HIPAA PRIVACY LG-15

Section: *LG (Legal – HIPAA Privacy)*	**Effective Date:** *May 2, 2011*
Policy Type: *Company Wide*	**Revision Date(s):** 11/13
	Annual Approval: *September 15, 2010*

POLICY: Rural/Metro Corporation and its subsidiaries the ("Company") are committed to protecting patient information. This policy establishes the standards for which Rural/Metro will maintain and manage Protected Health Care Information ("PHI") to maintain compliance with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA").

RESPONSIBLE OFFICER: Privacy Officer

PROCEDURE:

I. The Privacy Rule became effective on April 14, 2003. The Privacy Rule mandated the most significant changes to the health care industry since the passage of Medicare. HIPAA is a set of Federal standards and safeguards issued by the Department of Health and Human Services ("DHHS") and the Office of Civil Rights ("OCR") that must be met and implemented to assure the confidentiality of patient PHI.

The HIPAA Standards are not the only laws and regulations governing Rural/Metro with respect to the use of patient information. It is also Company policy to comply with other state and federal laws and regulations governing the privacy and security of patient information, to the extent those laws are not preempted by the HIPAA Standards. If there is any question as to whether a state law is preempted by the HIPAA Standards, please contact the Privacy or Security Officer.

This policy is applicable to all of the Company's subsidiaries. The Company's Compliance Department and the Corporate Compliance Committee will have the primary responsibility for monitoring and enforcing compliance with all HIPAA policies and procedures. Changes to this policy are not permitted without the approval of the Corporate Compliance Committee.

II. HIPAA PRIVACY STRUCTURE

The Company's HIPAA Privacy Structure consists of a Privacy Officer and Privacy Representatives located in operational areas.

Privacy Officer - The Corporate Compliance Officer or their designee will fill the role of the Privacy Officer. The Privacy Officer oversees all ongoing activities related to the development, implementation, and maintenance of, and adherence to the Company's HIPAA Privacy policies and procedures related to the privacy of and access to, PHI. The Privacy Officer is the main liaison to the Chief Executive Officer and the Board of

Directors concerning HIPAA compliance issues. The Privacy Officer's responsibilities include, but are not limited to:

- Ensuring the Company's HIPAA Privacy Policies are current with HIPAA regulations.
- Development and implementation of HIPAA training programs.
- Overseeing internal and external investigations of alleged violations of HIPAA policies and procedures.
- Work with operational Privacy Representatives to ensure that field business operations are compliant with the Company's HIPAA Privacy Policy.

Privacy Representative – Each operational department with access to PHI must designate a local Privacy Representative. The Privacy Representative is responsible to oversee all ongoing activities that relate to PHI at the operational level. The Privacy Representative shall serve as the designated liaison between field operations and the Privacy Officer. The local Privacy Representative's duties include, but are not limited to:

- Seek clarification to any questions regarding the Company's Privacy policies and to inform the Privacy Officer of any potential issues of non compliance with the Privacy Rule.
- Ensure the business/billing center complies with all applicable privacy requirements to ensure the Company's patient information privacy policies and procedures related to PHI are followed.
- Oversee the processing of patient requests for access to and to amend their PHI.
- To make decisions and answer questions related to issues and questions involving requests for access, amendment, and account of disclosures of PHI.
- Coordination and tracking of releases of PHI that are not for purposes of treatment, payment, or healthcare operations ("TPO").
- As appropriate assist the Privacy Officer or designee in resolving issues resulting from allegations of non-compliance pertaining to the field, business/billing or communications centers.

III. NOTICE OF PRIVACY PRACTICES ("NPP")

The Company and its subsidiaries will provide all patients with a copy of the Company's NPP (See Exhibit A). All patients will be given the opportunity to read the NPP and sign a form of acknowledgement; which may be included in the patient care report ("PCR") language or in a separate form.

The Company is required to obtain a signed acknowledgement of receipt of the NPP, except in emergency situations and when the patient's condition(s) prohibits them from physically and/or mentally signing. When the NPP cannot be delivered or the acknowledgement signature is unable to be obtained the Company will demonstrate a good faith effort to obtain the signature by documenting the condition(s) that prevented the patient from signing.

If a patient refuses to sign the acknowledgement, the reason for the refusal must also be documented.

If a signed patient acknowledgement is on file from a previous service or proof of mailing is on file, an additional acknowledgement is not required.

Any failed attempt to provide the NPP must be noted in the PCR and/or billing information form.

Business operations including billing, offices should be prepared to provide patients with a copy of the NPP when requested and when possible obtain a signed acknowledgement of receipt.

In addition to the NPP being provided at the time of the service, other areas are required to be prepared to provide the NPP:

A. National and local office web pages contain information on the Company's privacy practices and instruct patients or patient representatives how to provide a signed acknowledgment;

B. Mailing procedures to notify and receive signed acknowledgement of the NPP for patients who were not previously notified;

C. Business offices keep the NPP and acknowledgement forms for walk in customers;

D. Collection Agencies are required to notify the Company when the NPP has been requested. The related business operation is responsible to respond to the request.

IV. MINIMUM NECESSARY PRINCIPLE

A vital component of the Privacy Rule is the principle of "minimum necessary" use and disclosures of PHI. A covered entity must make reasonable efforts to use, disclose, and request only the minimum amount of PHI needed to achieve the intended purpose of the request for PHI. The minimum necessary requirement is not applicable to any of the following:

- disclosure to or request by a health care provider for treatment;
- disclosure to an individual who is the subject of the information, or the individual's representative;
- use or disclosure made pursuant to a patient's written authorization if within the scope of the authorization;
- disclosure to the Department of Health and Human Services ("DHHS"), or its designated representatives;
- uses and disclosures required by law; or
- use or disclosure required for compliance with the HIPAA Transactions Rule or other HIPAA Administrative Simplification Rules.

