PRIVACY POLICIES AND PROCEDURES

Revision History

Company's Privacy Policies and Procedures were adopted as of **8/1/19** by JorgensenHR's Board of Directors

Company's Privacy Policies and Procedures were modified as of [Date]. _____

Table of Contents

COMPANY RESPONSIBILITIES

I. JorgensenHR

JorgensenHR may be referred to as "JHR" or "Company".

The HIPAA Privacy Rules impose certain requirements on entities that create, receive, use or disclose Protected Health Information on behalf of their Covered Entity clients, individuals or Business Associate partners.

II. Document Control

A. Overview

JHR has created policies and procedures with respect to Protected Health Information that are designed to comply with the standards, implementation and specifications under §164.530(i)(1). The Company will change its policies and procedures as necessary and appropriate to comply with changes in the law, including the standards, requirements, and implementation specifications of §164.530(i)(2)(i).

A copy of this document is available with the Privacy Officer (PO), Barry Cohn, barry@jorgensenhr.com, 661-600-2070.

B. Security Document Library

These policies and procedures and related privacy practice information will be kept in our Security Documentation Library. The Library is located on our server on our P drive that is accessible to Renee Cohn, Barry Cohn and Ronni Kopulsky.

Documentation about privacy practices (logs of activities, etc.) will be kept in this Library or in a short file in the Library that will describe where the privacy practice documentation resides. The intended result is that anyone with access to the Security Documentation Library will be able to locate any piece of documentation associated with our privacy program.

Outdated and superseded materials from the Security Documentation Library will be kept in an archive (the Security Documentation Archive) for at least seven (7) years after the date when they are first outdated or superseded.

III. Management and Protection of Protected Client Data

A. Overview

The Privacy Rules place certain restrictions on the acquisition, use and disclosure of Protected Health Information (PHI). Further, under the rules and agreements signed by JHR with the Health Insurance Marketplaces, or Exchanges and in accordance with federal

regulations, the Company must also protect Personally-Identifiable Information (PII) that we may receive, use, transmit or store about any client or prospect who may purchase health insurance coverage through the Health Insurance Marketplaces, or Exchanges whether federally-facilitated, in a state partnership or state-operated. Collectively, we will refer to PHI and PII as "Protected Client Data." This definition applies to the information that falls within either definition.

These policies establish the minimum care with which Protected Client Data in the custody of JHR's personnel must be accorded.

B. Purpose

The purpose of this document is to provide basic instruction to all of JHR's employees regarding the management and protection of Protected Client Data.

C. Applicability

This policy applies to all JHR workforce members who have access or potential access to PHI.

D. Definitions

Covered Entity*:* a health plan, a health care clearinghouse, or a health care provider that transmits any health information in electronic form relating to any covered transaction.

Hybrid Entity: a single legal entity that is a Covered Entity whose covered functions are not its primary functions.

Protected Health Information **(PHI):** individually identifiable information relating to the past, present or future physical or mental health or condition of an individual, provision of health care to an individual, or the past, present or future payment for health care provided to an individual.

Personally-Identifiable Information (PII): any information about an individual maintained by JHR**,** including:

1. Any information that can be used to distinguish or trace the identity of an individual, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and
2. Any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information

Protected Client Data: PHI and/or Personally-Identifiable Information which is used, disclosed, transmitted, or stored by JHR.

Designated Record Set: a group of records maintained by or for a Covered Entity, Business Associate or Business Associate subcontractor that is: the medical and billing

records relating to an individual maintained by or for a health care provider; the enrollment, payment, claims adjudication, and case or medical management systems maintained by or for a health plan, or; used, in whole or in part, by or for a Covered Entity to make decisions about individuals.

Treatment, Payment and Health Care Operations (TPO) includes all of the following:

1. *Treatment* means the provision, coordination, or management of health care and related services, consultation between providers relating to an individual, or referral of an individual to another provider for health care.
2. *Payment* means activities undertaken to obtain or provide reimbursement for health care, including determinations of eligibility or coverage, billing, collections activities, medical necessity determinations and utilization review.
3. *Health Care Operations* include functions such as quality assessment and improvement activities, reviewing competence or qualifications of health care professionals, conducting or arranging for medical review, legal services and auditing functions, business planning and development, and general business and administrative activities including the creation of de-identified health information as defined by these regulations.

Disclosure: the release, transfer, provision of access to, or divulging in any other manner of information outside the entity holding the information.

Use: with respect to Protected Client Data, the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information.

Personal Representative: a person who has authority under applicable law to make decisions related to health care on behalf of an adult or an emancipated minor, or the parent, guardian, or other person who is authorized under law to make health care decisions on behalf of an un-emancipated minor.

Employees: all employees of JHR as well as its temporary employees, interns, independent contractors, trainees, and other persons whose conduct, in the performance of work for the Company its offices, programs or facilities.

Privacy Rules: the rules adopted by various state and federal agencies to implement the requirements of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and regulations promulgated under this Act as well as those obligations that arise under the privacy and security standards adopted by the Health Insurance Marketplaces, pursuant to 45 CFR §155.260.

E. Policy

Generally: Protected Client Data shall not be obtained, used or disclosed except as permitted or required by law.

Permitted and Required Uses and Disclosures: Protected Client Data may or shall be disclosed as follows:

1. To the individual
2. To carry out TPO activities as allowed under HIPAA and/or pursuant to and in compliance with a current and valid Authorization
3. In keeping with a Business Associate Agreement
4. As otherwise allowed or required under the HIPAA Rules or other federal and/or state laws concerning privacy of information that is used by JHR in the course of its business operations.

Minimum Necessary: Generally, when obtaining, using or disclosing Protected Client Data, or when requesting Protected Client Data from another entity, reasonable efforts must be made to limit the Protected Client Data used or disclosed to the minimum necessary to accomplish the intended purpose. However, the Privacy Rules were not intended to severely complicate business processes and JHR may, where appropriate, use a single format to provide data containing Protected Client Data for our various services. See *Minimum Necessary Provision*.

Accounting for Disclosures: An individual has a right to an accounting of disclosures of his/her Protected Client Data for up to a seven-year period. Individual Rights to PHI—Accounting See

1. **Confidential Communications**: JHR must respect the individual's right to request confidential communication of their PHI by alternative means or at alternative locations. See *Confidential Communications.*
2. **Complaint Process**: JHR must put into place a process for individuals to make complaints about our Privacy policies and procedures and/or our compliance with those policies and procedures See *Complaint Process.*
3. **Documentation**: JHR must maintain written or electronic copies of all policies and procedures, communications, actions, activities or designations as are required to be documented under this manual for a period of seven (7) years from the later of the date of creation or the last effective date.

F. Enforcement

An employee found to have violated this policy shall be subject to disciplinary action, up to and including termination of employment. In the case where inappropriate access, use or disclosure of Protected Client Data was or may have been involved, such individuals may additionally be reported to the appropriate enforcement agencies.

IV. Administrative Requirements for HIPAA Implementation

A. Overview

The Privacy Rules require that a Business Associate have in place appropriate administrative safeguards to protect the privacy of Protected Client Data.

B. Purpose

To provide instructions regarding Company's obligations relating to the implementation of administrative requirements of the Privacy Rules.

C. Applicability

This policy applies to all JHR workforce members who have access or potential access to PHI.

D. Special Definitions

Privacy Notice: The Notice of Privacy Practices relating to an entity's use and disclosure of Protected Client Data that is mandated under Privacy Rules for distribution to all individuals whose information will be collected by or on behalf of the entity.

E. Policy

Personnel Designations: JHR shall designate and document designations of the following:

1. Privacy Officer: JHR shall designate an individual as the Privacy Officer, responsible for the development and implementation of Company-wide policies and procedures relating to the safeguarding of Protected Client Data.
2. Contact Person or Office: JHR shall designate an individual, position title, or office that will be responsible for receiving complaints relating to Protected Client Data and for providing information about the Company's privacy practices.
3. Persons with access to Protected Client Data will be listed by title and each department shall include a listing of individual's names with our Privacy Officer and update on a periodic basis retaining the previous listing for a period of not less than 7 years.

Training Requirements: JHR shall document the following training actions:

1. All JHR employees shall receive training on applicable policies and procedures relating to Protected Client Data as necessary and appropriate for such persons to carry out their functions within JHR.
2. Each new employee shall receive the training as described above within thirty (30) days after joining JHR.
3. Each employee whose functions are impacted by a material change in the policies and procedures relating to Protected Client Data, or by a change in position or job description, shall receive the training as described above within a reasonable time after the change becomes effective.

Safeguards: JHR shall have in place appropriate administrative, technical, and physical safeguards to reasonably safeguard Protected Client Data from intentional or unintentional unauthorized receipt, use or disclosure. (See Security Policies and Procedures)

Complaint Process: JHR shall have in place a process for individuals to make complaints about the Company's HIPAA policies and procedures and/or the Company's compliance with those policies and procedures, and shall document all complaints received and the disposition of each complaint.

Sanctions: JHR shall have in place, apply and document application of appropriate sanctions against employees who fail to comply with HIPAA policies and procedures.

Mitigation Efforts Required: JHR, to the extent practicable, shall mitigate any harmful effects of unauthorized uses or disclosures of Protected Client Data by the Company or any of its Subcontractors.

Prohibition on Intimidating or Retaliatory Acts: Neither JHR nor any employee shall intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual for the exercise of their rights or participation in any process relating to HIPAA compliance, or against any person for filing a complaint with the Secretary of the U.S. Department of Health and Human Services, participating in an investigation, compliance review, proceeding or hearing, or engaging in reasonable opposition to any act or practice that the person in good faith believes to be unlawful under the Privacy Rules as long as the action does not involve disclosure of Protected Client Data in violation of the regulations.

Policies and Procedures: JHR shall document the following actions relating to its policies and procedures:

1. Required Policies and Procedures: JHR shall design and implement policies and procedures to assure appropriate safeguarding of Protected Client Data in its operations.
2. Changes to Policies and Procedures: JHR shall change its policies and procedures as necessary and appropriate to conform to changes in law or regulation. JHR may also make changes to policies and procedures at other times as long as the policies and procedures are still in compliance with applicable law. Where necessary, JHR shall make correlative changes in its Privacy Notice.

F. Documentation Requirements

JHR must maintain the required policies and procedures in written or electronic form, and must maintain written or electronic copies of all communications, actions, activities or designations as are required to be documented hereunder, or otherwise under the Privacy Rules, for a period of at least seven (7) years from the later of the date of creation or the last effective date.

V. Designation of a Privacy Officer

A. Purpose

JHR is committed to ensuring the privacy and security of PHI. In order to manage the facilitation and implementation of activities related to the privacy and security of PHI, Company has appointed and will maintain an internal Privacy Officer position. The Privacy Officer will be trained on all policies and procedures necessary to fulfill his or her responsibilities in ensuring the security and privacy of PHI.

