HIPAA PRIVACY POLICIES & PROCEDURES

USES AND DISCLOSURES OF PHI PERMITTED FOR REASONS OTHER THAN TREATMENT, PAYMENT AND HEALTH CARE OPERATIONS, AND WITHOUT INDIVIDUAL AUTHORIZATION

- 1. **POLICY:** In the following limited instances, which are in addition to Treatment, Payment and Health Care Operations, the Company is permitted to use or disclose PHI without an individual's authorization.
- 2. **PROCEDURE**:
  - 2.1 **USES AND DISCLOSURES THAT REQUIRE AN OPPORTUNITY FOR THE INDIVIDUAL TO AGREE OR TO OBJECT.**
    - (a) **Disclosures to Designated Individuals.** Company employees authorized to access PHI, without written authorization from the individual, may use or disclose PHI to any person *identified* by the individual, such as a family member or close friend, of any PHI directly relevant to such person's involvement with the individual's care or payment related to the individual's care as long as the following conditions are met:
      - (i) If the individual is present for, or otherwise available prior to, this type of use or disclosure and has the capacity to make health care decisions, Company employee will authorize the use or disclosure of the PHI if he or she: (1) obtains the individual's agreement; (2) provides the individual with the opportunity to object and the individual does not do so; or (3) the Company employee reasonably infers from the circumstances and based on professional judgment, that the individual does not object.
      - (ii) If the individual is not present for, or it is not possible to give the individual the opportunity to agree to the use or disclosure because of incapacity or an emergency, the Company employee will determine, based on professional judgment, whether the use or disclosure is in the best interest of the individual. If use or disclosure is made, only the PHI that is directly relevant to the third person's involvement with individual's health care or payment for health care will be used or disclosed.
    - (b) **Disclosures for Notification Purposes.** Company employees authorized to access PHI, without written authorization from the individual, may use or disclose PHI to notify, or assist in notifying (including identifying or locating), a family member, a personal representative of the individual, or another person responsible for the individual's care, of the individual's location, general condition or death. The Company employee also may use or disclose PHI to a public or private entity that is authorized by law or by its charter to assist in disaster relief, for the purpose of coordinating with such entities to notify (including identifying or locating) relatives or those close to the individual, of the individual's location, general condition or death.
  - 2.2 **USES AND DISCLOSURES FOR WHICH AN INDIVIDUAL'S AUTHORIZATION OR OPPORTUNITY TO AGREE OR OBJECT ARE NOT REQUIRED.**
    - (a) **Uses and Disclosures.** In the following circumstances, Company employees authorized to access PHI may use or disclosure of PHI without the individual's written authorization, and without giving the individual the

right to agree or object. To the extent not covered below, the Company will comply with additional requirements in the HIPAA Privacy Rule, as applicable.

- (i) To the appropriate governmental or judicial authority as required by law in situations of abuse, neglect or domestic violence; in the course of any judicial or administrative proceeding; for law enforcement purposes to a law enforcement official as required by law. The Company will only make such disclosures to the extent they are required by law and the use or disclosure complies with and is limited to the relevant requirements of the law.
- (ii) To the appropriate public health authority that is authorized by law to collect or receive PHI for the purpose of preventing or controlling disease (including notifying infected individuals when authorized by law), injury or disability; or to receive reports of child abuse or neglect.
- (iii) To persons or entities subject to the jurisdiction of the Food and Drug Administration ("FDA") to meet the reporting requirements of the FDA, such as submitting adverse event reports, tracking products for recalls, and conducting post-marketing surveillance to track compliance. The Company will comply with the additional requirements in the HIPAA Privacy Rule, as applicable.
- (iv) To an employer to comply with OSHA requirements related to medical surveillance and work related injuries, and to persons as authorized by workers' compensation laws.
- (v) To health oversight agencies for oversight activities authorized by law, *e.g*., fraud and abuse audits, investigations and inspections; licensure or disciplinary actions; and civil, administrative or criminal proceedings. The Company will comply with the additional requirements in the HIPAA Privacy Rule, as applicable.
- (vi) To coroners and medical examiners, and funeral directors, the PHI which is necessary to permit those persons to carry out their duties consistent with applicable law.
- (vii) To organ procurement organizations for donation purposes.
- (viii) For research purposes, provided that an Institutional Review Board or privacy board (as described in the Privacy Rule) approves the waiver of individual authorization.
- (ix) To appropriate persons and consistent with applicable laws and standards of ethical conduct, when the Privacy Officer believes, in good faith, that it is necessary to use or disclose the PHI to prevent or lessen a serious and imminent threat to the health and safety of a person or the public, or to assist law enforcement in identifying or apprehending an individual.
- (x) To military and veterans authorities, national security and intelligence sources, protective services for the President, correctional institutions and other custodial law enforcement, and Department of State for the purposes detailed in the HIPAA Privacy Rule.

- (b) **Verification Procedures.** Before making any such disclosures, the Company employee will verify the identity of the person requesting the PHI and the authority that person has to have access to the requested PHI.
  - (i) In the normal course, the Company employee will obtain the requisite verification by requiring the requester to send their request in writing on official stationery. The Company employee may also require the requester to provide any other documentation that he/she deems necessary, using professional judgment, to verify the authenticity of the requester.
  - (ii) If the request is made to the Company employee in person, the Company employee will require the requester to present sufficient official identification, such as a badge or official credential, to verify the requester's identity and authority.

        - (iii) If the request is made pursuant to a legal process, such as a subpoena, warrant or court order, the Company employee may rely on the veracity of that request.
        - (iv) If the Company employee determines, using professional judgment, that there is an emergency situation that does not allow for a written exchange, the Company employee may verify the requester's identity by calling the requester back. If this occurs, the Company employee must document the exchange and the nature of the emergency, and maintain the documentation in accordance with Company's policy on record retention and documentation.
    - 2.3 **DISCLOSURES TO BUSINESS ASSOCIATES.** The Company may disclose PHI to Business Associates after entering into a Business Associate Agreement, and consistent with Company's policy on business associate relationships.
    - 2.4 **DISCLOSURES BY WHISTLEBLOWERS AND WORKFORCE MEMBER CRIME VICTIMS.** A Company employee with access to PHI will not be disciplined if he/she discloses PHI to a health oversight agency or to an attorney only if he/she believes, in good faith, that the Company has engaged in unlawful conduct. If that employee believes that he/she should disclose PHI about a suspected perpetrator of a criminal act to a law enforcement official, if feasible, that employee should first discuss that disclosure with the Privacy Officer.