As a covered entity the Company is required to identify areas where PHI may be shared outside of the minimum necessary principle and create appropriate policies to minimize risk. As such, the Company has identified the following areas as potential risks:

- ***Radio Communication*** - Radio communication between medical response personnel and the communications center shall include only the minimum necessary amount of PHI to effectively provide service.
- **Emergencies** – In emergency situations radio communications should only contain the location and nature of the call by dispatch condition description or similar system. If possible, the disclosure of physician name, patient names, and direct or indirectly related conditions should not be communicated over the radio. Additional information should be conveyed in such a way to protect the privacy of patients, such as using codes to communicate certain information.
- **Non-Emergencies** – Non-emergency communications should only include the location and the equipment needed to complete the call. Additional information should be conveyed via other technologies, such as the telephone. If possible the use of patient or physician names, diagnosis codes, or conditions should be avoided.
- **Ambulance to facility communications** – Patient name and address should not be communicated over the radio unless required by on-line medical direction.
- ***Transfer of Patient Care*** - Company employees may share PHI with receiving facility personnel during the transfer of patient care. During the transfer of care, Company employees must take every precaution to guard PHI by speaking softly and directly with facility personnel and ensuring that PCRs or other documentation containing PHI is not left in the open or unattended.

V. DOCUMENT CONTROL

General Documentation Control

Documentation containing PHI should not be left unattended by Company employees. PHI is to be properly secured to prevent access by unauthorized persons, other employees, contract personnel and the general public.

A. All personnel authorized to access, obtain, or develop PHI according to their job function must have appropriate means to secure PHI.

B. Ambulance must have a secure place to store paper PCRs and other documents containing PHI.

C. Field personnel must ensure secured delivery of all documents containing PHI the appropriate business office or lock box.

D. Computer printed information with PHI (e.g., Computer Aided Dispatch reports) must be deposited in a secure place when not in use by authorized personnel.

E. All management personnel engaged in reviewing documents containing PHI must secure those documents when not actively using them or return them to the designated secure place.

F. All waste copies of documents containing PHI that were generated in the course of copying, printing, etc. **must be destroyed in a manner appropriate to the sensitivity of the information.**

Business Operations Containing PHI

All business operations will maintain documentation control procedures that secure documents containing PHI in order to minimize risk of incidental and unauthorized disclosures. Documents containing PHI will be kept secure within Company locations by following procedures in the policy including policy requirements for workplace security.

A. Filing cabinets will be locked after normal business hours if they are not in a locked down office or in another secured area of the building.

B. Access to files will be limited to billing personnel with a specific business purpose for access.

C. All documents, including claim forms, reports, and invoices will be retrieved and routed to the appropriate area daily. No printed documents will be left on printers or faxes after business hours.

D. Copier jams will be addressed immediately and any incomplete or jammed documents containing PHI will be shredded.

E. Company employees that typically do not work in the billing centers are not allowed on the "floor" of the billing center without an express business purpose such as the need to review documentation, resolve complaints, or to reconcile transports.

F. Visitors not employed by the Company must wait in the lobby area before being admitted to the billing center and be escorted at all times while in the office. It is the responsibility of the escort to secure all documents containing PHI in any area the visitor might access prior to admitting the visitor to the billing center.

G. Whenever possible, paper documents containing PHI shall be scanned or otherwise converted into electronic format and original paper documents should be shredded or otherwise destroyed so that the original documents cannot be reconstructed.

VI. DESIGNATED RECORD SETS ("DRS")

The DRS should only include HIPAA PHI, and should not include information used for operational purposes of the organization, such as quality assurance data, accident reports, and incident reports. They type of information included in the DRS is limited to medical records and billing records. (Procedures for requests for patient access, amendment, and restriction on the use of PHI can be found in the Patient Access, Amendment, and Restriction on Use of PHI section of this policy).

This policy establishes a definition of what information should be accessible to patients as part of the DRS. The DRS includes medical records that are created or used by the Company to make decision about the patient. The DRS may include the following records:

A. The PCR created by EMS field personnel which may include photographs, monitor strips, Physician Certification Statements ("PCS"), Refusal of Care forms, or other source data that is incorporated and/or attached to the PCR.

B. The electronic claims records and/or paper records of claims submission to Medicare or other insurance companies.

C. Any patient specific claim information, including responses from insurance payors, such as remittance advice statements, explanations of Medicare Benefits, charge screens, patient account statements, signature authorization and agreement to pay documents.

D. Medicare Advance Beneficiary Notice ("ABN") or other forms from insurance companies indicating coverage determinations, documentation submitted by the patient, and copies of the patient's insurance care of policy coverage summary, that relate directly to the care of the patient.

E. Other records created by other service providers such as first responder units, other ambulance services, air medical services, nursing homes, hospitals, police departments, etc., that are used by the Company as part of treatment and payment purposes related to the patient.

F. Amendments to PHI, or statement of disagreements by the patient requesting the amendment when PHI is not amended upon patient request, or an accurate summary of the statement of disagreement.

VII. WORKPLACE SECURITY

In order to prevent unauthorized or incidental uses and disclosures of PHI, the Company maintains strict requirement on the security, access, use, and disclosure of PHI. Access to PHI will be based on the role of the individual staff member, and access will be limited to the minimum necessary extent that the person needs to complete the necessary job function.

It is the responsibility of each employee to take the necessary security precautions at his/her workspace to ensure PHI is not disclosed inadvertently. Each workspace needs to be secured by each individual responsible for that workspace. Appropriate security measures may include, but are not limited to, the following:

A. All documents containing PHI are placed in a secure area, such as a locked cabinet or bin, when not being utilized at the workspace and when the workspace is unoccupied.

B. All faxes that may contain PHI are retrieved and placed in appropriate envelopes or in-baskets at the end of every shift, at a minimum.

C. Any documents (either written or electronic) that contain PHI and do not need to be part of the DRS shall be shredded or destroyed in a manner that they cannot be reconstructed once they no longer serve a business purpose and in accordance with the Company's Records Retention Policy (LG-06).