B. Policy

JHR has designated a Privacy Officer responsible for oversight of the policies and procedures regarding the privacy of health information.

C. Procedures

Our Privacy Officer (PO), Barry Cohn, has been trained regarding policies and procedures for the secure transmission and storage of individual health information, including:

1. Secure transmission and storage of individual health information in any form;
2. Control of access to individual health information;
3. Secure management of PHI;
4. Proper use and disclosure of PHI at the request of the individual;
5. Proper use and disclosure of PHI without the authorization of the individual;
6. Ensuring that any individual's authorization for the use or disclosure of PHI is protected as required;
7. Individual rights regarding PHI;
8. Developing and maintaining contracts with Business Associate Subcontractors regarding the use and disclosure of PHI;
9. Proper use of the Notice of Privacy Practices;
10. Incident and contingency plan procedures;
11. Auditing access to individual health information;
12. Maintenance of records regarding access to individual health information.
13. Training will be conducted within thirty days of a new Privacy Officer's employment with JHR.
14. Training will incorporate the specifications and implications of the Company's routine business activities.

VI. Maintaining Appropriate Documentation Regarding Compliance with HIPAA Privacy

A. Purpose

This policy is designed to give guidance and ensure compliance with provisions of HIPAA requiring covered entities to maintain documentation of policies, procedures, and other administrative documents in works and in accordance with the *Notice of Privacy Practices.*

B. Policy

JHR will implement policies and procedures with respect to PHI that are designed to comply with the standards, implementation specifications, or other requirements of the HIPAA Privacy regulations.

JHR will maintain documentation, in written or electronic from, of policies, procedures, communications, and other administrative documents as required by 45 CFR § 164.530(i) and (j) for a period of at least seven (7) years from the date of creation or the date when last in effect, whichever is later.

JHR will incorporate into its policies, procedures and other administrative documents any changes in law.

JHR will properly document and implement any changes to policies and procedures as necessary by changes in law.

C. Procedures

JHR's policies are designed to take into account the size and type of activities undertaken by Company with respect to PHI.

In implementing a change in the Notice of Privacy Practices, JHR will:

1. Ensure that the policy or procedure, as revised to reflect a change in JHR's privacy practice, complies with the standards, requirements, and implementation specifications of the Privacy regulations;
2. Document the policy or procedure as revised;
3. Revise the Notice to state the changes in practice and make the revised Notice available; and
4. Company will not implement a change in policy or procedure prior to the effective date of the revised Notice.

JHR may change policies or procedures that do not affect the content of the Notice of Privacy Practices, provided that the policy or procedure complies with the Privacy regulations and is documented as required in this policy.

The following documentation will be maintained in an organized manner:

1. Policies and procedures related to the use or disclosure of PHI;
2. Forms for the consent to use or disclose PHI;
3. For authorization to use or disclose PHI;
4. Requests for the use or disclosure of PHI;
5. Agreements with business associates referring to the use or disclosure of PHI; and
6. Notice of Privacy Practices and any changes made thereto.
7. Documentation will be maintained in a manner that allows necessary availability, while also ensuring the security of information.

VII. Minimum Necessary Provision

A. Overview

The Privacy Rules place certain restrictions on the receipt, use and disclosure of Protected Client Data in regards to the amount reasonably necessary to accomplish the task being performed. However, the Privacy Rules also allow Protected Client Data to be disclosed for business-appropriate needs.

The policies developed by JHR will follow this business-appropriate philosophy as well as that of administrative simplification, which is the subsection of the HIPAA law under which the Privacy Rule was developed. JHR shall use standard data formats for information acquisition or disclosure and tailor these formats to contain a business-reasonable minimum necessary amount of Protected Client Data. JHR's policies establish the Minimum Necessary Use provisions for Protected Client Data in the custody of Company employees.

B. Purpose

To issue instructions regarding JHR's obligations relating to the Privacy Rules to obtain, use and disclose only the minimum amount of Protected Client Data necessary to accomplish the intended purpose.

C. Applicability

This policy applies to all JHR workforce members who have access or potential access to PHI.

D. Policy

JHR will make reasonable efforts to ensure that the minimum necessary amount of Protected Client Data is disclosed, used, or requested to accomplish the intended purpose. Exceptions to the Minimum Necessary Requirement include disclosures:

1. To the individual who is the subject of the information.
2. Made pursuant to an authorization provided by the individual.
3. To healthcare providers for treatment purposes.
4. Required for compliance with the standardized HIPAA transactions.
5. Made to the Secretary of HHS or his/her agency pursuant to a privacy investigation.
6. Otherwise required by the Privacy Rules or other law.

Employees will be trained on the policy and procedures developed to apply these principles to the use or disclosure of, or requests for Protected Client Data.

E. Procedures

The following procedures will be implemented to ensure that this policy is enforced effectively across all of JHR:

1. Each user of a system which accesses Protected Client Data shall be identified and the classes or types of Protected Client Data to which access is needed and any conditions appropriate to such access will be established. It will be the responsibility of the Privacy Officer to maintain this information as outlined in the Access to Systems Containing Protected Client Data procedures in our Security Policies and Procedures.
2. Reasonable efforts will be taken to limit the access of each user of Protected Client Data to the amount needed to carry out the individual's duties. These efforts will include internal use of Protected Client Data.
3. For situations where Protected Client Data disclosure occurs on a routine and recurring basis, the Protected Client Data disclosed will be limited to the amount of information reasonably necessary to achieve the purpose of the disclosure.
4. Requests for disclosures that are not routine and recurring and thereby covered by JHR's standard procedures (other than to the individual, the Secretary of HHS or his agents or where required by law) shall be reviewed by the Privacy Officer to determine that the Minimum Necessary Provision is applied to the extent reasonable.
    a.

Questions regarding these procedures should be directed to our Privacy Officer.

F. Enforcement

Employees found to have violated this policy shall be subject to disciplinary action, up to and including termination of employment. In the case where inappropriate access, use or disclosure of Protected Client Data was or may have been involved, such individuals may additionally be reported to the appropriate enforcement agencies.

VIII. Disclosing and Requesting Only the Minimum Amount of PHI Necessary

A. Purpose

JHR is committed to ensuring the privacy and security of covered health information. To support the Company's commitment to confidentiality, JHR will ensure that the appropriate steps are taken to disclose only the minimum amount of PHI necessary to accomplish the particular use or disclosure, as required under 45 CFR §164.502(b), and other applicable federal, state, and/or local laws and regulations.

B. Policy

Agents and employees will follow proper procedures to ensure that only the minimum amount of covered health information necessary to accomplish the specific purpose of a use or disclosure is actually used or disclosed.

Agents and employees will request only the minimum amount of covered health information necessary to accomplish the specific purpose of the request.

This policy does not apply to the following uses or disclosures:

1. Disclosure to or requests by a provider for treatment;
2. Uses or disclosure made to the individual who is the subject of the information;
3. Uses or disclosure pursuant to an authorization;
4. Disclosure made to the Department of Health and Human Services;
5. Uses or disclosures required by law; and
6. Uses or disclosure required for compliance with applicable laws and regulations.

C. Procedures

All proposed uses or disclosures of covered health information will be reviewed by persons having an understanding of JHR's privacy policies, and sufficient expertise to understand and weigh the necessary factors.

The Company will only use, disclose, or request an entire record when the entire record is specifically justified as being reasonably necessary to accomplish the purpose of the use, disclosure, or request.

Within JHR, agents and employees require varying levels of access to PHI on a routine basis to appropriately accomplish their duties and responsibilities. Our Risk Assessment lists the access levels of those agents and employees that have access to PHI.

Access to PHI will be reasonably limited to that described in our Security Policies and Procedures by utilizing access control systems.

The following criteria will be used in limiting the amount of PHI requested, used, or disclosed:

1. Does the requesting individual have complete understanding of the purpose for the request, use, or disclosure of the PHI?
2. Are all of the individuals identified for whom the use or disclosure of the PHI is required?

Requests for disclosures of PHI will be reviewed on an individual basis in accordance with criteria listed in the policy.

Agents/employees may reasonably rely on requests by:

1. Public health and law enforcement agencies in determining the minimum necessary information for certain disclosures;
2. Other covered entities in determining the minimum necessary information for certain disclosures; or

3. By a professional who is a member of its workforce or is a business associate of JHR for the purpose of providing professional services to Company, if the professional represents that the information requested is the minimum necessary for the stated purpose.

D. Enforcement

Knowledge of a violation or potential violation of this policy must be reported directly to the Privacy Officer.

IX. Notice of Privacy Practices

A. Purpose

45 CFR §164.520 requires that notice be given to individuals of the use and disclosure of PHI as well as the individual's rights and covered entities' legal duties with respect to PHI. This policy is designed to give guidance and to ensure compliance with all laws and regulations regarding the provision of the notice of use of PHI by health plan providers. This policy is not applicable to inmates.

B. Policy

JHR will provide a formal notice to individuals regarding the use or disclosure of PHI pursuant to 45 CFR §164.520. This will be provided in a separate document entitled Notice of Privacy Practices.

The provision of the Notice given to individuals regarding the use and disclosure of PHI pursuant to 45 CFR §164.520 will comply with the policies and procedures described herein.

C. Procedures

The Notice will be provided to individuals with whom JHR has a direct relationship as follows:

1. No later than the date of the activation of health insurance coverage;
2. Upon request;
3. On or after the effective date of a revision;
4. Promptly available at the service delivery site for individuals to request and to take with them;
5. Posted in a clear and prominent location where it is reasonable to expect individuals seeking service from JHR to be able to read the Notice;
6. Automatically and concurrently for electronic notices, when the individual's first inclusion in health care coverage is delivered electronically. The individual who is the recipient of electronic Notice will be permitted to retain the right to obtain a paper copy of the Notice from the Company upon request.

JHR will prominently post its Notice on any websites that it maintains that provide information about its health care services or benefits, and will make the Notice available electronically through the website.

When providing the notice to an individual by email, JHR will:

1. Ensure that the individual has agreed to electronic Notice and such agreement has not been withdrawn; see Authorization to Receive Notice of Privacy Practices Electronically [NPP Folder].
2. Provide a paper copy of the Notice to the individual if JHR knows that an email transmission of the electronic Notice has failed, JHR will document compliance with and maintain the Notice, or joint Notice as applicable, by retaining copies of the Notices issued by JHR for a period of at least seven (7) years from the date of its creation or the date when it last was in effect, whichever is later.

D. Enforcement

Knowledge of a violation or potential violation of this policy must be reported directly to the Privacy Officer.

X. Revisions to Notice of Privacy Practices

A. Purpose

45 CFR §164.520 requires that notice be given to individuals of the use and disclosure of PHI as well as the individual's rights and covered entities' legal duties with respect to PHI. This policy is designed to give guidance to a Covered Entity and Business Associate when it makes changes to its Notice of Privacy Practices and to ensure compliance with all laws and regulations regarding the provision of the notice of use of PHI by Covered Entity. This policy is not applicable to inmates.