USES AND DISCLOSURES OF PHI THAT ARE REQUIRED OR PERMITTED BY THE PRIVACY RULE, OR PERMITTED BY AUTHORIZATION

- 1. **POLICY**: This Policy summarizes the uses and disclosures of patient protected health information ("PHI") that are required or permitted by the Health Insurance Portability and Accountability Act ("HIPAA") Privacy Rule, or permitted by authorization.
- 2. **PROCEDURES**
    - 2.1 **REQUIRED USES AND DISCLOSURES**. Company is required to use or disclose PHI in the following circumstances:
        - (a) **Individual Access**. To the individual who is the subject of the PHI contained in the designated record set, provided the individual's identity is reasonably verified by the Company employee, or if the request is to inspect and/or copy his/her PHI, Company follows procedures set forth in Company's policy regarding access to PHI.
        - (b) **Access by Secretary of HHS.** To the Secretary of the Department of Health and Human Services ("HHS") when the Secretary is investigating a complaint or monitoring compliance. The Company will verify the identity of the HHS requester**.**
    - 2.2 **DISCLOSURES TO FAMILY MEMBERS.**
        - (a) **Spousal Access**. A spouse must typically sign a HIPAA-compliant authorization releasing an individual's PHI to his or her spouse.
        - (b) **Parental Access**. Parents or guardians ("parents") are generally considered the personal representatives of unemancipated minors. As such, the Company generally responds to parental inquiries about their children's treatment and health care claims, and provides parents with access to the minors' PHI.
        - (c) **Emergency Access**. If a family member or close friend inquires on behalf of an individual who is being cared for by the Company or from whom it would be difficult to obtain an authorization, the Company may respond to that family member or close friend's inquiries. (This type of access does not require that the individual be incapacitated or unconscious.) However, before responding, the identity of the family member or close friend and the individual's identity must be verified. The PHI provided must be the minimum

necessary for the family member or close friend to ensure the individual receives the medical care he/she needs.

- 2.3 **USES AND DISCLOSURES OF PHI PERMITTED WHEN THE PATIENT IS DECEASED.** Company may disclose PHI of a deceased patient to a family member, other relative, close personal friend or other person previously identified by the patient as someone involved in the patient's care or payment for health care prior to the patient's death. PHI disclosed will be limited to what is *relevant* to the person's involvement in the patient's care. **NOTE**: if the Company has knowledge that the disclosure of PHI would be inconsistent with a preference previously expressed by the patient, the PHI requested will not be disclosed.
- 2.4 **USES AND DISCLOSURES PERMITTED FOR TREATMENT, PAYMENT OR HEALTH CARE OPERATIONS.** Company may use or disclose PHI for purposes of treatment, payment or health care operations *without* written authorization from the patient.
  - (a) **Treatment**. Company may use or disclose PHI for treatment purposes to assist any health care provider in that provider's treatment activities or to coordinate or manage with a health care provider to provide treatment for an individual so long as each entity has or had a relationship with the individual who is the subject of the protected health information being requested.
  - (b) **Payment**. Company may use or disclose PHI to obtain or provide reimbursement for the provision of health care. These payment activities must relate to an individual, and include: (i) billing, claims management, collection activities and related health care data processing; (ii) review of health care services with respect to medical necessity or coverage under a health plan; (iii) utilization review activities; and (iv) disclosure to consumer reporting agencies.
- 2.5 **USE AND DISCLOSURE OF PHI PERMITTED PURSUANT TO A VALID AUTHORIZATION**. Company will only use or disclose PHI to third parties for purposes other than treatment, payment or health care operations, or reasons other than those specified in the Privacy Rule as not requiring authorization or otherwise required by law, upon receipt of a valid, written authorization. Once a valid authorization is received, the Company will only use and disclose information consistent with the terms of the authorization. However, the standard authorization received by the Company will state that once disclosed, the PHI may no longer be protected, and that the information may be further disclosed by the recipient without any additional authorization from the individual. An individual may revoke, in writing, his or her signed authorization at any time, except to the extent that the Company has taken action in reliance on the authorization prior to revocation.
  - (a) Specific Instances for Which Authorization is Required Prior to Use or Disclosure:
    - b. Marketing: The company must obtain an authorization for any use or disclosure of protected health information for marketing, except: (i) Face-to-face communication made by the Company to the individual; (ii) A promotional gift of nominal value provided by Company; and (iii) Communications made to provide refill reminders or otherwise communicate about a drug or biologic that is currently being prescribed for a patient, provided that any payment received by Company in exchange for making the communication is "reasonably related" to Company's cost of making the communication. Costs are considered to be "reasonably related" if they cover direct and indirect costs to Company for making the communication, including the costs of labor, materials, and supplies, as well as capital and overhead costs.
  - (b) **Authorization Forms**. Authorization Forms must be signed prior to disclosing any PHI.