D. No documents containing PHI may be taken outside of the workspace without an authorized business need.

VIII. ROLE BASED LEVELS OF INTERNAL ACCESS

Access, use, and disclosure of PHI will be based on the role of the individual staff member in the organization, and should only be allowed to the extent that the person needs to access PHI to complete necessary job related functions. When PHI is accessed, disclosed, or used, the individuals involved will make every effort, except in patient care situations, to only access, disclose and use PHI to the minimum extent necessary to accomplish the intended business purpose.

Although, it would not be the normal pare of most employee roles, certain job functions require that individuals have access to the complete DRS as outlined in the Company Roles Based Matrix (See Exhibit B).

Access to PHI is limited to the persons in the Roles Based Matrix, and only to the PHI ad identified to be consistent with their job responsibilities.

The Company understands there may be exceptions to Role Based Access limitations and while this policy is designated to provide clarification for most circumstances, any employees needing clarification outside of this policy should contact the Privacy Officer or Representative.

- **Role-based Access – Exceptions**. Access to a patient's entire file, or DRS will not be allowed except as provided for in the role-based access or in those justified and documented situations where the entire DRS is necessary to accomplish a specific business purpose, such as resolution lawsuits, internal compliance and investigations, AG inquiries, customer complaints, etc.

- **Disclosures to and Authorizations from the Patient.** When communicating directly with the patient who is the subject of the PHI, employees are not required to limit the PHI disclosure to the minimum necessary amount of information required to perform the job function. In addition, disclosures need to be limited to PHI specifically requested by the patient unless the authorization to disclose PHI is requested by the Company.

  Requests received directly from third parties, such as Medicare, or other insurance companies, which request a Company employee to release PHI to those entities, the information in response to the request would be limited to what is needed for payment purposes. Medicare, Medicaid, and other representatives of the DHHS and the Centers for Medicare and Medicaid Services ("CMS") may request the entire patient records and are not subject to HIPAA restrictions on PHI.

- **Company Requests for PHI.** If an employee needs to request PHI from another health care provider on a routine or recurring basis, for purposes other than direct treatment of the patient, that employee must limit the request to only the reasonably necessary information needed for the intended purpose, as described below. For example, if the request is non-recurring or non-routine, such as making a request for documents via a subpoena, the employee must review the request to make sure it requires only the minimum necessary PHI to accomplish the purpose of the request.

Holder of PHI	Purpose of Request	Information Reasonably Necessary to Accomplish Purpose
Skilled Nursing Facilities	To have adequate patient records to determine medical necessity for service and to properly bill for services provided	
Hospitals	To have adequate patient records to determine medical necessity for service and to properly bill services provided	Patient face sheets, discharges summaries, Physician Certification Statements and Statements of Medical Necessity, Mobility Assessments
Mutual Aid Companies	To have adequate patient records to conduct joint billing operations for patients mutually treated/transported by the Company	Patient Care Reports

For requests not covered above, an employee much make this determination individually for each request and should consult his or her supervisor for guidance as appropriate.

- **Incidental Disclosures.** The Company understands that there will be occasions when there are incidental disclosures about PHI in the context of caring for a patient. The privacy laws were not intended to impede common health care practices that are essential in providing health care to the individual. Incidental disclosures are inevitable, but these will typically occur in radio or face-to-face conversation between health care providers, or when patient care information in written or computer form is left out the open for others to access or see. Radio communications for treatment is permitted, but if not necessary to broadcast patient name, address or other indentifying information, then refrain from doing so.

  The fundamental principle is that all staff needs to be sensitive about the importance of maintaining the confidence and security of all material created by the Company of uses that contain patient care information. Coworkers and other staff members should not have access to information that is not necessary for the staff member to complete his or her job. For example, it is generally not appropriate for field personnel to have access to billing records of patients.

  All personnel must be sensitive to avoiding incidental disclosures to other health care providers and others who do not have a need to know the information. It is important to pay attention to who is within earshot when making verbal statements about a

patient's health information and to follow the Company's procedures for avoiding accidental or inadvertent disclosures.

IX. SECURITY OF PHI

Verbal Security of PHI

Staff members should only discuss patient care information with those who are involved in the care of the patient, regardless of the physical location. The employee should be sensitive to his or her level of voice and to the fact that others may be in the area when he or she is speaking. This approach is not meant to impede anyone's ability to speak with other health care provider freely when engaged in the care of the patient. When it comes to treatment of the patient, the employee should be free to discuss all aspects of the patient's medical condition, treatments provided, and any of their health information the employee may have in his or her possession with others involved in the care of the patient.

- **Waiting or other Public Areas*:*** If patients are in waiting areas to discuss the service provided to them or to have billing questions answered, it is important to make sure that there are no other persons in the waiting area, or if so, bring the patient into a screened or other private area before engaging in discussion.

- **Garage Areas:** Staff members should be sensitive to the fact that other members of the public or other agencies may be present in the garage and other easily accessible areas. Conversations about patients and their health care should not take place in areas where those without a need to know are present.

Physical Security of PHI (See also the HIPAA Security Policy **LG-18**)

- **Patient Care Records:** Patient care documents should be stored in a safe and secure area. When any paper records concerning a patient are completed, they should not be left in open bins or on desktops or other surfaces. Only those with a need to have the information for the completion of their job duties should have access to any paper records.

- **Billing Records:** This includes all notes, remittance advices, charge slips or claims forms that are not maintained in a secure electronic format. These documents should not be left out in the open and should be stored in files or boxes that are secure and in an area with access limited to those who need access to the information for the completion of their job duties.

- **Computers and Personal Entry Devices:** Computer access terminals and other remote entry devices such as Personal Digital Assistance ("PDAs") and laptops should be kept secure. Access to any computer device should require password authentication as a minimum security measure. Staff members should be sensitive to who may be in viewing range of the monitor screen and take simple steps to shield viewing of the screen by unauthorized persons. All remote devices such as laptops

and PDAs should remain in the physical possession of the individual to whom it is assigned at all times.

