from the system after use. Employees needing

		assistance in disposing of electronic files should contact a member of our IT staff.

- Employees must not leave any PHI on fax machines, printers or copiers.
- Employees are to clean their workspace of PHI at the end of their work day and place the PHI in a secure location.
- Employees must exercise caution and discretion when leaving voicemail messages containing PHI.
- Employees are to escort visitors through work areas.
- Employees must exercise caution and discretion when e-mailing PHI internally within Otegrity, Inc..
- Employees must use appropriate encryption software when e-mailing PHI outside of Otegrity, Inc..
- Employees must not store PHI on handheld devices, such as smartphones.
- Employees must secure all hardcopy mail containing PHI.
- Employee workstations will be programmed to auto-lock after 10 minutes of inactivity.
- Employees should refrain from loading PHI on pooled laptops. Information stored on laptops will be routinely purged.