THE MINIMUM NECESSARY REQUIREMENT

- 1. **POLICY:** The Company applies the minimum necessary standard whenever it uses or discloses PHI to a third party, or requests PHI from another covered entity. This means that the Company makes reasonable efforts to limit the use or disclosure, or request of PHI to the minimum necessary to accomplish its intended purposes.
- 2. **PROCEDURE**
  - 2.1 **APPLICABILITY OF THE MINIMUM NECESSARY REQUIREMENT.** The Company will apply the minimum necessary standard to all uses and disclosures of PHI, except as follows:
    - (a) Disclosures to or requests by a health care provider for treatment purposes;
    - (b) Permitted and required disclosures to the individual who is the subject of the information;
    - (c) Uses or disclosures pursuant to a valid authorization executed by the individual;
    - (d) Disclosures made to the Secretary of HHS in accordance with the Privacy Rule; or
    - (e) Uses and disclosures required by law, and uses and disclosures that are required for compliance with the Privacy Rule.
  - 2.2 **IDENTIFICATION OF EMPLOYEES.**
  - (a) **Identified Employees.** The Company employees who need access to PHI are identified in Company's Policies on Personnel Designations and Limited Employee Access. No other Company employees may have access to PHI unless specifically authorized by the Privacy Officer.
  - (b) **Restrictions on Employee Access.** The Company employees who need access to PHI only have access to the PHI necessary for their job duties, unless specifically authorized by the Privacy Officer.
  - 2.3 **MINIMUM NECESSARY REQUIREMENT APPLIED TO USES AND DISCLOSURES OF PHI.**
    - (a) **Limited Data Sets.** A Limited Data Set is a limited set of identifiable patient information as defined by the HIPAA Privacy Rule, which may be disclosed to an outside party without a patient's authorization if certain conditions are met. The purpose of the use or disclosure may only be for research, public health, health care operations or by a business associate to create a Limited Data Set for the Company or the business associate.
      - (i) Limited Data Set information is information that excludes the following direct identifiers of the individual or the relatives, employers or household members of the individual:
        - (1) Names;
        - (2) Postal address information (except town, city, state and zip code may be used or disclosed);
        - (3) Telephone and Fax Numbers;
        - (4) Social Security numbers, medical record numbers, account numbers or certificate/license numbers;
        - (5) Vehicle identifiers and serial numbers, including license plate numbers;
        - (6) Device identifiers and serial numbers;
        - (7) Email Addresses, Web Universal Resource Locators (URLs) and Internet Protocol (IP) address numbers;
        - (8) Biometric identifiers (including finger- and voice-prints), and full-face photographic images and any comparable images.
      - (ii) Limited Data Set information may include an individual's town, city, state and zip code, and all elements of dates related to the individual (including birth date, admission date, discharge date and death date).
  - 2.4 **REQUESTS FOR PHI AND THE MINIMUM NECESSARY REQUIREMENT**. All requests for PHI initiated by the Company shall seek only the minimum necessary to accomplish the purpose for which the request is made.
  - 2.5 **LIMITATION REGARDING USING, DISCLOSING OR REQUESTING ENTIRE MEDICAL RECORD.** For all uses, disclosures, or requests to which the minimum necessary requirements apply, the Company will not use, disclose

or request an entire medical record, except when the entire medical record is specifically justified and Company has documented the specific justification.

Business Associate Relationships

- 1. **POLICY**: The Company ensures that its Business Associates, the entities that perform services for the Company and create, receive, maintain or transmit PHI that belongs to the Company in the course of providing such services, protect the privacy of the PHI and provide individuals with certain rights with respect to the PHI. After the Company obtains a Business Associate Agreement ("BAA") from a Business Associate, which provides that the Business Associate will protect the PHI and limit its use and disclosure of PHI, the Company discloses PHI to the Business Associate only to the extent necessary for the Business Associate to carry out its contractual duties.
- 2. **PROCEDURE**
    - 2.1 **BAA.** Before the Company discloses PHI to a Business Associate or permits a Business Associate to create, maintain or transmit PHI on its behalf, the Company enters into the required BAA**.** The Privacy Officer is responsible for assisting in identifying those vendors that require BAAs and ensuring that such BAAs are entered into. Upon execution, a copy of the BAA must be sent to the Privacy Officer.
    - 2.2 **MONITORING AND NON-COMPLIANCE.** ThePrivacy Officer monitors Business Associates' compliance with their obligations only if he/she has a reasonable belief that a Business Associate has violated its agreement. Any Company employee or Business Associate or agent who becomes aware that a Business Associate may be violating its obligations to the Company must immediately report such alleged violation to the Privacy Officer, who may investigate the matter and, if warranted, take reasonable steps to cure the violation.
        - (a) **Investigation**. The Privacy Officer may take the following steps as appropriate if he/she becomes aware of a possible violation of a BAA: (1) interview Company employees who may have knowledge of the alleged violation; (2) interview the Business Associate's employees who may have knowledge of the alleged violation; (3) collect any documentation from the Company or the Business Associate that relates to the alleged violation; (4) contact the Business Associate to obtain information related to the alleged violation; (5) review the documents that pertain to the alleged violation; and (6) take any other actions that the Privacy Officer deems appropriate.
        - (b) **Response If Violation Has Occurred.** If the Privacy Officer determines that the Business Associate has violated the agreement, the Privacy Officer may:
            - (i) sanction any Company employee involved with the violation;
            - (ii) request that the Business Associate sanction any of its employees who were involved with the violation;
            - (iii) coordinate with the Business Associate to perform a risk assessment for notification of Breach purposes and to send out or publish any necessary notifications of Breach in accordance with Company's breach notification policy and any relevant written agreements with the Business Associate;
            - (iv) mitigate any harmful effect that the Company knows of resulting from the improper use or disclosure of the PHI;
            - (v) take any remedial steps provided for by the BAA; and/or

- (vi) work with the Business Associate to cure the violation and ensure such violation will not occur again. But, if the reasonable steps taken to cure the violation are unsuccessful, the Company may terminate the contract with the Business Associate, if feasible. **NOTE**: If termination is not feasible because there are not other viable business alternatives for the Company, the Company will consult with the Privacy Officer regarding available remedies under current Privacy Rule provisions.

DE-IDENTIFICATION POLICY

- 1. **POLICY:** The Company may use or disclose de-identified information, which is health information that does not identify an individual and is not PHI, without obtaining the individual's authorization. If the Company re-identifies information, it becomes PHI that is treated in accordance with the Privacy Rule and the Company's Policies and Procedures.
- 2. **PROCEDURE**
  - 2.1 **CREATION OF DE-IDENTIFIED INFORMATION.** The Company may create, or direct a Business Associate to create, de-identified information pursuant to the following guidelines.
    - (a) **Expert Method.** The Company de-identifies information by designating an expert, who has the appropriate knowledge of, and experience with, statistical and scientific principles and methods for rendering information not individually identifiable and applies such principles and methods to:
      - (i) Determine that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is the subject of the information; and
      - (ii) Document the methods and results of the analysis that justify such determination.
    - (b) **Removal of Identifiers Method.** The Company de-identifies PHI by removing the following individual identifiers related to individuals, their relatives, household members and employers, and ensuring, to the extent practicable, that the de-identified information cannot be used, alone or in combination with other information, to identify the individual who is the subject of the information:
      - (i) Names;
      - (ii) All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, that complies with the additional requirements of §164.514(b)(2)(i)(B);
      - (iii) All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;
      - (iv) Telephone numbers, fax numbers, and e-mail addresses;
      - (v) Social Security numbers, medical record numbers and account numbers;
      - (vi) Certificate/license numbers, vehicle identifiers and serial numbers, including license plate numbers, and device identifiers and serial numbers;
      - (vii) Web Universal Resource Locators (URLs), and Internet Protocol (IP) address numbers;
      - (viii) Biometric identifiers, including finger-and-voice prints, full-face photographic images and any comparable images; and
      - (ix) Any other unique identifying number, characteristic or code.

