HRGi Holdings, Inc. Privacy Policy

BACKGROUND

The privacy and protection of information is important to our organization. This Privacy Policy outlines HRGi Holdings, Inc. (HRGi) general policy and practices for implementing Privacy Principles, including the information gathered, how the information will be used, the choice affected individuals have regarding the use of that information, and the ability of affected individuals to correct that information. This Privacy Policy applies to all Personally Identifiable Information (PII) and Protected Health Information (PHI) received, whether in electronic, paper, or verbal format.

All data handling activities conducted by HRGi are intended to be consistent with all applicable legal requirements in the jurisdictions where HRGi does business. This includes, but is not limited to, compliance with federal Health Insurance Portability and Accountability Act (HIPAA) and state privacy laws.

PURPOSE

The purpose of these standards is to protect the privacy of all personal and protected information owned, received, created, maintained, transmitted or used by HRGi and its Business Associates.

POLICY

All HRGi employees must complete training on HRGi's privacy and confidentiality policies, participate in other privacy education required by HRGi, including security and awareness training, and demonstrate adherence to policy standards while completing business operations. The Privacy Policy includes the standards listed below and all documented procedures provided for existing and future business processes. All employees of HRGi will be held to these standards. A paper copy of the Privacy Policy is available upon written request made to: Privacy Officer, HRGi Holdings, Inc., 9711 Washingtonian Blvd., Suite 300, Gaithersburg, MD 20878.

Definitions

1. *"Personal Information"* refers to all information owned, received, created, maintained, and transmitted by HRGi that may be deemed by a regulatory organization to be *Personally Identifiable Information (PII)* or *Protected Health Information* (PHI), defined as follows:

    - Personally Identifiable Information (PII) refers to any information that can be used to uniquely identify, contact, or locate a single person or can be used with other sources to uniquely identify a single individual. Pll includes, but is not limited to, the following:

        - Name

- Address
- Phone/Fax Number
- E-mail Address
- Social Security Number
- Employment Data
- Credit Card Information
- May include medical and health information, as defined by each state

PII does not include information that is collected anonymously or demographic information not connected to an identified individual.

- Personal Health Information (PHI) is information (1) that HRGi creates, receives, maintains or transmits that relates to the past, present or future: (a) physical or mental condition of an individual; (b) provision of health care to an individual; or (c) payment for the provision of health care for the individual, including incentive qualification; and (2) that identifies or can be reasonably used to identify an individual. PHI includes, but is not limited to, the following:

  - Personally Identifiable Information
  - Biometric Data
  - Address (postal and e-mail)
  - Date of Service
  - Date of Birth
  - Diagnosis
  - Effective Date
  - Family History
  - Name
  - Privacy ID
  - Service Provider
  - Termination Date
  - Social Security Number

2. A "Business Associate" is a person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity.

3. Staff includes HRGi employees, whether in an office or home-based.

Standards

1. **Compliance with the Law.** HRGi complies with all laws regulating the use and disclosure of Personal Information in each of the jurisdictions where it does business.

2. **Confidentiality Acknowledgement.** All employees must acknowledge their responsibilities for the safeguard and protection of Personal Information by signing a confidentiality acknowledgement at the time of employment.

3. **Use and Release of Information.** Access to Personal Information is restricted to the minimum necessary information needed for employees to perform their job duties. The Privacy Officer conducts regular reviews of the Personal Information used to ensure only the minimum necessary information is disclosed.

4. **Protecting Personal Information.** HRGi is committed to protecting the Personal Information of all customers, employees, and employees' dependents. Employees may not use or disclose Personal Information, except as permitted or required by applicable law and in accordance with the provisions of any applicable Business Associate Agreements.

   Employees in a HRGi Office. Office-based staff must restrict inappropriate viewing of Personal Information stored and accessed at their workstations. Paper PHI should be locked up when leaving workstations and all systems should be locked up when employees are away. Employees in an open or public area will be provided a privacy screen by the Privacy Officer. If an employee has not been provided a privacy screen and believes it is needed, a request may be made to the Privacy Officer.