B. Policy

JHR reserves the right to change the terms of its Notice and to make new Notice provisions effective for all PHI that it maintains.

JHR will provide each covered client/employee with a copy of any revisions of its Notice of Privacy Practices.

C. Procedure

JHR will post revisions to its Notice of Privacy Practices in a clear and prominent location where it is reasonable to expect individuals to be able to read the Notice.

JHR will provide each covered client or employee with a copy of any revisions of its Notice of Privacy Practices at the time of their next renewal.

If there is a need for Company to use or disclose any PHI of the covered client/employee it will mail a copy of any revisions of its Notice of Privacy Practices to their last known address.

The Privacy Officer will provide copies of the revisions of its Notice of Privacy Practices at any time.

JHR will prominently post its revisions to the Notice of Privacy Practices on any websites that it maintains that provide information about its client services or benefits, and will make the notice available electronically through the website.

XI. Training Policy

A. Overview

The Privacy Rules require that JHR train their employees on the requirements of our privacy policies and procedures developed to protect the Protected Client Data to which employees are provided access. JHR has determined that all applicable employees shall be trained on privacy so that they can provide the necessary assurances for the protection of Protected Client Data to clients, vendors and business partners as required under the Privacy Rules.

B. Purpose

To provide instructions to all applicable JHR employees regarding the requirement for HIPAA training.

C. Applicability

This policy applies to all JHR workforce members who have access or potential access to PHI.

D. Policy

General: It is the policy of JHR that all employees of the Company be trained on privacy and the Company policies and procedures created to protect Protected Client Data and all PHI held by the Company.

Duty Specific Training: Privacy training shall be appropriate to the tasks that each employee performs. In the case where an employee does not come into contact with Protected Client Data as a normal course of the employee's duties, the employee shall be trained on the Company policies and procedures.

New Employees: New employees shall be trained on the Company policies and procedures as part of their normal employment process and shall be trained on our privacy policies and procedures, if applicable, within 30-day of being employed by JHR. The Privacy Officer shall document this training within the 30-day period.

Material Change in Policies and Procedures: When a material change in the policies and procedures occurs, each employee shall receive training on such changes within 30 days of the implementation of the change. The Privacy Officer shall document this training within the 30-day period.

XII. Photocopier Policy

A. Overview

The Privacy Rules require that JHR implement appropriate administrative, technical, and physical safeguards to protect our clients'/employees' PHI.

B. Purpose

To provide instructions to all agents and employees regarding the use of copiers with respect to PHI and the measures necessary to maintain an adequate level of security for such information. This policy defines rules necessary to achieve this level of protection. These standards are designed to minimize the potential exposure to JHR from damages, which may result from unauthorized disclosure of PHI through facsimile use.

C. Applicability

This policy applies to all JHR workforce members who have access or potential access to PHI.

D. Special definitions

Photocopier: any electrically operated machine using a photographic method, as the electrostatic process, for making instant copies of written, drawn, or printed material.

E. Company Policies

The copier and the printers are for Company business use only. Do not copy/print personal or non-work related items.

Agents and employees must exercise utmost caution when photocopying documents. Photocopies containing PHI should be immediately added to the client file, and should be properly protected.

All copiers are configured to not store copies of the photocopied materials on the hard drive.

As a precaution the photocopier's hard drive will be erased before returning the copier to the leasing company.

F. Enforcement

Any agent/employee found to have violated this policy shall be subject to disciplinary action, up to and including termination of employment. In the case where inappropriate

access, use or disclosure of PHI was or may have been involved, such individuals may additionally be reported to the appropriate enforcement agencies.

XIII. Fax Policy

A. Overview

The Privacy Rules require that JHR implement appropriate administrative, technical, and physical safeguards to protect our clients'/employees' PHI.

B. Purpose

To provide instructions to all agents and employees regarding the use of faxes with respect to PHI and the measures necessary to maintain an adequate level of security for such information. This policy defines rules necessary to achieve this level of protection. These standards are designed to minimize the potential exposure to JHR from damages, which may result from unauthorized disclosure of PHI through facsimile use.

C. Applicability

This policy applies to all JHR workforce members who have access or potential access to PHI.

D. Special definitions

Fax: An electronic facsimile of a document stored as a series of zeroes and ones (binary data) that can be transmitted like normal computer data. When received by a fax machine, the incoming stream is translated into dots creating a representation of the original document.

Inappropriate Disclosure: The intentional or unintentional revealing of PHI to people who do not have a need to know or authority to access such information.

E. Company Policies

Agents and employees will wait by the fax machine to receive their own faxes. They must also exercise utmost caution when sending faxes to parties outside of JHR. Faxes containing PHI should only be sent to user or departmental specific fax machines and not to systems that have general access. Should PHI be disclosed by fax to an inappropriate party, JHR shall, to the extent possible, remediate such disclosures.

All fax documents sent by JHR shall contain the following statement:

> This message is intended only for the use of the individual or entity to which it is addressed, and may contain information that is privileged, confidential and exempt from disclosure under applicable law. No waiver of applicable privileges and/or protection against disclosure is intended. If the reader of this message is not the intended recipient, or

the employee or agent responsible for delivering the message to the intended recipient, you are hereby notified that any use of, dissemination, distribution or copying of this communication is strictly prohibited. If you have received this communication in error, please notify us immediately by telephone and shred this message. Thank you.

G. Procedure

In the cases where data that contains PHI is disclosed by fax machine use to an inappropriate party, the following procedure shall be followed:

1. The receiving party shall be contacted by telephone at the earliest opportunity and requested to destroy the fax without reading.
2. The name of the company, the person contacted, the date and time shall be recorded as well as any comments made by the person receiving such calls.
3. A fax shall also be sent to the receiving party containing the same instructions as detailed for the phone call requesting a return fax message indicating that the requested action was taken.
4. The cause of the inappropriate disclosure shall be determined and reported to our Privacy Officer.

Methods to prevent a reoccurrence of the inappropriate disclosure shall be formulated and put into place.

Any additional actions prescribed by regulations shall be performed to the extent possible.

H. Enforcement

Any agent/employee found to have violated this policy shall be subject to disciplinary action, up to and including termination of employment. In the case where inappropriate access, use or disclosure of PHI was or may have been involved, such individuals may additionally be reported to the appropriate enforcement agencies.

XIV. Scanner Policy

A. Overview

The Privacy Rules require that JHR implement appropriate administrative, technical, and physical safeguards to protect the privacy of PHI.

B. Purpose

To provide instructions to all agents and employees regarding the use of scanners with respect to PHI and the measures necessary to maintain an adequate level of security for such information. This policy defines rules necessary to achieve this level of protection. These standards are designed to minimize the potential exposure to JHR from damages, which may result from unauthorized disclosure of PHI.

C. Applicability

This policy applies to all JHR workforce members who have access or potential access to PHI.

D. Special Definitions

Scanner: An electronic copy of a document stored as a series of zeroes and ones (binary data) that can be transmitted like normal computer data. When received by a computer, the incoming stream is translated into dots creating a representation of the original document.

Inappropriate Disclosure: The intentional or unintentional revealing of Personally-Identifiable Information to people who do not have a need to know or authority to access such information.

E. Procedure

Scanned material goes from the copier/scanner to the S drive on the server using a protected network. After the employee accesses the document on the S drive, they save it on the R, P or Z drive in the appropriate file for permanent storage

F. Enforcement

Any agent/employee found to have violated this policy shall be subject to disciplinary action, up to and including termination of employment. In the case where inappropriate access, use or disclosure of PHI was or may have been involved, such individuals may additionally be reported to the appropriate enforcement agencies.

XV. Business Associate Subcontractor Agreements

A. Overview

The Privacy Rules impose certain requirements on Business Associates who create, receive, use or disclose Protected Client Data on behalf of their Covered Entity partners. JHR must comply with the requirements in this section.

B. Purpose

To provide instructions to all of JHR's workforce regarding the necessity of and the requirements for Business Associate Agreements relating to Subcontractors, and in some cases other Covered Entities, who receive, use or disclosure Protected Client Data on behalf of the Company.

C. Applicability

This policy applies to all JHR workforce members who have access or potential access to PHI.

D. Policy

Generally: JHR may disclose Protected Client Data to a Business Associate Subcontractor, or allow a Business Associate Subcontractor to create or receive Protected Client Data on the Company's behalf, if adequate assurances that the Business Associate Subcontractor will appropriately safeguard the Protected Client Data obtained from the Company. JHR must document these assurances through a written agreement. This requirement does not apply with respect to:

1. Disclosures made to a provider concerning the individual's treatment, payment or health care operations, or;
2. Uses or disclosures made to a governmental agency for purposes of public benefit eligibility or enrollment determinations where such agency is authorized by law to make these determinations.

Content Requirements: The agreement between JHR and a Business Associate Subcontractor must meet the following requirements, as applicable:

1. Establish permitted and required uses or disclosures of Protected Client Data that are consistent with those authorized for the entity, except that the agreement may permit the Business Associate Subcontractor to use or disclose Protected Client Data for its own management and administration if such use or disclosure is required by law or the Business Associate Subcontractor obtains reasonable assurance from the entity to which the Protected Client Data is disclosed that the confidentiality of the Protected Client Data will be maintained.
2. Provide that the Business Associate Subcontractor will:
    a. Not use or disclose the Protected Client Data except as authorized under the agreement or required by law.
    b. Use safeguards to prevent unauthorized use or disclosure.
    c. Report unauthorized uses or disclosures to the Company.
    d. Pass on the same obligations relating to protection of Protected Client Data to any subcontractors or agents.
    e. Make Protected Client Data available for access by the individual or his/her personal representative, in accordance with relevant law and policy.
    f. Make Protected Client Data available for amendment, and incorporate any approved amendments to Protected Client Data, in accordance with relevant law and policy.
    g. Make information available for the provision of an accounting of uses and disclosures in accordance with relevant law and policy.
    h. Make its internal practices, books and records relating to its receipt or creation of Protected Client Data available to the Secretary of HHS for purposes of determining the entity's compliance with Privacy Rules.
    i. If feasible, return or destroy all Protected Client Data upon termination of contract; if any Protected Client Data is retained, continue to extend the full protections specified herein as long as the Protected Client Data is maintained.

j. Authorize termination of the agreement by the entity upon a material breach by the Business Associate Subcontractor.

Compliance Responsibilities*:* If JHR knows of a pattern or practice of the Business Associate Subcontractor that amounts to a material violation of the Agreement, JHR must attempt to cure the breach to end the violation, and if unsuccessful, terminate the Agreement. If terminating the Agreement is not feasible JHR must report the problem to the Secretary of HHS.