        - (x) Business Associates. The Company may disclose PHI to a Business Associate for de-identification, whether or not the de-identified information is to be used by the Company.
    - 2.2 **RE-IDENTIFICATION.** The Company may assign a code to de-identified information in order to later re-identify the information. Re-identified information and the re-identification code is PHI that may be disclosed and used only as permitted by the Privacy Rule and these Policies and Procedures. In addition, the Company will make a reasonable effort to limit the use, disclosure or request of re-identified PHI to the minimum necessary to accomplish the intended purpose in accordance with Company's minimum necessary policy.

COMPLAINTS

- **1. POLICY:** All individuals or parties, including Company employees and their dependents, who believe that privacy rights have been violated or who have a complaint arising under the Privacy Rule or these Policies and Procedures have the right to make an inquiry or complaint with the Company, or with the Secretary of Health and Human Services.
- **2. PROCEDURE TO FILE A COMPLAINT WITH THE COMPANY**
    - 2.1 **Reporting**. Individuals may report a complaint to the Company as follows:
        - An individual must make a complaint in writing to the Privacy Officer. The complaint must include the individual's name, address and the last four digits of his/her Social Security number, a description of the individual's complaint, and any documentation that supports his/her complaint. The Privacy Officer is available to discuss any questions the individual might have about the complaint procedure. An individual may contact the Privacy Officer at the following address and phone number:
            - ***Heather Sims,***
              203 N Mathewson
            - ***Wichita, Ks, 67214***
              3165196859
    - 2.2 **Investigation.** When an individual makes a complaint, the Privacy Officer will promptly investigate the circumstances related to the report.
        - a. **Reasonable Steps.** The Privacy Officer may take the following steps, as he/she deems appropriate, to investigate the alleged violation: (1) interview the individual complainant; and (2) interview the Company employees or Business Associates who may have knowledge of the alleged violation and review any relevant documents that pertain to the alleged violation. These procedures are not exclusive and the Privacy Officer may take any steps he/she deems necessary to investigate the complaint.
        - b. **Confidentiality**. Confidentiality will be maintained throughout the investigative process to the extent practicable and consistent with the need to undertake a full investigation.
        - c. **Results of Investigation.** If the Privacy Officer determines that a violation has occurred, he/she may take action as is necessary and supported by the facts, including:
            - (i) sanctioning the Company employees who have acted improperly, and requesting that any Business Associate employees who have acted improperly be sanctioned by the Business Associate;
            - (ii) working with a Business Associate to cure any violation by the Business Associate, or terminating the Business Associate Agreement if no cure is possible;

        - (iii) mitigating any harmful effect that the Company knows of resulting from the improper use or disclosure of PHI as per Company's mitigation policy.
    - d. **Determination.** Upon completion of the investigation, appropriate action will be taken, as necessary and supported by the facts.
- 2.3 **PROCEDURE TO FILE A COMPLAINT WITH SECRETARY OF HHS.**
    - a. **Filing Complaint.** To file a complaint with the Secretary of HHS, the individual should send a letter to 200 Independence Avenue, S.W., Washington, D.C. 20201, call 1.877.696.6775 or visit www.hhs.gov/ocr/privacy/hipaa/complaints.
    - b. **Timing.** The complaint must be filed within one hundred and eighty (180) days of the individual's knowledge of the alleged violation.
- 2.4 **DOCUMENTATION.** Information related to each complaint received by the Company and the disposition of each complaint will be documented by the Company, and that documentation will be retained for six (6) years in accordance with Company's record retention policy.

PERSONNEL DESIGNATIONS

- 1. **POLICY:** The Company has designated a Privacy Officer.
- 2. **PROCEDURE**
    - 2.1 **PRIVACY OFFICER DESIGNATION.** The Company has designated a Privacy Officer who is responsible for overseeing and directing the development and implementation of the Company's Privacy Policies and Procedures in compliance with the Privacy Rule.
        - (a) **Designated Privacy Officer.** The Company has designated the following Privacy Officer:
        - ***Heather Sims,***
          203 N Mathewson
        - ***Wichita, Ks, 67214***
          3165196859
        - (b) **Duties and Responsibilities.** The Privacy Officer is responsible, either directly or by his/her delegated authority, for monitoring and ensuring the Company's compliance with the Privacy Rule requirements and these Policies and Procedures. The Privacy Officer:
            - (i) Oversees the development and implementation of HIPAA compliance processes, and supervises the day-to-day aspects of compliance with the Privacy Rule;
            - (ii) Coordinates with Company employees to identify HIPAA non-compliant processes and systems, and to develop and implement those changes necessary to ensure all processes and systems are HIPAA compliant;
            - (iii) Serves as central liaison for internal HIPAA systems and processes, and for external business partners and vendors involved in HIPAA systems and processes;
            - (iv) Communicates HIPAA compliance assessment findings, including cost and risk exposure, to the Company and impacted personnel;
            - (v) Tracks action items;
            - (vi) Prepares budgets for HIPAA compliance as necessary and appropriate;
            - (vii) Responds to inquiries from individuals, government officials and other third parties regarding uses and disclosures of PHI, and promptly renders determinations in response to such inquiries and requests;
            - (viii) Oversees workforce training on HIPAA compliance;

        - (ix) Maintains a current list of Business Associates;
        - (x) Ensures that the Company's Notice of Privacy Practices is timely disseminated to individual customers;
        - (xi) Reviews and revises the Notice of Privacy Practices to reflect any changes to the law or these Policies and Procedures or practices;
        - (xii) Responds to inquiries from individuals about the Company's privacy procedures;
        - (xiii) Investigates any complaints that allege that any Company employee or a Business Associate has not complied with or has violated these Policies and Procedures;
        - (xiv) Investigates and conducts risk assessments related to any breach of the Privacy Rule to determine whether notification of breach is required and, as appropriate and necessary, provides such notification;
        - (xv) Oversees document maintenance and retention policies; and
        - (xvi) Reviews and revises Company's HIPAA Policies and Procedures as required or needed to ensure continued compliance with the Privacy Rule and any other applicable law.
    - 2.2 **DOCUMENTATION.** Documentation related to these personnel designations will be retained for 6 years in accordance with Company's record retention policy.