X. PERMITTED AND REQUIRED DISCLOSURES OF PHI

The Company conforms to the requirements of the Privacy Rule for required and permitted disclosures of PHI. This policy outlines circumstances when it is permitted and/or required to disclose PHI.

Required Disclosures

The Company is required to disclose PHI:

1. To individuals who request their own PHI or an accounting of PHI disclosures. See also Patient/Patient Representative Access to PHI in this policy.

2. When required by DHHS or its representatives to determine a covered entity's compliance with the Privacy Rule or other government regulations; and

3. When the disclosure is required by law.

Permitted Disclosures

The Company is permitted to use and disclose PHI without patient consent or authorization or without allowing the patient to object or agree to the disclosure in the following circumstances:

1. The PHI is used by or disclosed to the individual who is the subject of the PHI;

2. The use or disclosure is for the covered entity's treatment, payment, or health care operations ("TPO") or specified TPO purposes of another covered entity;

3. The use or disclosure is incidental to a permitted use or disclosure and reasonable safeguards are in place;

4. The use or disclosure is based on and is in compliance with a valid authorization (See also Authorization to Use/Disclose PHI for Non-Permitted and/or Required Purposes in this policy); or

5. For specified purposes the use or disclosure is based on an agreement. Example: A shredding company is not considered to be a covered entity because they are not directly involved in the treatment of a patient. However, because they do handle documentation containing PHI, on behalf of a covered entity, certain safeguards must be in place. The privacy rule stipulates that covered entities must sign business associate agreements ("BAAs") with non-covered entities that have access to their PHI.

XI. ACCOUNTING FOR NON TPO DISCLOSURES (NOT REQUIRING AUTHORIZATION)

Whenever PHI is disclosed for purposes other than TPO, the disclosure of this information must be documented. Documentation of each non-TPO disclosure is to be made on an Accounting Log for Non-TPO Disclosures of PHI (See Exhibit C). Patient and Patient representatives have the right, under the HIPAA Privacy Rule, to request an accounting of certain uses or disclosures of PHI made by the Company and its business associates for six (6) years prior to the date of the request.

The purpose of this policy is to ensure accurate accounting of disclosures made by the Company on behalf of the patient that was not related to TPO and to establish procedures to provide the patient full accounting of such disclosures upon their request.

The following is a list of categories of PHI disclosures that can be made without authorization of the patient or patient representative however; these disclosures must be accounted for. All determinations to approve non-TPO disclosures and to determine if such a disclosure falls into one of the following categories the determination should be made by the Local Privacy Representative or the Privacy Officer.

- Public health purposes
- Judicial or Administrative proceedings (i.e. subpoena)
- Reports of abuse, neglect or domestic violence when required by law
- Health oversight agency – Must temporarily suspend a patient account if requested to do so by any agency or official and the agency/official gives a written statement that an accounting would impede an agency's activities for a specified period of time.
- Law Enforcement – In addition to Health oversight agency stipulations, the accounting requirement does not apply to disclosures to correctional facilities and other law enforcement custodial situations.

Logging Disclosures

When a disclosure of PHI is made for purposes other than treatment, transport, or for billing TPO, the following steps need to occur:

1. Complete an "Accounting Log for Disclosures of Protected Health Information" for the patient whom the disclosure occurred; sign and date the log
2. Make a copy for the patient record
3. Forward the original log to the billing department responsible for the patient's DRS.

4. Forward a copy to the local Privacy Representative responsible for tracking non-TPO disclosures.

5. Note the customer account in the billing system with the disclosure date, requestor, purpose of the request, and the PHI disclosed.

6. Attach the original accounting log to the DRS.

Providing Patient and Legal Representative Accounting of Non-TPO Disclosures

When a patient or legal representative requests an accounting of disclosures of the PHI made by the Company or a business associate:

1. Mail or fax the patient or legal representative a copy of the Patient Request for an Accounting of Non-TPO Disclosures (See Exhibit D).

2. Instruct the patient to complete the personal information sections of the form and provide their signature and request date

3. Upon receipt of the appropriately completed form, document all disclosures listed in the DRS in the list of use and disclosures section of the Patient Accounting Form and make a copy of their file

4. Mail or fax the completed form to the patient or legal representative

5. Mail a copy of the completed form to the Privacy Officer at the corporate office:

Rural/Metro
9221 E. Via De Ventura
Scottsdale, AZ 85258
ATTN: Privacy Officer

XII. AUTHORIZATION TO USE/DISCLOSE PHI FOR NON-PERMITTED AND/OR REQUIRED PURPOSES

The Company must obtain a written authorization from the patient for use or disclosure of PHI that is not permitted and/or required by the law as defined by HIPAA.

In the event the Company wishes to use PHI for a purpose that is not permitted and/or required by law (i.e., for marketing or promotional purposes), approval from the Legal/Compliance Department must be granted and the signed authorization from the patient must be obtained prior to the non-permitted use or disclosure of PHI.

XIII. DISCLOSURE TO THE MEDIA

The Company will disclose operational information to the media in conformance with HIPAA and all other applicable laws. HIPAA does not expressly address disclosures of

PHI to the media. Media disclosures shall consist of de-identified information or information that does not constitute PHI.

Each operation should appoint a designee who specialize in media disclosures procedures and policies and will make final determinations on what information is or is not disclosed based on HIPAA regulations and other Company policies regarding public statements. Field employees should be instructed to refer members of the media requesting information to the appointed designee. To ensure there are no inappropriate disclosures or uses of PHI, only the following information may be disclosed to members of the media:

- **Hospital Name.** The name of a hospital to which unidentified patient(s) have been transported so long as doing so would not reveal any identifiable information about a particular patient or the patient's specific condition (i.e., psychiatric hospital).

- **Number of Patients.** The total number of patient involved in an accident or transported to a facility may be provided. You may not indicate specifics about the patient, the patient's condition or other indentifying information, such as a particular vehicle a patient was driving or which particular patient went to which particular facility.