   Home-based Staff. Home-based staff must ensure that their workspace is private. This includes ensuring that phone conversations that include Personal Information are not overheard by friends and family, printing Personal Information only when necessary, and keeping Personal Information locked up when not in use. Employees may not download and/or store Personal Information on non-HRGi devices.

5. **Breach of Information.** Employees are required to promptly report any improper uses or disclosures of Personal Information to the Privacy Officer via e-mail at privacy@hrgi.com. HRGi follows all applicable laws related to breach notification and mitigation.

6. **Lost or Stolen Equipment.** All occurrences of lost or stolen equipment must be immediately reported to HRGi management. If Personal Information is stored on the lost equipment, the event must also be immediately reported to the Privacy Officer via e-mail at privacy@hrgi.com.

7. **Secured Physical and Electronic Personal Information.** Personal information possessed by HRGi is appropriately secured through restricted access to business areas and placement in locked storage when not in use.

   Electronic Personal information is encrypted while in transit through publicly-accessible networks. Information Security Officers review encryption processes of systems that move information. Standards for encryption are included in HRGi's Security Policy. Personal

Information is encrypted when copied to a CD, jump drive, etc. and sent or carried outside the Company. Additionally, a security review is performed on data at rest and encryption is applied, as needed. This includes Personal Information stored on laptops and other mobile devices.

Personal information sent through the Postal Service should be scrubbed to remove any Personal Information other than the minimum required. First Class mail is not traceable and should only be used for mailings that include less than 50 individual's Personal Information. Certified mail should be used to send large volumes of Personal Information (over 50 individuals).

To the extent possible, employees should not remove or transport Personal Information outside of their workspace or home office. If a business reason exists to transport Personal Information, employees must ensure all electronic Personal Information is encrypted and paper PHI is appropriately secured while in transit and locked up when not in use.

8. **Use of Non-HRGi Devices.** Staff may use non-HRGi equipment to access e-mail. All mobile devices accessing e-mail should be password protected. E-mail will be remotely wiped by HRGi if a personal device is lost or stolen or if staff leave the organization. Web-based applications may be used from non-HRGi devices only when an encrypted connection, such as SSL, is established. Personal Information accessed on non-HRGi devices may not be downloaded or stored.

9. **Personal Information Received from Customers.** HRGi advises customers not to send Personal Information to HRGi via e-mail unless encrypted. HRGi encourages its customers to send any necessary Personal Information to HRGi through the U.S. Postal Service, by secure fax, via telephone (speaking directly to HRGi representatives), or by using a secure ftp connection.

10. **Use of Social Security Numbers (SSN).** HRGi believes in the importance of appropriately safeguarding Social Security Numbers obtained during the normal course of conducting business. To the extent possible, an alternate ID, such as an employer identification number or a HRGi-generated privacy identification number will be used for individual identification. However, if business needs require the use of a SSN, it is HRGi's practice not to disclose SSNs (all or part) unless a compelling business need is identified or if legally required. Access to SSNs is limited to staff with a business need to know SSNs.

    a. **Third Parties.** In order to ensure the security of SSNs if a business need requires the disclosure of the full SSN to a third party, notification must be submitted in writing to the Privacy Officer privacy@hrgi.com. The Privacy Officer approves all requests prior to sharing any SSNs with a third party.

    b. **Printed Materials.** Any information or documents which are mailed or faxed to clients, customers, or other individuals should not include SSNs. Exceptions are allowed only when a state or federal law requires SSNs to be in the document. If the law requires inclusion of a SSN, it must not be viewable through the window of an envelope.

c. **E-mail.** Messages and any attachments sent via e-mail must not contain SSNs. A business exception may be made with Privacy Officer approval for internal e-mails if necessary to transact business.