NON-RETALIATION AND WAIVER

- 1. **POLICY**: The Company, Company employees and Business Associates are prohibited from intimidating, threatening, coercing, discriminating against or taking any retaliatory action against any individual for exercising his/her rights under the Privacy Rule or these Policies and Procedures. In addition, the Company is prohibited from requiring any individual to waive his/her rights under HIPAA as a condition of the provision of treatment, payment or eligibility for health care benefits.
- 2. **PROCEDURE**
    - 2.1 **PROHIBITED RETALIATORY ACTIONS.** The Company, Company employees and Company's Business Associates will not retaliate against <u>any</u> individual because he/she:
        - a. Exercised any right under, or participated in any process established by, the Privacy Rule or these Policies and Procedures;
        - b. Filed a complaint with the Company or the Secretary of HHS, or acted with regard to Notification of Breach in accordance with Company's policies;
        - c. Testified, assisted or participated in an investigation, compliance review, proceeding or hearing conducted by the Secretary of HHS; or
        - d. Opposed any act or practice made unlawful by the Privacy Rule or improper by these Policies and Procedures, provided that the individual has a good faith belief that the practice opposed is unlawful or contrary to these Policies and Procedures, and the manner of the opposition is reasonable and does not involve an impermissible disclosure of protected health information ("PHI").
    - 2.2 **WAIVER.** Individuals may not be required to waive their rights under the Privacy Rule or these Policies and Procedures, including their rights to file a complaint with the Secretary of Health and Human Services under HIPAA or obtain a notification of Breach, as a condition of treatment, payment or eligibility for health care benefits.
    - 2.3 **SANCTIONS.** Any Company employees found to have retaliated against an individual for making a complaint, for participating in an investigation, or for seeking or obtaining a waiver from an individual, will be subject to

appropriate sanctions. Any Business Associate's employee found to have retaliated against an individual or sought or obtained a waiver from an individual may be sanctioned in accordance with the Business Associate's sanctions policies.

NOTIFICATION OF BREACH

1. **POLICY:** To notify individuals, the Secretary of Health and Human Services (the "Secretary") and the media of breaches of Unsecured PHI in accordance with the Notification of Breach Rule, 45 C.F.R. Part 164, subpart D, and the HIPAA Final Rule, in accordance with the Company Breach Response Plan included below.

2. **PROCEDURE**

BREACH RESPONSE PLAN

I. Introduction

This Breach Response Plan (the "Plan") is intended for Wichita's Littlest Heroes (the "Company") employees, including those responsible for responding to breaches (defined below). The Plan provides guidance in identifying, evaluating, remediating and reporting any: (i) confirmed or suspected breach of physical, network or system security; (ii) privacy breach; or (iii) material noncompliance with the Company's information privacy and security policies and procedures. The guidance in this Plan applies to all information, data, and technology used by the Company.

This Breach Response Plan is effective as of December 31, 2019. This Plan supersedes any previous breach response plans.

II. Plan Updates and Retention

The Company will review and update this Plan at least once annually, after each incident, and as necessary and appropriate to comply with changes in the law. Company will distribute the Plan to all employees and contractors after each update but does not supersede any incident response policies or procedures that the Company has implemented to comply with the HIPAA Security Rule.

The Company will maintain this Plan and any documentation created pursuant to this Plan, including breach notification letters and risk assessments, in written or electronic form, for a period of at least six (6) years after the date of creation or the date when last in effect, whichever is later, and any additional period required by Company record retention policies and procedures.

III. Breach Response Contact(s)

The following individual(s) ("Breach Response Contact") shall be contacted in the event of a suspected breach:

Heather Sims (heather@wichitaslittlestheroes.com)

The Breach Response Contact's responsibilities shall include, but not be limited to:

Leading breach response activities and assessing a breach's impact and priority;

Correlating information across multiple Company components;

Coordinating information and evidence gathering forensic investigations and follow-up activities;

Updating and closing breach tickets for security breach incidents involving successful penetrations; and

Preparing and disseminating updates and reports to other Company personnel as necessary.

IV. Breach Response Process

The Company breach response process consists of at least the following steps:

A. Preparation and Training

Thorough preparation is essential for prompt and effective breach response. Company will ensure that all Company employees and contractors know how to identify incidents and know the proper procedures for reporting incidents to members of the Breach Response Contact during their initial orientation.

B. Identification

Some incidents, such as theft of computers or unauthorized physical access to Company facilities, are easily identified, whereas computer security incidents can be more difficult to identify. Typical symptoms of computer security incidents include: (i) unsuccessful logon attempts; (ii) suspicious entries in system or network logs; and (iii) disruption of service, or inability of one or more users to login to an account.

When an actual or suspected incident is reported, the Breach Response Contact shall use the Breach Response Checklist (attached as Appendix A) to gather as much information about the suspected incident as possible. If the suspected incident involves a possible compromise of any sensitive or personally identifiable information, including PHI, as that term is defined in the Data Breach Notification Procedures (attached as Appendix B), the Breach Response Contact shall contact internal or external legal counsel (the "Legal Counsel") immediately.

C. Containment

Once the Breach Response Contact is notified of a possible incident, containing the incident shall be the first priority. Consideration will be given to factors such as system backup, risk to continuing operations, and changing passwords or access controls lists on compromised systems and data. This step also includes determining the cause of the incident, improving system defenses, determining system vulnerabilities and removing the cause of the incident to eliminate the possibility of recurrence. It may be necessary to activate business continuity plans and/or disaster recovery plans. The process of containing an incident will differ depending on the incident type.

D. Assessment

Once the incident has been contained, the Breach Response Contact will conduct a detailed investigation to determine the cause of the incident, the extent of damage to systems or facilities, and the quantity and nature of the compromised information, if any. During the investigation, the Breach Response Contact shall, at a minimum, investigate, tally, identify and document:

All affected Company facilities and systems;

Company employees, contractors, subcontractors and vendors with access to the affected facilities and systems, along with usage and/or entry logs;

Vulnerabilities exploited by the attackers;

Damage inflicted by the incident; and

Information compromised during the incident.

As part of the investigation, the Breach Response Contact, in conjunction with Legal Counsel, shall conduct and document a risk assessment that addresses, at a minimum, the following questions:

Who used or received the information?

Have steps been taken to mitigate the risk to any PHI?

What type of information was disclosed?

What amount of information was disclosed?

For incidents involving PHI, the Company shall use the Risk Assessment Questionnaire (attached as Appendix C) in conducting the risk assessment.