E. Enforcement

A Business Associate found to have violated this policy shall be subject to remedial action, up to and including termination of contract. In the case where inappropriate access or use of Protected Client Data was or may have been involved, these individuals may additionally be reported to the appropriate law enforcement agencies.

XVI. Incident Reporting and Breach Notification—Business Associate

A. Purpose

As required by the Breach Notification Rule, JHR will notify the affected Covered Entity of any Breach of Unsecured PHI.

B. Policy

A Breach shall be treated as discovered by JHR on the first day which such Breach is known to Company or, through the exercise of reasonable diligence, would have been known to Company. Company will mitigate, to the extent practicable, any harmful effect that is known to Company of a use or disclosure of PHI by Company in violation of the requirements of the agreement between JHR and the Covered Entity.

C. Procedures

Following the discovery of a Breach of Unsecured PHI, JHR shall notify Privacy Officer of Covered Entity of such breach without unreasonable delay and in no case no later than fifteen (15) calendar days after discovery of the Breach.

JHR shall include, to the extent possible, in the breach notification:

1. The identification of each individual whose unsecured PHI has been, or is reasonably believed by Company to have been, accessed, acquired, used, or disclosed during the breach;
2. A brief description of what happened, including the date of the breach and the date of discovery of the breach, if known;
3. A description of the types of unsecured PHI that were involved in the breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);
4. Any steps individuals should take to protect themselves from potential harm resulting from the breach;
5. A brief description of what Company is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches; and
6. Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, website, or postal address.

XVII. Sanctioning of Employees, Agents, and Contractors

A. Purpose

JHR has established and will apply appropriate sanctions against its employees, as well as agents and contractors, who fail to comply with its policies and procedures. This policy is designed to give guidance and ensure compliance with all applicable laws and regulations related to sanctioning for violating Company's policies and procedures. Under the HIPAA, penalties for misuse or misappropriation of health information include both civil monetary penalties and criminal penalties. Civil penalties range from the minimum of $100 to a maximum of $50,000 per violation, with an annual maximum of $1.5 million. Criminal penalties vary from $50,000 and/or 1-year imprisonment to $250,000 and/or 10 years' imprisonment (42 USC § 1320d).

B. Overview

Violation of JHR Benefits policies and rules may warrant disciplinary action. The Company has a system of progressive discipline that may include verbal warnings, written warnings, and suspension. The system is not formal, and JHR Employee Benefits may, in its sole discretion, utilize whatever form of discipline is deemed appropriate under the circumstances, up to, and including, immediate termination of employment. The Company's policy of progressive discipline in no way limits or alters the at-will employment relationship.

C. Policy

JHR will apply appropriate sanctions against members of its workforce who fail to comply with JHR's policies and procedures.

The type of sanction applied shall vary depending on the severity of the violation, whether the violation was intentional or unintentional, whether the violation indicates a pattern or practice of improper access, use or disclosure of health information, and similar factors.

Employees, agents and contractors should be aware that violations of a severe nature may result in notification to law enforcement officials as well as regulatory, accreditation, and/or licensure organizations.

The policy and procedures contained herein do not apply specifically when JHR employees exercise their right to:

1. File a complaint with HHS;
2. Testify, assist, or participate in an investigation, compliance review, proceeding, or hearing under Part C of Title XI;
3. Oppose any act made unlawful by the HIPAA Privacy Rule, provided the individual or person has a good faith belief the act opposed is unlawful, and the manner of the opposition is reasonable and does not involve a disclosure of PHI in violation of the HIPAA Privacy Rule;
4. Disclose PHI as a whistleblower when the disclosure is to a health oversight agency, public health authority, or an attorney retained by the individual for purposes of determining the individual's legal options with regard to the whistleblower activity; or
5. An employee who is a victim of a crime and discloses PHI to a law enforcement official, provided that the PHI is about a suspected perpetrator of the criminal act and is limited to the information listed in the policy entitled "Disclosing PHI for Law Enforcement Release."

D. Procedure

The following sanctions apply for failure to comply with the Company's policies and procedures or with the requirements of HIPAA regulations:

First privacy infraction

If the infraction is:

1. A simple infraction and
2. The first infraction in the last three (3) years,

The sanction will be retraining the employee on the appropriate policy/procedure and placement of a written letter of reprimand in the employee file. The letter will notify the person of the nature of this infraction and of sanctions for future potential infractions.

Second privacy infraction, or first serious infraction

If the infraction is:

1. A serious infraction or
2. The second infraction of either type within three (3) years,

The sanction will include a written letter of reprimand that is given to the person at fault, placement of a copy of the letter in the employee file, and one week's suspension without pay. The letter will notify the person of the nature of this infraction and of sanctions for future potential infractions.

Third privacy infraction or second serious infraction

If the infraction is:

1. A second serious infraction within three (3) years, or
2. A third infraction of any type within three (3) years,

The sanction will be dismissal from the workforce members.

All sanctions will be documented and retained for a period of at least seven (7) years from the date of its creation or the date when it was last in effect, whichever is later.

We define a serious infraction as one that results in known significant damage or that threatens imminent significant damage. Other infractions are simple infractions.

Mitigation Efforts Required

JHR, to the extent practicable, shall mitigate any harmful effects of unauthorized uses or disclosures of PHI by the Company or any of its Business Associates.

Prohibition on Intimidating or Retaliatory Acts

The Company will not retaliate against an employee for filing a complaint and will not tolerate or permit retaliation by management, employees or co-workers.

Neither JHR nor any employee shall intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual for the exercise of their rights or participation in any process relating to HIPAA compliance, or against any person for filing a complaint with the Secretary of the U.S. Department of Health and Human Services, participating in an investigation, compliance review, proceeding or hearing, or engaging in reasonable opposition to any act that the person in good faith believes to be unlawful under the Privacy Rules as long as the action does not involve disclosure of PHI in violation of the regulations.

CLIENT RIGHTS

XVIII. Individual Rights Relating to Protected Client Data

A. Overview

The Privacy Rules provide individuals with certain rights regarding their Protected Client Data.

B. Purpose

It is the purpose of this section to provide instructions regarding JHR obligations in complying with an individual's rights under the Privacy Rules to provide the individual with access to, a copy of and an accounting for disclosures of Protected Client Data relating to the individual.

C. Applicability

This policy applies to all JHR workforce members who have access or potential access to PHI.

D. Special Definitions

Personal Representative means a person who has authority under applicable law to make decisions related to health care on behalf of an adult or an emancipated minor, or the parent, guardian, or other person who is authorized under law to make health care decisions on behalf of an un-emancipated minor.

E. Policy

Right to Access and Copy Protected Client Data

Individuals have a right to access and copy their Protected Client Data and any information in designated record sets except as follows:

1. Denial of Access: JHR must provide a timely, written denial of access to the individual, written in plain language, explaining the basis for the denial, any applicable right of review, and describe how the individual may complain to JHR (including name or title of contact, and phone number) or the U.S. Secretary of Health and Human Services (HHS).
    a. To the extent possible, the individual must be given access to any information requested after excluding the information for which entity has grounds for denying access.
    b. If JHR does not maintain the information for which access has been requested, but knows where it is maintained, Company must inform the individual where to direct the request for access.
    c. Denial of Access without a right of review: Individuals may be denied access and right to copy Protected Client Data relating to the individual when:
        1) Information was compiled in anticipation of litigation.

2) Care was provided under the direction of a correctional institution and provision of access would jeopardize health, safety, or rehabilitation.
3) Information was collected in the course of research that includes treatment of the individual and the individual agreed to a suspension of the right of access during the research period.
4) Where such access would provide the individual access to the Protected Client Data of other individuals.

2. Provision of Access: JHR must provide an individual with access to the information in the form or format requested if it is readily producible in such form or format, or in a readable hard copy or other form or format as mutually agreed to, either by arranging for a convenient time and place for inspection and copying, or mailing the information at the individual's request.

    a. If the information is maintained in more than one place, the information need only be produced once in response to a current request for access.
    b. JHR may provide a summary of the information in lieu of providing access, or may provide an explanation of the information to which access is provided if the individual, in advance, agrees.
    c. JHR may impose a reasonable, cost-based fee for copying, or preparing a summary or explanation of the information provided that the fee includes only the cost of copying supplies, postage, and labor for preparing the summary or explanation as agreed to by the individual.

3. Documentation: JHR must document and retain for seven (7) years from the date of its creation the designated record sets subject to access and the names or titles of persons responsible for receiving and processing requests for access.

Right to Request an Amendment of Protected Client Data

An individual has the right to have JHR amend Protected Client Data or other information in the designated record set for as long as the Company maintains the information. JHR must act on the request within sixty (60) days of receipt, or within ninety (90) days if the Company notifies the individual within the first 60 days of the reasons for delay and the date by which action will be taken. [See Request and Response to Amend Form.]

1. Accepting the Amendment: If JHR accepts the amendment, in whole or in part, it must:

    a. Timely inform the individual that the amendment is accepted, and obtain his/her identification of an agreement to have JHR notify relevant persons with a need to know.
    b. Make reasonable efforts to inform and timely provide the amendment to those persons and others, including Subcontractor Business Associates, that JHR knows to have the affected Protected Client Data and that may have relied, or be foreseen to rely, on that information to the detriment of the individual.

2. Denying the Amendment: JHR may deny the request if it determines that the record:

a. Was not created by JHR (unless the individual provides reasonable basis to believe that the originator of the record is no longer available to act on the request);
b. Is not part of the designated record set;
c. Would not be available for inspection; or
d. Is accurate and complete.

2. Denial Requirements: If JHR denies the amendment, in whole or part, it must:
   a. Provide the individual with a timely denial, written in plain language and including:
      1) The basis for denial;
      2) Notice of the individual's right to submit a written statement of disagreement, and instructions on how to file the statement, or to request that future disclosures of the Protected Client Data include copies of the request and the denial; and
      3) A description of how the individual may complain about the decision to JHR or to the U. S. Secretary of HHS.
   b. Permit the individual to submit a statement of disagreement (but entity may reasonably limit its length).
   c. Provide a copy of any rebuttal prepared to the individual.
   d. As appropriate, identify the part of the record subject to the disputed amendment and append or otherwise link the request, the denial, and any statement of disagreement or rebuttal to the record.
   e. For future disclosures of the record, include any statement of disagreement or, in response to the individual's request, the amendment request and the denial (or an accurate summary of either of the foregoing). If standard transaction format does not permit the appending of the additional information, it must be transmitted separately to the recipient of the standard transaction.
3. Notification of Amendment: If JHR is informed by a Covered Entity or another Business Associate of a Covered Entity about an amendment to the record, JHR must amend the information in its record by, at a minimum, identifying the affected records and appending or otherwise providing a link to the location of the amendment.
4. Documentation: JHR must document the titles of the persons or offices responsible for receiving and processing requests for amendments.