- **Designation of Crewmembers.** The designation of crewmembers as paramedics or EMTs is not PHI. You may state, for example, that one paramedic and two EMTs were involved in care for the patient(s) involved in a motor vehicle accident. However, you are not permitted to describe the type of care rendered to patients at the scene or on the way to the hospital. Nor are you permitted to speculate on what injuries a patient may or may not have sustained.

- **Type of Transport.** You may indicate that a particular call was an emergency and that transportation was facilitated by ambulance or helicopter. Do not discuss information about the patient's condition.

- **Non-PHI.** Information that is not classified as PHI, such as de-identified information may be released to the media consistent with company policy and other federal and state laws.

XIV. DISCLOSURE TO LAW ENFORCEMENT

The Company maintains strict compliance with HIPAA requirements for releases of PHI to law enforcement. There are six (6) situations where some or all PHI may be disclosed to law enforcement. These situations fall into one of three (3) categories; and the following procedures should be followed when responding to law enforcement requests for PHI:

Required by Law

You are required by law to give a patient's PHI to law enforcement regardless of the patient's consent when law enforcement presents you with:

A. **Subpoena, Summons or Warrant ("SSW")**. Confirm that the paper you receive is in fact a subpoena, summons or warrant and that it specifically identifies the PHI you are required to disclose.

1. A subpoena, summons, or warrant is issued by a Court, judicial officer or grand jury. Be sure the SSW has one of these designations as the issuer.

2. Once you have confirmed the SSW is valid, carefully read the SSW as you should only provide the PHI specifically listed in the document. You are legally required to disclose ONLY that information that is contained in the four corners of the document you are given by law enforcement. You are NOT to disclose any other information not specifically requested in the SSW.

3. If the SSW requests the entire PCR, or utilizes language such as "any and all records" pertaining to the patient, you must provide the entire PCR and any other documentation in the patient's record.

4. DO NOT disclose information based on a verbal request from law enforcement.

5. Keep a copy of the SSW with the non-TPO disclosure accounting log.

6. Please note, this policy addresses SSWs served by law enforcement; not private litigants.

B. **Administrative Requests/Investigative Demand.** An administrative request/investigative demand is a written request for PHI by a federal, state, or local government agency authorized to make such requests. If you receive an administrative request/investigative demand, you may ONLY give out a patient's PHI as long as the information requested is:

1. Relevant and material to law enforcement inquiry;

2. Specific and limited in scope to the inquiry; and

3. Non-PHI information could not be used (i.e., PHI may only be disclosed to law enforcement in response to an administrative request/investigative demand when information about PHI would be insufficient).

C. **Burns, Firearm Injuries, Abuse, Domestic Violence**. In some states operations are legally obligated to report to law enforcement certain types of injuries related to gunshot wounds, burns, or incidents of abuse (i.e., child abuse, elder abuse, or domestic violence). State law governs these reporting requirements, and these types of disclosures of PHI are permitted where you are required to make such reports under state law. Contact your supervisor for a list of injuries that you must report under state law in the particular jurisdiction where you are employed.

Permitted Disclosure

The following is a list of situations where PHI may be disclosed, after asking law enforcement the purpose of the request and without the patient's authorization, consent or permission, when law enforcement requests PHI.

A. If law enforcement indicates that they need the PHI to identify or locate a suspect, fugitive, material witness, or missing person, you may disclose only the PHI listed below:

- Name,
- Address,
- Date of birth,
- Place of birth,
- Social Security Number,
- Blood type,
- Type of injury,
- Date of Treatment,
- Time of Treatment, and
- Description of distinguishing physical characteristics (i.e., weight, hair color, eye color, facial hair, scars and tattoos).

B. DO NOT give law enforcement any PHI when the sole purpose of the request is to assist law enforcement with their investigation to help build a case against a suspect. Law enforcement's request must conform to the SSW section of this policy.

C. DO NOT disclose for the purposes of identification or location of any PHI related to the patient's:

- DNA or DNA analysis,
- Dental records, or
- Typing, samples or analysis of body fluids or tissue (except blood type).

D. There may be circumstances when a patient has been the victim of a crime and law enforcement will request certain PHI, the following procedure should be followed in this situation:

1. A supervisor or designated privacy representative should ask the patient for consent to disclose PHI to law enforcement. You may disclose PHI about a crime victim to law enforcement if the crime victim consents to the disclosure.

2. If the patient is temporarily unable to consent, ask the law enforcement agent if they can wait until the patient is able to give consent.

3. If law enforcement cannot wait until the patient is able to consent because to do so would compromise an immediate law enforcement need (i.e., determine if a crime has occurred), then you may disclose the patient's PHI.

4. Ask for and obtain law enforcements' assurance that the PHI you provide will not be used against the victim and that the information is needed immediately. While these assurances may be given verbally, document that you received them.

E. You are permitted to disclose PHI about a patient whom you believe is a victim of abuse, neglect, or domestic violence, where these disclosures are required by state law. You may provide this information to a government authority including Social Services and law enforcement. You should contact your supervisor or designated privacy representative for information regarding the law specific to your area. When providing PHI in this circumstance, take the following steps:

1. If possible ask the patient for their consent. If the patient agrees to the disclosure of PHI, document this, and disclose the information to law enforcement.

2. If the patient does not consent, you may disclose PHI to law enforcement as required by State law if:
   a. You believe the disclosure is necessary to prevent serious harm to the patient or other potential victims, or

b. The patient is unable to consent due to incapacity,
c. Law enforcement assures you the PHI will not be used against the victim, and
d. Law enforcement activities would be adversely affected without the PHI.

3. If PHI has been disclosed without the patient's consent or because the patient was unable to consent, or because the patient was unable to provide consent.

4. DO NOT contact the patient if you believe by doing so you would put them at a greater risk of harm.

Operational Disclosure

A. You may disclose PHI to law enforcement when you think the patient has died as a result of a crime. Limit the PHI to the basic facts about the victim and circumstances of the death.