E. Remediation

After the damage has been assessed, the Breach Response Contact shall take all reasonable steps necessary to remediate damages resulting from the incident. If the incident involves malicious code ("malware"), all infected systems shall be scanned and cleaned to ensure that no malware remains. If outside attackers gained access to Company systems, any system vulnerabilities exploited by the attackers shall be secured and the Breach Response Contact shall conduct a risk assessment to identify any additional vulnerabilities. If Company property is stolen, additional physical security measures shall be introduced to prevent future thefts.

Once remediation efforts are finished, and systems and facilities have been restored to their operational states, the Breach Response Contact shall arrange to have the affected systems and facilities monitored to ensure that they continue to operate normally.

F. Reporting to Law Enforcement and Others

If the Breach Response Contact believes that the incident was the result of a criminal or tortious act, it may, after consulting with Legal Counsel, decide to demand compensation from the perpetrator and/or refer the case for criminal prosecution. In either case, Company shall first consult with Legal Counsel in order to fully understand the benefits and consequences of pursuing these legal remedies. Depending on the type of information compromised, Company may also have regulatory and/or contractual reporting or notification obligations. Legal Counsel shall help the Breach Response Contact determine which, if any, regulatory agencies or persons it is required to notify.

G. Internal Notification and Reporting

The Breach Response Contact shall promptly provide Company managers with an incident report describing the nature of the incident, how the incident was identified, any damage caused by the incident (including compromised information), any steps taken to remediate damage caused by the incident, and the overall cost associated with the incident, including damages and expenses for response and remediation.

H. External Notification and Reporting

It may be necessary under federal or state law for Company to notify affected persons whose information may have been compromised. The Breach Response Contact shall work with Legal Counsel to identify situations when notification is necessary and to receive further instructions on reporting and notification requirements and processes. Further details are provided in the Data Breach Notification Procedures (attached as Appendix B).

I. Process Evaluation; Updating Policies

Once the incident response is complete, the Breach Response Contact shall meet to discuss how the incident was handled, objectively evaluate the Team's response, and identify areas for improvement. These "lessons learned" shall be used to update the Company Breach Response Plan, Company information privacy and security policies and procedures, and other Company policies and procedures as appropriate.

J. Business Associate Breach Reports

Breach reports made by Company Business Associates shall also be reported to the Breach Response Contact for evaluation and/or monitoring when necessary.

Appendix A

Breach Response Checklist

General Information

Incident Reported By:

Name:_____

Title: _____

Phone:_____

E-mail: _____

Breach Response Contact:_____

Date and Time Detected:

_____

Location of Incident:

_____

Additional information:_____

_____

Date/Time contacted:_____

Incident Information

Type of Incident Detected:

_____

Incident Location:

_____

Information and Systems Affected:

_____

_____

_____

Hardware Manufacturer:_____

Serial Number:

_____

Is the system connected to the network? Y N

System name:

_____

Additional Information:

_____

_____

_____

_____

Incident Response

System isolated from network? Y N

Evidence preserved? Y N

Types of evidence preserved: _____

_____

Additional info:

_____

_____

_____

_____ _____

Remediation actions taken: _____

_____ **Notification/reporting necessary? Y N**

_____ _____

_____ _____

Follow up actions taken: _____ _____

_____ _____

Appendix B

Data Breach Notification Procedures

The federal Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), Health Information Technology for Economic and Clinical Health ("HITECH") Act and corresponding regulations promulgated by the U.S. Department of Health and Human Services ("HHS"), including HIPAA Omnibus Final Rule ("HIPAA Final Rule"), require covered entities (as defined under the Health Insurance Portability and Accountability ("HIPAA") and corresponding Security and Privacy Rules) to notify the affected or potentially affected individuals if they discover that there has been a breach of the security of their data system(s) (electronic or paper) resulting in the possible disclosure of PHI to an unauthorized person. Some state statutes have notification requirements that (i) are more stringent than the federal HIPAA Final Rule requirements or (ii) apply to different categories of information. Accordingly, Company shall make notifications as required by the federal and state breach notification laws in the manner prescribed herein.

I. HIPAA Breach Notification Rule Procedures

A. Application of Procedures These procedures shall apply whenever Company suffers a security incident that results in a "breach," which is defined as unauthorized acquisition, access, use or disclosure that compromises the security or privacy of unsecured PHI of a Company patient or a participant in Company's employee group health plan, where Company is unable to demonstrate that there is a low probability that the PHI has been compromised.

For purposes of these Data Breach Notification Procedures, the term PHI has the same definition as provided in the HIPAA Privacy and Security Rules and the Company information privacy and security policies and procedures, but excludes information that does not contain any the following:

A person's first and last name;

Postal address information, including zip code;

Telephone numbers;

Fax numbers;

Electronic mail addresses;

Social Security number;

Date of birth;

Medical record number;

Health plan beneficiary numbers;

Account numbers;

Certificate/license numbers;

Vehicle identifiers and serial numbers, including license plate numbers;

Device identifiers and serial numbers;

Web Universal Resource Locators (URLs);

Internet Protocol (IP) address numbers;

Biometric identifiers, including finger and voice prints;

Full-face photographic images and any comparable images; and

Any health information that identifies an individual and with respect to which there is a reasonable basis to believe that the information can be used to identify an individual.

Unsecured PHI includes PHI (as defined above) that is not rendered unusable, unreadable or indecipherable to unauthorized individuals through the use of a technology or method specified by HHS.

When a security incident occurs, the Breach Response Contact, in consultation with Legal Counsel, shall make an initial determination as to whether any unsecured PHI was likely acquired by an unauthorized person and whether the incident constitutes a "breach."

The Breach Response Contact shall document its determination as to whether any unsecured PHI was likely acquired by an unauthorized person and its determination as to whether the incident constituted a "breach" (including a determination that the incident did not constitute a breach and the reasons why).

B. Sequence of Procedures

Upon a determination by the Breach Response Contact and Legal Counsel that an unauthorized person has acquired or is likely to have acquired unsecured PHI, the Breach Response Contact shall take the following actions:

Identify and document the type, scope and character of the incident, including the date of the incident and the date the incident was discovered, using the Breach Response Checklist;

Take all necessary measures to promptly contain the incident;

Assess the quantity, nature and extent of the unsecured PHI believed to have been acquired by an unauthorized person, using the Risk Assessment Questionnaire and in conjunction with Legal Counsel;

Implement necessary measures to restore the integrity of the system and remedy any associated security vulnerability;

Determine whether to contact law enforcement to investigate the incident and report the incident if appropriate or required by federal or state law, in consultation with Legal Counsel;

Make expeditious notice, in the method outlined below, to any affected person whose unsecured PHI is discovered to have been compromised unless otherwise directed by law enforcement, in consultation with Legal Counsel; and

Notify, if appropriate, consumer reporting agencies.