Right to an Accounting of Disclosures An individual has a right to receive an accounting of disclosures of their PHI for the previous seven (7) years.

1. Disclosures <u>excepted</u> from this accounting requirement:
   a. To carry out treatment, payment and health care operations.
   b. To individuals or groups of individuals allowed under an authorization signed by the individual who is the subject of the Protected Client Data.
   c. To the individual to whom the Protected Client Data relates.
   d. For national security or intelligence purposes as defined in the privacy regulations.

e. To correctional institutions or law enforcement officials.
f. That occurred prior to the compliance date for the Covered Entity.

2. JHR must temporarily suspend an individual's right to receive an accounting of disclosures to a health oversight agency or law enforcement official, as provided, for the time specified by such agency or official if requested in accordance with these provisions.
3. Disclosures included in Accounting:
   a. The date of the disclosure
   b. The name of the entity or person who received the protected information, and if known, the address of such entity or person
   c. A brief description of the PHI disclosed
   d. A brief statement of the purpose of the disclosure that reasonably informs the Participant of the basis for the disclosure.
4. Provisioning of Accounting of Disclosures:
   a. JHR must act on the individual's request for an accounting, no later than 60 days after receipt of such a request. The Company may extend the time frame by no more than 30 days. This extension may only be used once.
   b. The first accounting within any 12-month period must be provided without charge. Each subsequent request by the same individual may include a reasonable, cost-based fee, provided JHR informs the individual in advance of the fee and provides the individual with an opportunity to withdraw or modify the request in order to avoid or reduce the fee.

F. Enforcement

An employee found to have violated this policy shall be subject to disciplinary action, up to and including termination of employment. In the case where inappropriate access, use or disclosure of Protected Client Data was or may have been involved, such individuals may additionally be reported to the appropriate enforcement agencies.

XIX. Confidential Communications

A. Overview

Clients have the right to request confidential communication of their PHI by alternative means or at alternative locations. JHR must accommodate all reasonable requests.

B. Purpose

It is the purpose of this section to provide instructions regarding Company's obligations in complying with an individual's rights under the Privacy Rules to provide the individual with confidential communication of PHI.

C. Applicability

This policy applies to all JHR workforce members who have access or potential access to PHI.

D. Policy

JHR must accommodate all reasonable requests from the client for confidential communication, and may not condition accommodation of the request or require an explanation as a condition of accommodating the request.
Requests for confidential communication apply to:

1. Communications from JHR to the client; and
2. Information that would be sent to the named insured of an insurance policy that covers the client as a dependent of the named insured.

E. Procedures

Requests for confidential communication must include the client's designation of the means and location of alternative delivery of the PHI. For example, these requests may include, but not be limited to:

1. Communication by telephone to an alternate phone number;
2. Mail to an address other than the address of record;
3. A request for telephone communication only; or
4. Sealed envelope delivery rather than a post card.

The only basis upon which JHR may decline to accommodate a reasonable request for confidential communication is in the event the client fails to:

1. Provide an alternative address, telephone number or other communication method or location in his or her request; or
2. Provide information about how payment for the additional communication requirements will be handled, if applicable.

Requests for confidential communication must be made in writing to our Privacy Officer. The client may use the *Authorization and Release Form to Disclose PHI* (in General Forms…).

When a client makes a request for confidential communications, JHR will verify the client's identity by confirming the birthdate, social security number, etc.; by confirming a form of identification; or by verifying the signature of the client.

The client must be informed:

1. Of any fees or charges to be paid by the client related to the type of confidential communication requested.
2. If JHR is not able to meet the request for confidential communication.

Once designated, alternate means of communication should remain in effect until the client informs JHR otherwise. However, in certain limited circumstances and with the prior consent of the Privacy Officer, Company may contact an individual for treatment, payment and/or health care operations purposes at an address or via a means that differ from the means/method initially agreed to by JHR.

By way of example, in the event that a client refuses to respond to JHR's communication (e.g. client fails to return phone calls), the employee should bring the problem to the attention of the Privacy Officer for JHR to determine whether the client should be contacted via a means or at an address other than the address or method requested by the client.

F. Documentation

JHR's Privacy Officer or other designee is responsible for ensuring that the information is documented and communicated to the appropriate individuals. JHR will document the acceptance or denial of a client's request for confidential communications, as well as maintain all documentation relating to the request in the client's permanent record.

G. Enforcement

Employees found to have violated this policy shall be subject to disciplinary action, up to and including termination of employment. In the case where inappropriate access, use or disclosure of Protected Client Data was or may have been involved, such individuals may additionally be reported to the appropriate enforcement agencies.

XX. Authorization to Use or Disclose PHI

A. Overview

The Privacy Rules provide individuals with certain rights regarding their Protected Client Information.

B. Purpose

HIPAA requires a Covered Entity and their Business Associates to obtain authorization to use or disclose PHI for all purposes not explicitly permitted under the regulations. 45 CFR §164.508(b)(4); §164.508(c); §164.508(d). As such, JHR has created the following policies and procedures to comply with all applicable laws and regulations.

C. Applicability

This policy applies to all JHR workforce members who have access or potential access to PHI.

D. Policy

JHR will comply with the requirements set forth in 45 CFR §164.508(d) to request authorization to use or disclose PHI. Except as stated in these Privacy Policies and Procedures, JHR will not condition services on the provision of an authorization.

E. Procedure

The authorization will be written in plain language. Any authorization initiated by the Company for the disclosure of PHI will contain the following:

1. A description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion;

2. A description of each purpose of the requested use or disclosure;
3. The name or other specific identification of the person(s), or class of persons, authorized to make the requested use or disclosure;
4. The name of other specific identification of the person(s), or class of persons, to whom the Company may make the requested use or disclosure;
5. An expiration date or an expiration event that relates to the individual or the purpose of the use or disclosure;
6. Statement of the individual's right to revoke the authorization in writing and the exceptions to the right to revoke;
7. A description of how the individual may revoke the authorization;
8. A statement that information used or disclosed pursuant to the authorization may be subject to re-disclosure by the recipient and no longer protected by 45 CFR §164;
9. The signature of the individual; or signature of personal representative with a description of the personal representative's authority to act for the individual and documentation of verification of that identity with date;
10. A statement that the individual may refuse to sign the authorization;
11. For marketing uses or disclosures, if applicable, a statement that the use or disclosure of the requested information will result in direct or indirect remuneration to the Company from a third party;
12. A statement that the Company will not condition treatment, payment, enrollment in the health plan, or eligibility for benefits on the individual's providing authorization for the requested use or disclosure, except as provided in these Privacy Policies and Procedures.
13. In addition, as part of the authorization process, the Company will provide individuals with any facts they need to make an informed decision as to whether to allow release of the information.
14. The Company will document and retain the signed authorization for a period of at least 7 years from the date of its creation or the date when it last was in effect, whichever is later.
15. The Company will provide the individual with a copy of the signed authorization.
16. The authorization will not be combined with another document to create a compound authorization, unless:
    a. The other document is a similar authorization;
    b. The authorization is for the use or disclosure of PHI created for research that includes treatment of the individual.

F. Enforcement

Employees found to have violated this policy shall be subject to disciplinary action, up to and including termination of employment. In the case where inappropriate access, use or disclosure of Protected Client Data was or may have been involved, such individuals may additionally be reported to the appropriate enforcement agencies.

XXI. Individual Revocation of an Authorization to Disclose PHI

A. Purpose

As organizations request authorization from individuals to use their PHI, there will be cases where individuals will initially grant authorization only to later change their minds. In these instances, JHR has created policies and procedures to accommodate individuals who may wish to revoke their authorization.

B. Policy

JHR will allow an individual to revoke an authorization to use or disclose their PHI, except in situations where:

1. JHR has taken action in reliance thereon;
2. The authorization was obtained as a condition of obtaining insurance coverage and other law provides the insurer with the right to contest a claim under the policy.

JHR will take all necessary steps to honor and comply with an individual revocation of an authorization to use or disclose PHI, unless stated otherwise in this policy.

C. Procedure

JHR will not impose a time restriction on when an individual may revoke authorization to use or disclose their PHI.

JHR will require individuals to request the revocation of authorization to use or disclose PHI in writing.

XXII. Permitted and Required Use and Disclosure of Protected Client Data

A. Overview

The Privacy Rules impose certain requirements on Covered Entities and Business Associates who create, receive, use or disclose Protected Client Data on behalf of their Covered Entity partners.

B. Purpose

To provide instructions to all JHR employees regarding the receipt, uses and disclosures of Protected Client Data, which are permitted or required by HIPAA.

C. Applicability

This policy applies to all JHR workforce members who have access or potential access to PHI.

D. Special Definitions

Public Health Authority means a governmental agency or authority, or a person or entity acting under a grant of authority from or a contract with such a public agency, including the employees or agents of the public agency, its contractors and those to whom it has granted authority, that is responsible for public health matters as part of its official mandate.

E. Policy

State and federal law permit and require certain receipt, uses and disclosures of Protected Client Data such as those related to Business Associate Agreements. Additional uses and/or disclosures are allowed or required related to public responsibility that require no agreement or authorization on the part of the individual who is the subject of the Protected Client Data. It is the policy of JHR to obtain, use and disclose Protected Client Data only as permitted and/or required by law or regulation including the following situations:

1. Treatment, Payment or Healthcare Operations: Protected Client Data may be used or disclosed for the purposes of providing treatment, payment or healthcare operations. Such disclosures will be made only as allowed by and pursuant to prevailing state and federal law.
    a. Discussions involving Protected Client Data shall be conducted only in appropriate business areas including but not limited to offices, conference rooms and other non-public areas;
    b. Conducted only for the purpose of fulfilling a legitimate business need; and
    c. Conducted with regard to and in compliance with the "minimum necessary provision," See *Minimum Necessary Provision.*
2. Contained in a Business Associate Agreement: For permitted and required uses or disclosures of Protected Client Data that are consistent with those authorized by the Covered Entity in a Business Associate Agreement.
3. Required by Law: Protected Client Data may be used or disclosed to the extent such use or disclosure complies with and is limited to the requirements of such law.
4. Abuse and Neglect: Except for reports of child abuse or neglect, Protected Client Data about an individual believed to be a victim of abuse, neglect, or domestic violence may be disclosed to a governmental authority authorized to receive such reports if the individual agrees or the reporting entity believes, in the exercise of professional judgment, that the disclosure is necessary to prevent serious physical harm. If the individual lacks the capacity to agree, disclosure may be made if not intended for use against the individual and delaying disclosure would materially hinder law enforcement activity. The individual whose Protected Client Data has been released must be promptly informed that the report was made unless doing so would place the individual at risk of serious harm.
5. Judicial Proceedings: Protected Client Data may be disclosed in response to a court order.
6. Law Enforcement: Protected Client Data may be disclosed for the following law enforcement purposes and under the specified conditions:
    a. Pursuant to court order or as otherwise required by law, i.e. laws requiring the reporting of certain types of wounds or injuries;

b. Decedent's Protected Client Data may be disclosed to alert law enforcement to the death if entity suspects that death resulted from criminal conduct;

5. Serious Threats to Health or Safety: Consistent with applicable law and ethical standards, Protected Client Data may be used or disclosed if the entity believes in good faith that the use or disclosure is necessary to prevent or lessen a serious and imminent threat to a person or the public, and disclosure is to someone reasonably able to prevent or lessen the threat, or the disclosure is to law enforcement authorities to identify or apprehend an individual who has admitted to violent criminal activity that likely caused serious harm to the victim or who appears to have escaped from lawful custody. Disclosures of admitted participation in a violent crime are limited to the individual's statement of participation and are not permitted when the information is learned in the course of treatment to affect the propensity to commit the subject crime, or through counseling, or therapy or a request to initiate the same.
6. Specialized Government Functions:

    a. National Security and Intelligence: Protected Client Data may be disclosed to authorized federal officials for the conduct of lawful intelligence, counter intelligence, and other activities authorized by the National Security Act.
    b. Protective services: Protected Client Data may be disclosed to authorized federal officials for the provision of protective services to the President, foreign heads of state, and others designated by law, and for the conduct of criminal investigations of threats against such persons.
    c. Public Benefits: Protected Client Data relevant to administration of a government program providing public benefits may be disclosed to another governmental program providing public benefits serving the same or similar populations as necessary to coordinate program functions or improve administration and management of program functions.