B. You may disclose PHI to law enforcement when you have a good faith belief that the crime was committed on your employer's premises that resulted in the PHI. This includes the station houses, operational buildings, parking lots, ambulances, and other company vehicles.

C. You may voluntarily offer PHI to law enforcement when you believe it is necessary to alert law enforcement to:

1. The commission of a crime

2. The nature of a crime

3. The location of the crime

4. The location of a crime victim

5. The identity, description, and location of the perpetrator of a crime.

XV. PATIENT AND PATIENT ACCESS TO PHI

The Company maintains strict requirements regarding the access, amendment and/or restriction of PHI by patients and their designees.

A. Upon request by a patient or a patient representative for access to PHI, the office will provide the appropriate Request for Access Form (See Exhibit E and Exhibit F) to the patient or their representative. A valid Patient Representative may be:

1. A health care agent or other representative appointed by a legal document called a "Power of Attorney, " "Durable Power of Attorney," "Health Care Power of Attorney" or similar title;

2. The executor or administrator of a decedent's estate (as evidenced by a legal document such as "letters testamentary" or other document from a probate court showing that the individual is authorized to act as the executor or administrator of the estate);

3. An individual with a signed written authorization by a patient identifying the patient representative as having legal authority to act on the patient's behalf;

4. A parent or guardian of a minor child (where state law permits a parent to make the minor's health care decisions); or

5. A third party such as a state or county child services agency with legal custody of the minor or other individual with legal responsibility over the patient's health care.

B. The Company must receive the correctly completed Patient/Patient Representative Access form before determining if access to PHI will be granted. The Patient/Patient Representative Access form outlines the appropriate identification and/or legal authorization that must be provided to prove identity or to verify the patient representative has the proper authority to act on behalf of the patient. A copy of the driver's license, passport or other form of government-issued photo identification is required to identify both the patient and the patient representative making the request. The patient representative must also provide proof they have the legal right to act on the patient's behalf before they are granted access to the patient's PHI.

C. The completed form will be presented to the Privacy Representative of the local billing office for verification and processing.

D. The local Privacy Representative will act upon the request within 30 days, if not sooner. Generally the Company must respond to requests for access to PHI within 30 days of receipt of the access request, unless the designated record set is not maintained on site, in which case the response period may be extended to 60 days. If the Company is unable to respond to the request within these time frames, the requestor must be given written notice no later than the initial due date for a response, explaining why the Company could not respond within the time frame and in that case the Company may extend the response time by an additional 30 days.

E. Upon the local Privacy Representative's approval of access, the patient or patient representative will have the right to access only PHI contained in the DRS and

may obtain a copy of the PHI contained in the DRS upon verbal or written request.

F. The Company may establish a reasonable charge (as state and federal laws allow) for copying PHI for the patient or the patient representative.

G. Patient or patient representatives access may be denied for the reasons listed below and in some cases, the denial of access may be appealed to the Company for review.

1. If 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. If the PHI makes reference to another person (other than a health care provider) and a licensed health professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to cause substantial harm to that person;

3. If the request for access is made by the requestor as a personal representative of the individual about whom the requestor is requesting the information and a licensed health professional has determined, in the exercise of professional judgment, that access is reasonably likely to cause harm to the individual or another person;

4. If the denial of the request to access PHI is for reasons a, b, or c, then the patient or patient representative may request a review of the denial of access by sending a written request to the local Privacy Representative.

5. The Company will designate a licensed health professional, who was not directly involved in the denial, to review the decision to deny access. The Company will promptly refer the request to this designated review official. The Review Official will determine within a reasonable period of time whether the denial is appropriate. The Company will provide the patient or patient representative with written notice of the determination of the designated Review Official.

6. The patient or patient representative may also file a complaint in accordance with the Procedure for Filing Complaints about Privacy Practices if the patient or patient representative is not satisfied with the Company's determination.

H. The following are reasons to deny access to PHI that are not subject to review, are final, and may not be appealed by the patient or the patient representative:

1. If the information the patient or patient representative requested was compiled in reasonable anticipation of, or use in, a civil, criminal or administrative action or proceeding;

2. If the information the patient or patient representative requested was obtained from someone other than a health care provider under a promise of confidentiality and the access requested would be reasonably likely to reveal the source of information.

3. The patient or the patient representative must be notified in writing by using the Denial of Request for Access to Protected Health Information notice (See Exhibit G) as to why access to the PHI has been denied

I. Access to the actual files or computers that contain the DRS should not be permitted. If upon access approval, the patient or patient representative chooses to view copies of the DRS at a Company location, they may do so in a confidential area under the direct supervision of a designated Company employee. Requests for access to PHI at alternate Company locations will be met when reasonable. **UNDER NO CIRCUMSTANCES SHOULD ORIGINAL COPIES OF PHI LEAVE THE PREMISES**.

J. Whenever a patient or patient representative accesses a DRS, a note should be maintained in a log indicating the time and date of the request, the date access was provided, what specific records were provided for the review and what copies were left with the patient or patient representative.

K. Notwithstanding the above, effective February 17, 2010, when requested by a patient, a covered entity must restrict the disclosure of PHI to the patient, if (1) except as otherwise required by law, the disclosure is to a health plan for purposes of carrying out payment or health care operations (and is not for purposes of carrying out treatment); and the PHI pertains solely to a health care item or service for which the health care provider involved has been paid out of pocket in full.

L. **Right to Copy of PHI Maintained in an Electronic Format.** Notwithstanding the above, effective February 17, 2010, to the extent that the Company uses or maintains an electronic health record with respect to a patient's PHI the patient may obtain a copy of that PHI in an electronic format and, if the patient so chooses, may have the Company transmit a copy directly to an entity or person clearly, conspicuously, and specifically designated by the patient. Additionally, any fee that we charge for providing a copy of the PHI (or a summary or explanation of the information), if the copy is in an electronic form, will not be greater than the Company's labor costs in responding to such request for the copy.

XVI. PATIENT BILLING

The patient has the right to limit disclosures to health plans if they agree to pay the account in full. This is must be enforced at the time the patient makes Rural/Metro aware of their request.