11. **Digital Certificates.** Digital certificates may only be obtained from certified authorities licensed to meet international privacy and electronic commerce requirements. Online transactions must be reviewed and secured through certificate validation where appropriate. Examples of how digital certificates are used at the Company include ensuring web pages are not changed without correct authorization, as well as providing encryption capabilities.

12. **Data Retention.** Records containing Personal Information are retained for 10 years from the termination of the client under which the information was gathered.

13. **Shredding and Disposal.** Once retention requirements are met, all Personal Information (in paper form} is shredded. Personal Information on diskettes, tapes, CDs, etc. is erased per NIST *Guidelines for Media Sanitation* if the device will be reused or destroyed in accordance with Information Security policies.

14. **Recording of Telephone Conversations.** Recording of telephone conversations may only be done with notice to or consent of all parties. Parties to non-business calls on recorded lines must also be notified of the recording. Recording features may only be added with Privacy Officer approval.

15. **Taking Photos and Use of Audio Recording Devices.** Employees are prohibited from using audio recording devices, taking photos of, or video recording images that put privacy at risk.

16. **Leaving Information on Answering Machines.** Messages left by employees should include the employee's first name, company name, and phone number (including extension, if applicable). Personal Information should not be left on an answering machine.

17. **Texting.** Personal Information should never be texted to a mobile device.

18. **User IDs and Passwords**. Passwords for user IDs are encrypted in storage. No one may ask to obtain or change a user ID or password other than the person associated with the user ID and password. Users will be required to positively identify themselves prior to password changes.

19. **Faxing Information.** Faxes require the party's consent or an established business relationship. Any time documents are faxed, only the minimum amount of Personal Information should be included. Social Security Numbers may not be sent via fax.

20. **Marketing Restrictions.** Sharing PHI with affiliated companies and non-affiliated third parties for marketing purposes requires the individual's consent. Additionally, the use of Personal Information (other than PHI) by another affiliated company for marketing purposes is restricted by various laws and must meet certain guidelines. Contact Marketing or the

Privacy Officer at privacy@hrgi.com for additional information or usage review.

21. **Credit and Debit (Payment) Card Data**. The acceptance of credit, debit, or purchasing card data for payment of services must be approved by the Controller and Privacy Officer. Usage must be in compliance with Payment Card Industry (PCI) Data Security Standards.

22. **Privacy Training.** All employees are required to complete a privacy training course upon hire and at least annually thereafter and in accordance with changes in law.

23. **Privacy Officer Duties.** HRGi's Privacy Officer is responsible for:
    a. Ensuring HRGi compliance with federal and state privacy laws.
    b. Creating a risk assessment (reviewed as needed) of business processes, systems, and users to identify potential exposure or misuse of Personal Information.
    c. Identifying and documenting the minimum required Personal Information needed to complete business processes and provide customer service.
    d. Creating a written procedure for identifying and handling inappropriate uses and disclosure of Personal Information; reviewing all breaches of Personal Information; providing notice of breaches of unsecured PHI to the impacted individuals and the Department of Health and Human Services or state agencies, as required by law; and managing any efforts to mitigate breaches to the extent practicable.
    e. Participating in any federal or state audit conducted in relationship to personal information.
    f. Facilitating the creation and maintenance of policies and procedures required by federal and state law to protect Personal Information.

Enforcement

HRGi uses a self-assessment approach to ensure compliance with this Privacy Policy and verifies periodically that the Policy is accurate and comprehensive for the information intended to be covered. The Policy shall be prominently displayed, completely implemented, and accessible to individuals required to comply with the policies and standards included.

Management is responsible for ensuring that their direct reports understand the scope and implications of the Policy. Human Resources must also ensure that all employees have acknowledged this policy and keep a copy of their acknowledgement in the employee's file.

Failure to adhere to the requirements of the Privacy Policy is cause for disciplinary action up to and including termination, as determined by HRGi Management, using guidelines defined by the Human Resources Department.