7. Workers' Compensation: Protected Client Data may be disclosed as authorized and to the extent necessary to comply with laws relating to workers' compensation and other similar programs.

F. Procedures

The following procedures will be implemented to ensure that this policy is enforced effectively across all parts of JHR:

1. Any request for disclosure of Protected Client Data pursuant to a court order, warrant or subpoena must be directed to the appropriate Company individual for review and action. Upon receipt of such court order, warrant or subpoena, employees shall include an acknowledgement receipt to ensure that the document was actually received by the appropriate Company individual and will retain a copy of the court order, warrant or subpoena received. If the acknowledgement is not received within two working days of submitting to the appropriate Company individual, then the request will be resubmitted to the Privacy Officer.
2. Any request for disclosure of Protected Client Data by a law enforcement agent must be directed to the appropriate Company individual for review and action. Any such

requests shall include an acknowledgement of receipt to ensure that the request was actually received by the appropriate Company individual and will retain a copy of the request received. If the acknowledgement is not received within two working days of submitting to the appropriate Company individual, then the request will be resubmitted to the Privacy Officer.

3. Any request for disclosure of Protected Client Data by a public health authority must be directed to the appropriate Company individual for review and action. Any such request will include an acknowledgement of receipt to ensure that the document was actually received by the appropriate Company individual and will retain a copy of the request. If the acknowledgement is not received within two working days of submitting to the appropriate Company individual, then the request will be resubmitted to the Privacy Officer.
4. Any request for disclosure of Protected Client Data by a national security, intelligence or other federal agency must be directed to the appropriate Company individual for review and action. Any such request will include an acknowledgement of receipt that the document was actually received by the appropriate Company individual and will retain a copy of the request. If the acknowledgement is not received within two working days of submitting to the appropriate Company individual, then the request will be resubmitted to the Privacy Officer.

G. Enforcement

An employee found to have violated this policy shall be subject to disciplinary action, up to and including termination of employment. In the case where inappropriate access, use or disclosure of Protected Client Data was or may have been involved, such individuals may additionally be reported to the appropriate enforcement agencies.

XXIII. Complaint Process

A. Overview

The Privacy Rules require that JHR provide a process for individuals to make complaints concerning Company's policies and procedures required by these regulations and document all complaints received, and the dispositions of these complaints, if any.

B. Purpose

To issue instructions regarding Company’s obligations relating to the Privacy Rules to provide a process for individuals to complain about the entity's policies and procedures and the requirement to document complaints received and the disposition of these complaints.

C. Applicability

This policy applies to all JHR workforce members who have access or potential access to PHI.

D. Policy

JHR shall maintain a process to receive complaints from individuals about Company's privacy policies and procedures, for complaints from individuals who believe their privacy rights have been violated and from employees or Subcontractor who believe that JHR is not abiding by its policies and procedures and/or assurances concerning Protected Client Data. This process shall include the following:

1. A designated person to provide information about submitting a complaint whose name or title and telephone number will be published to the individuals, employees and Subcontractors.
2. A system and software or log with which to record complaints received by the named individual and the dispositions of complaints recorded, if any.
3. JHR shall work in good faith to resolve complaints received to the satisfaction of the submitter, where possible.

E. Procedures

The following procedures will be implemented to ensure that this policy is enforced effectively across all parts of JHR:

1. Complaints shall be submitted in writing on paper or electronically.
2. Complaints shall be entered into the complaint tracking system by the Privacy Officer in the exact words provided by the submitter.
3. The Privacy Officer shall investigate complaints and make a determination as to whether or not the complaint has merit.
4. The Privacy Officer shall present complaints received to Jeana Hutchings, Managing Owner.

    a. If the Privacy Officer has completed the investigation of the complaint and made a determination, such determination shall be presented to Jeana Hutchings.
    b. If the investigation has not been completed nor a provisional determination made by the Privacy Officer, it shall be the prerogative of Jeana Hutchings to make a summary determination or to direct the Privacy Officer to continue with the investigation and to report on the complaint at the next scheduled meeting.
    c. If a determination is made that JHR is in violation of the Privacy Rules or that changes are needed in the Notice of Privacy Practices or Business Associate Agreement to clarify the allowed practices of JHR, the Company's Privacy Officer and management shall determine the actions that the Company shall take.
    d. Complaint determinations and actions that JHR takes pursuant to such complaints, if any, shall be reported to the submitter of the complaint, if such person is known.
    e. The Privacy Officer, or designated agent, shall update the complaint tracking system with the findings of the investigation, any determination made, direction or actions of the Company with regard to the complaint, and a copy of any information provided to the submitter in response to their complaint.

F. Enforcement

Any employee found to have violated this policy shall be subject to disciplinary action, up to and including termination of employment. In the case where inappropriate access, use or disclosure of Protected Client Data was or may have been involved, such individuals may additionally be reported to the appropriate enforcement agencies.

XXIV. Individual Rights to PHI—Accounting

A. Purpose

HIPAA requires that individuals have a right to receive an accounting of various instances when PHI about them is disclosed by a Covered Entity, subject to certain time-limited exceptions for disclosures to law enforcement and oversight agencies. JHR has developed policies and procedures to address the accounting of instances when PHI has been used or disclosed for purposes other than treatment, payment, or health care operations.

B. Policy

JHR will allow individuals to receive an accounting of instances where PHI about them is used or disclosed, except for the following purpose:

1. To carry out treatment, payment and health care operations;
2. To persons involved in the individual's care or other notification purposes;
3. For national security or intelligence purposes;
4. To correctional institutions or law enforcement custodial situations.

JHR will not allow individuals to receive an accounting of instances where PHI about them is used or disclosed prior to April 14, 2003.

JHR will utilize Company files and systems for documenting and maintaining an accounting of when PHI has been disclosed for purposes other than treatment, payment or health care operations.

C. Procedure

JHR will allow an individual to obtain an accounting of instances when their PHI has been disclosed.

JHR will allow an individual to receive an accounting of disclosures of PHI made by the Company in the seven (7) years prior to the date on which the accounting is requested.

The accounting will be in writing and will include disclosures made to or by Business Associate Subcontractors of JHR.

Each accounting of a disclosure will include the following:

1. The date of the disclosure;

2. The name of the entity or person who received the PHI and, if known, the address of such entity or person;
3. A brief description of the PHI disclosed;
4. A brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure; or in lieu of such statement:
    a. A copy of the individual's written authorization to use or disclose the PHI, or
    b. A copy of a written request for a disclosure required by the HHS Secretary to investigate or determine the Covered Entity's compliance with applicable laws and regulations.

JHR will act on the individual's request for an accounting not later than 60 days after receipt of the request by:

1. Providing the individual with the accounting requested, or
2. Extending the time to provide the accounting by no more than 30 days.
3. In the event that JHR extends the time to provide the accounting, within 60 days after receipt of the request, it will provide the individual with a written statement of the reasons for the delay and the date by which the Covered Entity will provide the accounting.
4. JHR will not extend the time to provide the accounting more than once.
    a. The first accounting to an individual in any 12-month period will be without charge.
    b. Any fee imposed by JHR for each subsequent request for an accounting by the same individual within the 12-month period will be cost-based.
    c. Upon imposing a fee, JHR will inform the individual in advance of the fee and provide the individual with an opportunity to withdraw or modify the request for a subsequent accounting in order to avoid or reduce the fee.

JHR will document and retain the following for a period of at least seven (7) years from the date of its creation or the date when it last was in effect, whichever is later:

1. The information required to be included in an accounting;
2. The written accounting that is provided to the individual;
3. The title of the persons or officer responsible for receiving and processing requests for an accounting by individual.

The Privacy Officer is responsible for responding to a request from an individual for an audit trail of instances when their PHI has been disclosed for purposes other than treatment, payment, or health care operations.

XXV. Alternate Means of Receiving Confidential Communications

A. Purpose

It is important to ensure that individuals can receive communications regarding their PHI in a means and location that the individual feels safe from unauthorized use or disclosure.

A Business Associate must permit individuals to request and must accommodate reasonable requests by individuals to receive communications of PHI from the Business Associate by alternative means or at least alternative locations.

B. Policy

JHR will take necessary steps to accommodate reasonable requests by individuals to receive confidential communications of PHI.

In complying with the first procedure of this section, JHR will provide confidential communications by alternative means or at alternative locations.

C. Definition

Employees with Appropriate Clearance: Workforce members who have been properly trained and designated to assist the Privacy Officer in handling individuals' requests for access to their PHI and inquiries about other Individual Rights.

D. Procedure

JHR will require individuals to make a request for a confidential communication in writing. See *Request for Alternate Methods of Communication* (General Forms).

JHR will not require an explanation from the individual as to the basis for the request as a condition of providing communications on a confidential basis.

When appropriate, JHR will condition the provision of a reasonable accommodation on information as to how payment, if any, will be handled, and specification of an alternative address or other method of contact.

1. An alternative means or location will be designated on a case-by-case basis that is satisfactory to both JHR and the individual before communication of PHI is made.
2. The Privacy Officer, using professional judgment and considering all relevant factors, will be responsible for deciding the alternative means or location to communicate PHI to an individual.

Once it is determined that use or disclosure is appropriate, employees with appropriate access clearance will access the individual's PHI using proper access and authorization procedures.

The requested PHI will be delivered to the individual in a secure and confidential manner, such that the information cannot be accessed by employees or other persons who do not have appropriate access clearance to that information.