XVII. AMENDMENTS TO PHI

A. Following a request to access PHI, a patient or patient representative may request an amendment to the PHI and request restriction on its use in some circumstances.

B. Telephone communication concerning PHI of the patient is only permitted when discussing the treatment of the patient, payment of an account or continued health care operations. However, the caller must provide the necessary information to identify the patient and the date of service of the account in question. The Company's business/billing offices determine the minimum requirements of patient identity for telephone discussions. If the patient or patient representative has provided the appropriate information to identify the patient, normal demographic (i.e., street address, social security number, insurance identification number, etc.) changes can be requested and provided by making the appropriate changes to the Company's billing system. However, if changes to PHI of the DRS are requested, the Patient/Patient Representative Request for Access form must be sent to the requestor.

C. The patient or patient representative may only request amendment to PHI contained in the DRS. The "Request for Amendment of Protected Health Information" Form (See Exhibit H) must be accompanied with a correctly completed Patient or Patient Representative Request for Access Form.

D. The Company must act upon a Request for Amendment within 60 days of the request. If the Company is unable to act upon the request within 60 days, it must provide the requestor with a written statement of the reason(s) for the delay and in that case, may extend the time period in which to comply by an additional 30 days.

E. All requests for amendment must be forwarded immediately to the local Privacy Representative for review.

F. Any amendment request regarding the patient's current medical condition, past medical history, current medications, allergies or any other medical information must be supported by documentation from the patient's physician or facility.

G. If the local Privacy Representative grants the request for amendment, then the requestor will receive an Acceptance of Request for Amendment of Protected Health Information notice (See Exhibit I) indicating that the appropriate amendment to the PHI or record that was the subject of the request has been

made. If the local Privacy Representative denies the request for amendment the requestor will receive a Denial of Request for Amendment to Protected Health Information notice (See Exhibit J).

H. There must be written permission provided by the patient or patient representative so that the Company may notify the person(s) with which the amendments need to be shared. The Company must provide the amended information to those individuals identified by having received the PHI that has been amended as well as those persons or business associates that have such information and who may have relied on or could be reasonably expected to rely on the amended PHI.

I. The patient or patient representative must identity individuals who may need the amended PHI and sign the statement in the Request for Amendment form giving the Company permission to provide them with the updated PHI.

J. The Company will add the request for amendment, the denial or granting of the request, as well as any statement of disagreement by the patient or patient representative and any rebuttal statement by the Company to the DRS.

K. The Company may deny a request to amend PHI for the following reasons:

1. If Company personnel did not create the PHI at issue;

2. If the information is not part of the DRS; or

3. The PHI is accurate and/or complete.

L. The Company must provide the following in denying a request to amend PHI:

1. A written denial written in plain language that states the reason for the denial.

2. The individual's right to submit a statement disagreeing with the denial and to whom the individual may file such a statement and if possible, appeal;

3. A statement that, if the individual does not submit a statement or disagreement, the individual may request the Company provide the request for amendment and the denial with any future disclosures of PHI;

4. A description of how the individual may file a complaint with the Company, including the name and telephone number of the appropriate contact or to the Secretary of the Department of Health and Human Services.

M. If the patient or their representative submits a written letter of disagreement the Company may prepare a rebuttal to the patient or the patient representative. The letter of disagreement and rebuttal will be appended to the PHI.

N. If the Company receives a notice from another covered entity, such as a hospital, that it has amended its own PHI in relation to a particular patient, the Company must amend any of its PHI that would be affected by this amendment.

XVIII. RESTRICTION ON USE OF PHI

Effective February 17, 2010, when requested by a patient, a covered entity must restrict the disclosure of PHI of the patient, if (1) except as otherwise required by law, the disclosure is to a health plan for purposes of carrying out payment or health care operations (and is not for purposes of carrying out treatment); (2) the PHI pertains solely to a health care item or service for which the health care provider involved had been paid out of pocket in full. A patient or their representative may request a restriction on the use and disclosure of their PHI according to the following:

A. Correctly completed Patient or Patient Representative Request for Access Form must be received by the Company before providing the patient or their representative the Request for Restriction of Protected Health Information form (See Exhibit K).

B. All requests for restriction regarding use and disclosure of PHI must be submitted in writing on the approved Company form. All requests will be reviewed and either approved or denied by the Privacy Official.

C. If the Company agrees to the restriction, the restriction must be documented and the associated PHI may not be used or disclosed, except when the individual who requested the restriction is in need of emergency medical services, and the restricted PHI is needed to provide the emergency medical service or treatment.

D. A restriction may be terminated if the individual agrees to or requests the termination. Oral agreements to terminate a restriction must be documented in the patient's record.

E. The Company is not required to restrict PHI that was created or received after the restriction was requested as long as the patient or patient representative is notified that PHI created or received after the restriction is not included in the restriction. PHI that was restricted prior to the Company terminating the restriction must continue to be treated as restricted PHI.

XIX. EXTERNAL COMPLAINTS

Individuals have the right to make a complaint directly to the Privacy Official concerning the Company's HIPAA policies and procedures with respect to the use and disclosure of PHI. The Privacy Official must log information about the allegations and details of the

investigations in the Log for Processing External Compliant about Privacy Practices (See Exhibit L).

Individuals also have the right to make a complaint to the government if they have concerns the Company is not complying with the requirements of the federal Privacy Rule. The Company will notify complainants of their rights and procedures for filing complaints by use of the Patient Procedure for Filing Compliance about Privacy Practices notice (See Exhibit M). Individuals may file a complaint with the Secretary of the U.S. Department of Health and Human Service ("HHS") by following the requirements below:

A. Upon notification of a complaint, the local office shall instruct the complainant of their rights under the HIPAA Privacy Rule as explained in the Patient Procedures for Filing Complaints About Privacy Practices.

B. A complainant may make a verbal complaint to a Company representative. The Company representative should encourage the complainant to submit their concerns in writing. The Company representative must document their conversation and notify the local Privacy Representative or the Privacy Official.