C. Timeline for Notification

Upon completion of the sequence of procedures set forth above and in the absence of any law enforcement request for delay, Company management shall promptly, without unreasonable delay, and in no case later than 60 calendar days after the date of discovery of the breach, notify any person whose unsecured PHI was compromised, provided that, if the Breach Response Contact is not able to complete these steps in an expeditious manner, Legal Counsel shall consider whether notification to affected individuals can be made before the investigation and remediation have been fully completed. Notification shall be made in the manner set forth below.

If law enforcement informs Company that notification would impede its ability to conduct an investigation or cause damage to national security and requests that Company delay notification, such request shall be obtained in writing, including the time for which a delay is required, and delay notification as specified in the writing. If Company receives such a request orally, then the Breach Response Contact shall document the statement, including the identity of the official making the statement, and delay notification temporarily and no longer than 30 days from the date of the oral statement, unless a written statement is provided during that time.

D. Method of Notification

When Company, as determined by Legal Counsel, discovers a breach of Unsecured PHI, Company shall notify the individual(s) whose Unsecured PHI has been, or that Company reasonably believes to have been, compromised as a result of the breach, as follows:

Written notice: notification will be sent by first-class mail to the affected individual (or in the case of deceased individuals, the next of kin or personal representative of the affected individual) at the last known address of the affected person (or next of kin or personal representative).

E-mail notice: if the affected individual has agreed to electronic notice and such agreement has not been withdrawn, notification will be sent to the affected individual by electronic mail.

Substitute notice: in the event that there is insufficient or out-of-date contact information that precludes written notification to fewer than 10 affected individuals, a substitute form of notice reasonably calculated to reach the affected individual will be used, *e.g.*, telephone.

Conspicuous posting on the Company website: in the event that there is insufficient information for 10 or more affected individuals, then notifications shall be in the form of a conspicuous posting for a period of 90 days on the home page of the Company website or conspicuous notice in major print or broadcast media in geographic areas where the affected individuals likely reside.

Telephone notice: in any case that requires urgency because of possible imminent misuse of unsecured PHI, notification may be made by telephone or other means, as appropriate, in addition to the notification methods described above. In the event that notification is made by telephone, it shall be made directly to the affected individual in appropriate circumstances and documented in a log that includes the date, time and content of the communication.

In addition to the notification to affected individuals, in the event that the breach involves more than 500 residents of a state or jurisdiction, Company will notify prominent media outlets serving the state or jurisdiction, without unreasonable delay and in no case later than 60 calendar days after the date of discovery of the breach.

In addition to the above, Company will notify HHS, as follows:

For a breach involving 500 or more individuals, Company will provide notification to HHS contemporaneously with the notice to affected individuals in the manner specified by HHS.

For a breach involving fewer than 500 individuals, Company will maintain a log or other documentation of the breach, and no later than 60 days after the end of each calendar year, provide notification to HHS of breaches occurring during the preceding calendar year, in the manner specified by HHS.

E. Notification Language and Record Keeping

The text of all notifications shall be approved by Legal Counsel and Company management. Notifications shall include, to the extent possible:

A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;

A description of the types of unsecured personal information 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);

Any steps affected persons should take to protect themselves from potential harm resulting from the breach (including, for example, advice that the individual should monitor his/her accounts and credit reports and contact information for the credit reporting agencies);

A brief description of what Company is doing to investigate the breach, to mitigate harm to individuals, to mitigate risk to the PHI (such as obtaining the recipient's satisfactory assurances that the PHI will not be further used or disclosed or will be destroyed) and to protect against any further breaches; and

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.

All notices shall be documented and maintained by Breach Response Contact and Legal Counsel.

II. State-Specific Notification Procedures

As referenced above, state statutes may have notification requirements that may be (i) more stringent than the federal HIPAA Final Rule requirements or (ii) applicable to different categories of information. For example, in addition to PHI, some state notification requirements apply to other types of personally identifiable information, such as Social Security number, driver's license number, state ID card number or credit or debit card numbers, combined with any required security code, access code or password. Since the requirements may vary from state to state, the Breach Response Contact shall consult with Legal Counsel for each separate incident to determine whether any state-specific notification requirements apply and to obtain instructions on the state-specific notification procedures. The Breach Response Contact shall also ensure the Company's compliance with additional notification requirements under applicable state laws, such as notification to certain state agencies.

Appendix C

Risk Assessment Questionnaire

As set forth in the Breach Response Plan, and pursuant to the Company information privacy and security policies and procedures, the HIPAA Privacy and Security Rules and the Breach Notification Rule, following a potential security breach, the Breach Response Contact, in conjunction with Legal Counsel shall conduct and document a risk assessment as described below.

I. Factual Description of Incident

[Describe the incident in detail, including relevant date(s)]

[Identify the date on which the incident was discovered]

[Identify the information that may have been compromised]

[Identify any persons or entities who may have used or received the information]

[Describe all actions taken by or at the direction of the Breach Response Contact to investigate the incident]

[Describe any mitigation or remediation steps taken]

[Provide any other information relevant to the implementation of the Breach Response Plan]

II. Three Step Risk Assessment

[Provide detailed responses to each question below]

Step 1 : Has there been an impermissible use or disclosure of PHI that violates the Company information privacy and security policies and procedures, the HIPAA Privacy and Security Rules or the HIPAA Final Rule? If not, there is no breach. If so, the analysis continues to Step 2.

Step 2 : Is it possible to demonstrate that there is a low probability that the PHI has been compromised? To determine whether such low probability exists, the Breach Response Contact conducts a fact-specific risk assessment, which may consider the following factors (this list is not exclusive or exhaustive):

a. What type and amount of Unsecured PHI was used or disclosed?

(i) Does the information contain identifiers in addition the name, such as Social Security number, medical record number or plan membership number?

(ii) Does the information contain particulars about an individual's diagnosis or medical condition, or is it limited to demographic information?

(iii) Does the information contain data that is highly sensitive, such as HIV test results, mental health information, or substance abuse information?

(iv) Could the information be used to commit financial fraud or medical identity theft?