Employees will appropriately document the request and delivery of the PHI.

In the event that the identity and legal authority of an individual or entity requesting PHI cannot be verified, employees will refrain from disclosing the requested information and report the matter to the Privacy Officer in a timely manner.

E. Enforcement

Knowledge of a violation or potential violation of this policy will be reported directly to the Privacy Officer.

Additional Policies and Procedures for the JHR Health Plan

JHR provides a Health Plan to its employees; therefore, there are additional specific requirements regarding protecting employee health data relative to the Plan.

Note: All the requirements that pertain to protected client data (PII and PHI) also apply to protected employee data (PHI).

XXVI. Notice of Privacy Practice for Employees

A. Overview

45 CFR §164.520 requires that notice be given to individuals of the use and disclosure of PHI as well as the individual's rights and covered entities' legal duties with respect to PHI.

B. Purpose

This policy is designed to give guidance and to ensure compliance with all laws and regulations regarding the provision of the notice of use of PHI by health plan providers.

C. Applicability

This policy applies to all JHR employees who participate in the JHR Health Plan.

D. Special Definitions

JHR Health Plan: the health insurance plan provided by JHR to its employees and administered by the Benefits Administrator

E. Policy

JHR will provide a formal notice to individuals regarding the use or disclosure of PHI pursuant to 45 CFR §164.520. This will be provided in a separate document entitled Notice of Privacy Practices.

The provision of the notice given to individuals regarding the use and disclosure of PHI pursuant to 45 CFR §164.520 will comply with the policies and procedures described herein.

The Notice will be provided to health plan participants as follows:

1. No later than the date of the activation of health insurance coverage;
2. Upon request;
3. On or after the effective date of a revision;
    a. Posted in a clear and prominent place within the Company
    b. Automatically and concurrently for electronic notices, when the individual's first inclusion in health care coverage is delivered electronically. The employee who

is the recipient of electronic Notice will be permitted to retain the right to obtain a paper copy of the notice from JHR upon request.

JHR will prominently post its Notice on any employee web sites that it maintains that provide information about its health care services or benefits, and will make the Notice available electronically through the web site.

When providing the Notice to an individual by email, JHR will:

1. Ensure that the individual has agreed to electronic Notice and such agreement has not been withdrawn.
2. Provide a paper copy of the Notice to the individual if JHR knows that an email transmission of the electronic notice has failed.

JHR will document compliance with and maintain the Notice by retaining copies of the Notices issued by JHR for a period of at least seven (7) years from the date of its creation or the date when it last was in effect, whichever is later.

F. Enforcement

Knowledge of a violation or potential violation of this policy must be reported directly to Barry Cohn, our Privacy Officer.

XXVII. Individual Rights to PHI—Requesting Restriction on Uses and Disclosures

A. Overview

The Health Insurance Portability and Accountability Act (HIPAA) requirements provide an individual with the right to request restrictions to the use and disclosure of his or her PHI. While Covered Entities are not required to permit the requested restrictions, they are required to permit the request. If the Covered Entity agrees to the requested restrictions, the Covered Entity may not make uses or disclosures that are inconsistent with such restrictions unless such uses or disclosures are mandated by law. This provision does not apply to health care provided to an individual on an emergency basis.

B. Purpose

To provide information to JHR employees participating in the JHR Health Plan regarding restrictions on the uses and disclosures of their PHI.

C. Applicability

This policy applies to all JHR employees participating in the JHR Health Plan.

D. Policy

JHR will allow an individual to request that uses and disclosures of their PHI be restricted.

Upon agreeing to such restriction, the Company will not violate such restriction except as specified within this policy and procedure.

The Company is not required to honor an individual's request in the following situation(s):

1. When the individual who requested the restriction is in need of emergency treatment and the restricted PHI is needed to provide the emergency treatment.
2. If restricted PHI is disclosed to a health care provider for emergency treatment, JHR will request that such health care provider not further use or disclose the information.

If the Company agrees to an individual's requested restriction, the restriction does not apply to the following uses and disclosures:

1. To an individual accessing their own PHI;
2. To an individual requesting an accounting of their own PHI;

Instances for which consent, an authorization, or opportunity to agree or object is not required, such as judicial and administrative purposes; health oversight; research, law enforcement; public health; to avert a serious threat to health and safety; cadaveric organ, eye, or tissue donation; decedents; Workers' Compensation; victims of abuse, neglect, or domestic violence; specialized government functions; required by law.

JHR will terminate its agreement to a restriction in the following situations:

1. The individual agrees to or requests the termination in writing;
2. The individual orally agrees to the termination and the oral agreement is documented;
3. The JHR informs the individual that it is terminating its agreement to a restriction. Such termination is only effective with respect to PHI created or received after it has so informed the individual.

JHR will document and retain the restriction for a period of at least seven (7) years from the date of its creation or the date when it last was in effect, whichever is later.

XXVIII. Reviewing a Denial to Access PHI

A. Overview

JHR recognizes that individual rights are a critical aspect of maintaining quality service and is committed to allowing individuals to exercise their rights under 45 CFR §164.524 and other applicable federal, state, and/or local laws and regulations.

B. Purpose

To support this commitment, JHR will maintain and update, as appropriate, written policies and procedures to provide guidance on employees and organizational responsibilities with respect to the rights of individuals regarding their PHI. However, situations may arise when agency employees must make a determination to deny an individual access to their PHI, in accordance with applicable laws and regulations. In certain circumstances, individuals may

request that the denial be reviewed. The policies and procedures herein have been established to assist personnel in such a review.

C. Applicability

This policy applies to all JHR employees participating in the JHR Health Plan.

D. Policy

JHR will take necessary steps, in a timely and professional matter, to address individual requests to access, inspect, and/or obtain a copy of their PHI that is maintained in a designated record set.

JHR will adhere to procedures pertaining to access to PHI contained herein when denying access, inspection, or copying of PHI.

JHR will adhere to the following procedures when reviewing a denial to access PHI.

The Company will review a denial for access to PHI when requested by the individual (use Request/Denial to Inspect and Copy form), in the following situations:

1. A licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to endanger the life or physical safety of the individual or another person;
2. The PHI makes reference to another person (unless such other person is a health care provider) and a licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to cause substantial harm to such other person; or
3. The request for access is made by the individual's personal representative and a licensed health care professional has determined, in the exercise of professional judgment, that the provision of access to such personal representative is reasonably likely to cause substantial harm to the individual or another person.
4. All denial reviews will be conducted by a licensed health care professional who is designated by the Company to act as a reviewing official and who did not participate in the original decision to deny.
5. The designated reviewing official will be determined on a case-by-case basis by the Privacy Officer.
6. JHR personnel with appropriate access clearance will promptly refer a request for review to the designated reviewing official.
7. The designated reviewing official will determine, within a reasonable period of time, whether or not to deny the access requested based on the applicable standards.
8. Our Privacy Officer or designee, will promptly provide written notice to the individual of the determination of the designated reviewing official and take other action as required to carry out the designated reviewing official's determination.

This policy and procedure will be documented and retained for a period of at least seven (7) years from the date of its creation or the date when it last was in effect, whichever is later.

Knowledge of a violation or potential violation of this policy must be reported directly to the Privacy Officer.

XXIX. Individual Rights to PHI—Accepting Requests for Amendments to PHI

A. Overview

According to 45 CFR §164.526, individuals have the right to request an amendment or correction to their Protection Health Information. Entities have the right to deny the request to amend or correct PHI. Unless the individual provides a reasonable basis to believe that the originator of PHI is no longer available to act on the requested amendment, this provision applies to PHI created by the covered entity.

B. Purpose

For both of those situations, JHR has created policies and procedures to address the issue and to comply with any applicable laws.

C. Applicability

This policy applies to all JHR employees participating in the JHR Health Plan.

D. Policy

JHR will provide for an individual to request an amendment to their PHI or a record in a designated record set for as long as the information is maintained in the designated record set.

1. JHR will allow an individual's request to amend PHI that was not created by the Company if provided a reasonable basis to believe that the originator of the information is no longer available to act on the request.
2. JHR Benefits Administrator will be responsible for receiving, processing, and responding to requests for amendments to PHI.
3. All individual requests for amendments to protected or other health information will be in writing.
4. JHR Benefits Administrator will inform the individual that it requires individuals to make requests in writing.
5. Individuals will document the reason(s) to support the requested amendment.
6. The request will be referred to a designated health care professional for review. This health care professional will be selected by JHR on a case-by-case basis.

An individual's request for amendment may be denied if the requested PHI or record:

1. Was not created by the Company;
2. Is not part of the designated record set;
3. Would not be available for inspection under the requirements for individual rights to access PHI; or
4. Is accurate and complete.

If the requested amendment is denied, JHR will follow the procedures outlined in Denying Requests for Amendment to PHI.

1. JHR Benefits Administrator will inform the individual no later than 60 days after receipt of such a request if the amendment is accepted.
2. The time period for the action by the Company will be extended by no more than 30 days.
3. If the time period for action is extended, JHR Benefits Administrator will, within 30 days after receipt of the request, provide the individual with a written statement of the reasons for the delay and the date by which the Company will complete action on the request.
4. The time period for action will not be extended more than once.

If the requested amendment is accepted, JHR Benefits Administrator will:

1. Make the appropriate amendment; or
2. Arrange to have the necessary health care professional make the amendment.

Upon accepting and completing a requested amendment, Renee Cohn or designee will perform the following tasks:

1. Inform the individual, in a timely manner, and obtain the individual's identification and agreement to have the Company notify the relevant persons with which the amendment needs to be shared
2. Make reasonable efforts to inform and provide the amendment within a reasonable time to persons identified by the individual as needing the amendment;
3. Make reasonable efforts to inform and provide the amendment within a reasonable time to persons, including business associates that the Company knows have the affected PHI and that may have relied, or could foreseeably rely, on such information to the detriment of the individual.

In completing the amendment, Renee Cohn or designee will, at a minimum, identify the affected information in the designated record set and append or otherwise provide a link to the location of the amendment.

In the event that another covered entity notifies the Company of an amendment to an individual's PHI, Renee Cohn or designee will amend the respective information by, at minimum, identifying the affected information in the designated record set and appending or otherwise providing a link to the location of the amendment.

This policy and procedure will be retained for a period of at least seven (7) years from the date of its creation or the date when it last was in effect, whichever is later.

XXX. Denying Requests for Amendments to PHI

A. Purpose

Under HIPAA, individuals have the right to request an amendment or correction to their PHI, or a record about the individual for as long as that information is contained in a designated record set. Entities have the right to deny the request to amend or correct PHI. Unless the individual provides a reasonable basis to believe that the originator of PHI is no longer available to act on the requested amendment, this provision applies to PHI created by the Covered Entity. JHR has created policies and procedures to address this issue and to comply with any applicable laws.