(v) What is the likelihood of re-identification of any de-identified PHI?

b. Who impermissibly used or received the PHI?

(i) Was it another covered entity or business associate? Company in its capacity as employer? Another employee who is not authorized to access PHI? A member of the public?

c. Was the PHI actually acquired or viewed? Or did only the opportunity exist for the information to be acquired or viewed?

d. What steps have been taken to mitigate the risk to the PHI? Has the information been returned? Is it possible to verify that electronic information was not accessed, opened, copied or compromised?

If it can be demonstrated that there is a low probability that the PHI has been compromised, notification is not required. If not, the Breach Response Contact proceeds to Step 3 of the analysis.

Step 3 : Does the breach fall within one of the following three exceptions to the definition of a breach? If so, there is no breach.

a. Was the breach an unintentional access, use or disclosure of PHI by a Company employee or a business associate's workforce member that was an action taken in good faith and within that person's scope of authority, and which did not result in any further, impermissible use or disclosure of the PHI?

b. Was the breach an inadvertent disclosure by and between a Company employee or a business associate's workforce member authorized to access PHI, and was the PHI not further used or disclosed in an impermissible manner?

c. Is there a good faith belief by Company and/or its business associate that the unauthorized person who received the PHI would not reasonably have been able to retain the PHI?

III. Conclusion

[Identify and explain whether the incident constitutes a "breach" as defined in the Breach Response Plan, the HIPAA Final Rule and the Breach Notification Rule, and whether notification of the disclosure is required.]

BREACH RESPONSE PLAN EFFECTIVE: DECEMBER 31, 2019

HIPAA PRIVACY POLICIES & PROCEDURES

NOTICE OF PRIVACY PRACTICES

- 1. **POLICY:** The Company disseminates and maintains a Notice of Privacy Practices ("Privacy Notice" or "Notice") that clearly states the manner in which it may use and disclose an individual's protected health information ("PHI"), and provides adequate notice of an individual's rights and Company's legal duties with respect to PHI. Individuals have a right to request and receive a paper copy of the Privacy Notice at any time.
- 2. **PROCEDURE**
  - 2.1 **PRIVACY NOTICE.**
    - (a) **Responsibility.** The Privacy Officer is responsible for developing, reviewing, revising, updating and disseminating the Company's Privacy Notice to ensure that it conforms to these Policies and Procedures.
    - (b) **Notice Requirements.** The Privacy Notice will be in plain language and include the content requirements set forth in 45 C.F.R. § 164.520.
  - 2.2 **DISSEMINATION OF NOTICE.**
    - (a) **Time to Notify Individuals.**
      - (i) **Notification.** The Company must distribute the "Notice of Privacy Practices" to an individual prior to the individual's first receipt of health care services or, in emergency situations, as soon as reasonably practicable.
    - (b) **Availability of Privacy Notice.**
      - (i) **Electronic Notice.** The Company may provide Notice to an individual by e-mail if the individual agrees to such Notice. If the Company becomes aware that e-mail transmission has failed, a paper copy of the Notice must be provided to the individual. An individual receiving e-mail Notice always maintains the right to obtain a paper copy of Notice from the Company upon request.
      - (ii) **Paper Copy of Notice.** Individuals have a right to a paper copy of the Privacy Notice, even if they have previously agreed to receive the Privacy Notice electronically. Individuals may receive a copy of the Privacy Notice by:
        - (1) **In-Person Request.** An individual may make a request in person to a Company employee.
        - (2) **Written Request.** An individual can submit a request for Notice in writing to:
          - ***Heather Sims,***
          - ***203 N Mathewson***
            Wichita, Ks, 67214
            3165196859
      - (iii) **Availability on Website**. To the extent the Company maintains a website, the Privacy Notice must be placed and maintained on the Company's web site and be available electronically through the website.
  - 2.3 **ACKNOWLEDGEMENT OF RECEIPT.**
    - (a) **Acknowledgement of Paper Copy of Notice.** Each paper copy of the Privacy Notice given to an individual shall have attached to it a cover page entitled Patient Acknowledgement of Receipt of Notice of Privacy Practices, included below as Exhibit A, which the individual will be asked to date and sign at the time the individual is given the Privacy Notice. If the individual is unable or unwilling to date and sign the acknowledgement form, Company employees should document in writing on the face of the acknowledgement form the reason for the inability or refusal of the individual to sign. Such reason could simply be, *e.g.*, that the individual refused to sign after being requested to do so. Company's duty under the law is only to make a good

faith effort to obtain the acknowledgement of receipt. If the individual does not want to sign the acknowledgement form, he or she is not required to do so.

- (b) **Acknowledgement of Electronic Notice.** If an individual wishes to receive the Notice electronically, the system should request the participant to acknowledge receipt electronically.

- 2.4 **DOCUMENTATION.** The Company will retain copies of the Privacy Notices issued by it for six (6) years following their last effective date, in accordance with Company's record retention policy.

EXHIBIT A

NOTICE OF PRIVACY PRACTICES: *ACKNOWLEDGEMENT OF RECEIPT*

- By signing this form (the "Acknowledgement"), you acknowledge receipt of the Notice of Privacy Practices ("NPP") of Wichita's Littlest Heroes. Our NPP provides information about how we may use and disclose your protected health information. We encourage you to read it in full.
- Our NPP is subject to change. If we change our NPP, you may obtain a copy of the revised NPP by:
-
- [accessing our website/contacting our organization at: wichitaslittlestheroes.com
- If you have any questions about our NPP, please contact: Heather Sims.
- I acknowledge receipt of this NPP.
- _____

  Participant's Signature

  _____

  Date

-

  Participant's Name (Please Print): _____

- If this Acknowledgement is being signed by a personal representative (such as a parent or guardian) on behalf of the patient, complete the following:
-

  Personal Representative's Name(Please Print): _____
-

  Description of Personal Representative's Authority: _____
- ***Inability to Obtain Acknowledgement***
- If it is not possible to obtain the individual's Acknowledgement, describe the good faith efforts made to obtain the Acknowledgement, and the reasons why the Acknowledgement was not obtained.
-

  Patient Name: _____
- **Reasons why the acknowledgement was not obtained**:

- □ Participant refused to sign the Acknowledgement even though the participant was asked to do so and the participant was given the NPP.
- □ Other: _____
- Signature: _____

  WLH Representative

  Date: _____
- Print Name: _____

  WLH Representative