B. Policy

JHR permits an individual to request an amendment or correction to their PHI or a record in a designated record set for as long as the information is maintained in the designated record set.

JHR may deny an individual's request for amendment if it determines that the requested PHI or record:

1. Was not created by JHR, unless the individual provides a reasonable basis to believe that the originator or PHI is no longer available to act on the requested amendment;
2. Is not part of the designated record set;
3. Would not be available for inspection under the requirements for individual rights to access PHI; or
4. Is accurate and complete.

C. Procedure

Renee Cohn or designee will be responsible for receiving, processing, and responding to requests for amendments to PHI.

All individual requests for amendments to protected or other health information will be in writing, and directed to Renee Cohn.

1. Individuals must document the reason(s) to support the requested amendment.
2. The request will be referred to a designated health care professional for review, who will be selected by JHR on a case-by-case basis.
3. Renee Cohn or designee will inform the individual no later than 60 days after the individual's request if the amendment is denied.
    a. On occasions where JHR needs more than 60 days to make a decision, the time period for the action will be extended by no more than 30 days provided that:
    b. JHR will provide the individual with a written statement of the reasons for the delay and the date by which JHR will complete the action on the request; and
    c. JHR will not extend the time period for action more than once.

4. Upon denying an amendment in whole or in part, JHR will provide the individual with a written denial in accordance with the time frames outlined above.

a. The denial will be written in plain language and will contain the following:

1) The basis for denial;
2) The individual's right to submit a written statement disagreeing with the denial;
3) A description of how the individual may file such a statement;
4) A description of how the individual may file a complaint to JHR pursuant to its complaint procedures including the name or title and telephone number of the contact person or office designated to receive such complaints.
5) A description of how the individual may file a complaint with the Department of Health and Human Services;
6) The following statement: "*If individual does not submit a statement of Disagreement, then individual may request that JHR to provide the individual's request for amendment and the denial with any future disclosures of the Protected Health Information that is the subject of the amendment.*"

5. If the individual provides a statement of disagreement, JHR will prepare a written rebuttal to the individual's statement of disagreement.
   a. JHR will provide the individual with a copy of the above rebuttal.
   b. JHR will append or otherwise link the following to the designated record set or PHI that is the subject of the disputed amendment:
      1) The individual's request for an amendment;
      2) The denial of the request;
      3) The individual's statement of disagreement, if any; and
      4) JHR rebuttal, if any.

Any subsequent disclosures of the PHI to which an individual's written disagreement relates will include the following:

1. The material appended as described above; or
2. An accurate summary of any such information.

If the individual has not submitted a written statement of disagreement, JHR will include the individual's request for amendment and JHR's denial, or an accurate summary of such information, with any subsequent disclosure of the PHI only if the individual has requested such action.

This policy and procedure will be retained for a period of at least seven (7) years from the date of its creation or the date when it last was in effect, whichever is later.

XXXI. Identifying when Routine Health Information Becomes PHI

A. Overview

JHR is committed to ensuring the privacy and security of covered employee health information.

B. Purpose

To support this commitment, JHR will ensure that the appropriate steps are taken to properly identify and secure individuals' PHI as required under 45 CFR Part 164 and other applicable federal, state, and/or local laws and regulations.

C. Applicability

This policy applies to all JHR employees participating in the JHR Health Plan.

D. Policy

The following information will be designated as PHI: Any health information, including demographic information collected from an individual, transmitted or maintained in any form or medium, that:

1. Is created or received by a health care provider, health plan, JHR, or health care clearinghouse; and
2. Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and
    a. That identifies the individual; or
    b. With respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Routine health information meeting the above definition will be automatically designated as PHI immediately upon its creation or receipt by JHR.

The Company will adhere to all applicable laws, regulations, policies, and procedures when maintaining, using, and disclosing PHI.

In the event of a discrepancy, the following persons, respectively, will be responsible for designating routine health information as PHI:

1. Renee Cohn, Benefits Administrator
2. Barry Cohn, Privacy Officer

XXXII. Disclosing and Requesting only the Minimum Amount of PHI Necessary

A. Overview

JHR is committed to ensuring the privacy and security of covered employee health information.

B. Purpose

To support the Company's commitment to covered employee confidentiality, JHR will ensure that the appropriate steps are taken to disclose only the minimum amount of PHI

necessary to accomplish the particular use or disclosure, as required under 45 CFR §164.502(b), and other applicable federal, state, and/or local laws and regulations.

C. Applicability

This policy applies to all JHR employees participating in the JHR Health Plan.

D. Policy

The Benefits Administrator or designee will follow proper procedures to ensure that only the minimum amount of covered employee health information necessary to accomplish the specific purpose of a use or disclosure is actually used or disclosed.

Employee records will be stored on the P drive on our server and in file cabinets in the locked office of Ronni Kopulsky, Human Resources Administrator.

Employees will request only the minimum amount of covered employee health information necessary to accomplish the specific purpose of the request.

This policy does not apply to the following uses or disclosures:

1. Disclosure to or requests by a provider for treatment;
2. Uses or disclosure made to the individual who is the subject of the information;
3. Uses or disclosure pursuant to an authorization;
4. Disclosure made to the Department of Health and Human Services;
5. Uses or disclosure required for compliance with applicable laws and regulations.

All proposed uses or disclosures of covered employee health information will be reviewed by the Benefits Administrator who has an understanding of the Company's privacy policies and employees, and sufficient expertise to understand and weigh the necessary factors.

The Company will only use, disclose, or request an entire record when the entire record is specifically justified as being reasonably necessary to accomplish the purpose of the use, disclosure, or request.

Within the Company, only the Benefits Administrator and those employees documented in our Risk Assessment have access to employee PHI on a routine basis to appropriately accomplish their duties and responsibilities:

1. Access to PHI will be reasonably limited to that described above by utilizing access control systems.
2. Requests for disclosures of PHI will be reviewed on an individual basis in accordance with criteria listed in the policy.

The Benefits Administrator or designee may reasonably rely on requests by:

1. Public health and law enforcement agencies in determining the minimum necessary information for certain disclosures;
2. Other covered entities in determining the minimum necessary information for certain disclosures; or;

3. By a professional who is a member of its workforce or is a business associate of the Company for the purpose of providing professional services to the Company, if the professional represents that the information requested is the minimum necessary for the stated purpose.

E. Enforcement

Knowledge of a violation or potential violation of this policy must be reported directly to the Privacy Officer.

XXXIII. PHI – Disclosure of Genetic Information (GINA)

A. Overview

HIPAA requires a covered entity to obtain authorization to use or disclose PHI for all purposes not explicitly permitted under the regulations: 45 CFR §164.508(b)(4); §164.508(c); §164.508(d). Included in the definition of health information is genetic information: 45 CFR §160.103. Title I of the Genetic Information Nondiscrimination Act of 2008 (GINA) prohibits health insurers and health plans from discriminating against beneficiaries on the basis of genetic information. However, certain exceptions apply for long-term care policies, as such.

B. Purpose

JHR has created the following policies and procedure to comply with all applicable laws and regulations.

C. Applicability

This policy applies to all JHR employees participating in the JHR Health Plan.

D. Policy

JHR will include a statement in its Notice of Privacy Practices that it will not use or disclose genetic information of an individual for underwriting purposes.

The Benefits Administrator or designee will follow proper procedures to ensure that genetic information not released for a health insurer's or health plan's underwriting purposes, unless it is a long-term care policy.

The Company will not disclose the following health information to a health insurer or health plan for the purpose of underwriting:

1. Information related to genetic tests of an individual;
2. The genetic tests of family members of an individual;
3. The manifestation of a disease or disorder in family members of an individual. "Manifestation" means a disease, disorder, or pathological condition that an individual has been or could reasonably be diagnosed with by a health care professional with appropriate training and expertise in the field of medicine involved:

4. Any request for, or receipt of, genetic services, or participation in clinical research which includes genetic services, by an individual or any family member of the individual.

The Company may disclose such information if it is a long-term care policy.

XXXIV. Conditioning Services or Eligibility on the Provision of an Authorization to Disclose PHI—Health Plans

A. Overview

Generally, JHR may not condition the provision of treatment, payment, enrollment, or eligibility for benefits on the provision of an authorization to use or disclose an individual's PHI. However, certain exceptions apply.

B. Purpose

JHR is committed to ensuring that all covered employees receive the highest quality of care and services, and therefore will take necessary steps to comply with applicable laws and regulations regarding the conditioning of services on an authorization.

C. Applicability

This policy applies to all JHR employees participating in the JHR Health Plan.

D. Policy

JHR may condition the following on the provision of an authorization requested by the Company:

1. Enrollment in health plan or eligibility for benefits if the authorization is requested by JHR prior to an individual's enrollment, and if the authorization is sought for the health plan's eligibility or enrollment determinations relating to the individual or for its underwriting or risk rating determinations;
2. Payment of a claim for specified benefits if the disclosure is necessary to determine payment of such claim;
3. The provision of health care that is solely for the purpose of creating PHI for disclosure to a third party for the disclosure of the PHI to such third party.

JHR will not condition enrollment, eligibility, or payment of a claim on the provision of an authorization for the use or disclosure of psychotherapy notes.

All requests for disclosures of PHI that require authorization will be directed to JHR Benefits Administrator.

1. JHR Benefits Administrator, in close consultation with the requesting party, will determine the nature of the request and whether it is necessary to condition payment or services on obtaining the authorization. The policies stated herein will be the deciding factors.

2. If such conditions are determined necessary, the JHR Benefits Administrator will inform the enrollee, potential enrollee, or applicable provider, including the reason for the conditioning of services.

XXXV. Restricting Disclosure of PHI to Health Plans

A. Purpose

The HITECH Act sets forth certain circumstances in which a covered entity now must comply with an individual's request for restriction of disclosure of his or her PHI (PHI). Specifically, section 13405(a) of the HITECH Act requires that when an individual or their designated representative requests a restriction on disclosure pursuant to §164.522, the covered entity must agree to the requested restriction unless the disclosure is otherwise required by law.

B. Applicability

This policy applies to all JHR employees participating in the JHR Health Plan.

C. Policy

JHR will agree to the requested restriction of disclosure by any covered employee, guardian or personal representative of certain PHI to a health plan for payment or health care operation, for items or services that have been paid in full and out-of-pocket (unless the disclosure is otherwise required by law).

JHR will take all necessary steps to honor and comply with an individual's request for limitations and restrictions of PHI.

JHR will require the covered employee to request the restriction by completing the Request for Limitations and restrictions of PHI.

JHR will agree to the requested restriction (unless the disclosure is otherwise required by law), if:

1. The request for restriction is on disclosures of PHI to a health plan for the purpose of carrying out payment or health care operations, and if
2. The restriction applies to PHI that pertains solely to a health care item or service for which the health care provider has been paid out-of-pocket, in full.