C. A complainant may file a complaint in writing, either on paper or electronically. All written complaints should be addressed to the Privacy Official at: 9221 E. Via De Ventura, Scottsdale, AZ 85258.

D. Upon receipt of the written complaint the Privacy Official, will complete the Log for Processing Complaints About Privacy Practices and the following steps will be taken:

1. Investigations – The Privacy Official will review the complaint to determine if it is justified. If the complaint is warranted, the Privacy Official will initial an investigation. The investigation may include interviews with employees, a review of pertinent policies, and the circumstance regarding any alleged acts.

2. Mitigation – If the investigation reveals a violation of HIPAA regulations on the part of the Company or its employees, business associates, or contracted entity, the privacy official must mitigate, to the extent possible, any damage that may result from the violation. This may include notifying the subject of the unauthorized release of PHI and/or self-disclosure of the incident on behalf of the Company to the Secretary of the United States Department of Health and Human Services.

E. The Privacy Rule states the following requirements when filing a complaint to HHS:

1. A compliant must be filed in writing either on paper or electronically.

2. A complaint must name the entity that is subject of the complaint and describe the acts or omissions believed to be in violation of the applicable standards of the Federal Privacy Rule or the applicable standards, requirements and implementation specification of sub part E of part 164 of the Federal Privacy Rule.

3. A complaint must be filed within 180 days of when the complainant knew of should have known the act or omission complained of occurred, unless the Secretary, for good cause shown, waives the time limitation.

4. The Secretary may prescribe additional procedures for the filing of complaints, as well as the place and manner of filing, by notice in the Federal Register.

XX. INTERNAL COMPLAINTS

When an employee suspects or knows about non-compliance with any of the Company's privacy policies, including a breach of privacy or any unauthorized use or disclosure of a patient's PHI, it is the employee's responsibility to report the suspected or known incident immediately. The employee shall report the suspected incident by filing a formal complaint directly with the Privacy Official or by one of the following:

1. Using the anonymous Rural/Metro Hotline at 877-631-5722.

2. In writing to 9221 E. Via De Ventura, Scottsdale, AZ 85258.

The Company follows a non-retaliation policy and employees should not fear making identified complaints or expressing concerns in good faith regarding the Company's privacy practices to the Privacy Official or any other member of management. The Privacy Official will follow the same remediation and investigation procedures listed above.

XXI. BUSINESS ASSOCIATES AGREEMENTS

The Company, as a covered entity under HIPAA, must enter into business associate agreements with vendors, companies and individuals performing function s or services on behalf of the Company when those functions or services involve the use or disclosure of the Company's PHI.

A "business associate" is someone who performs certain services on behalf of a covered entity where those services involve the access, use or disclosure of PHI. The Company is generally not a business associate of another health provider. Possible examples of business associates are:

- Software consultants
- Employment agencies
- Consultants
- Legal services (outside counsel)

In some cases a covered entity may contract with other entities or persons who are NOT business associates. These entities do not have authorization to have access to PHI and do not perform a service that involves PHI. However, incidental disclosures may occur during the course of performing a service. In this instance, a confidentiality agreement should be in place.

It is critical to determine whether it is necessary to enter into a business associate agreement and/or restrict or limit access to PHI. It is the responsibility of the Privacy Officer or Privacy Representative to determine if the function or service to be provided by the outside party mandates a signed business associate agreement as defined by HIPAA.

The Company is responsible for contractually obligating the other party to comply with HIPAA and the Company must include specific language in its business associates agreements, as required by the Privacy Rule. If the Privacy Officer or Representative is unsure if a vendor, company or individual performing a service on behalf of the Company requires a business associate agreement or confidentiality agreement between two parties, the Privacy Officer or Representative should seek clarification from outside counsel with expertise in HIPAA regulations.

The Company has established specific language to comply with the legal requirements when entering into contractual relations with business associates. The most current Business Associated Agreement can be obtained by contacting the Legal or Compliance Department.

XXII. BREACH NOTIFICATION

The Company recognizes that it has an obligation to provide proper notice to all affected individuals whose unsecured PHI has been, or is reasonably believed to have been breached. The Company will, following the discovery of a breach of unsecured PHI, notify each individual whose unsecured PHI has been or is, reasonably believed to have been, accessed, acquired, used, or disclosed. The Company will also notify HHS and media outlets in accordance with Federal Regulations.

"Breach" means the acquisition, access, use, or disclosure of PHI in a manner not permitted under the HIPAA Privacy Rule which compromises the security or privacy of the PHI.

"Compromises the security or privacy of the PHI" means poses a significant risk of financial, reputational, or other harm to the individual.

Breach excludes: (1) any unintentional acquisition, access, or use of PHI by Workforce member or person acting under the authority of the Company, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure; (2) any inadvertent disclosure by a person who is authorized to access PHI at the Company to another person authorized to access PHI at the Company or a Business Associate, and the information received as a result of such

disclosure is not further used or disclosed; and (3) a disclosure of PHI where the Company has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

"Unsecured PHI" means PHI that is not been rendered unusable, unreadable, or indecipherable to unauthorized individual through the use of a technology or methodology specified by HHS on its website.

XXIII. MEDICAL RECORDS OF EMPLOYEES

The Company will, to the extent required by law, protect medical records it receives about employees in a confidential manner. Generally, only those with a need to know the information will have access to it, and, even then, they will only have access to as much information as minimally necessary for the legitimate use of the medical records.

The Company is a self-insured company and as such the Company Health Plan ("the Plan") may at times access the PHI related to insurance claims. HIPAA requires that the Plan follow rules that protect PHI from improper uses and disclosures. The Company's Group Health Plan Privacy Notice provided to all employees enrolled in the Plan, explains how the Company complies with the requirements.

Employment records, including certain medical records of employees that are related to the job, are **not** considered to be PHI, and therefore not subject to HIPAA safeguards. Those employment records include, but are not limited to:

1. Information obtained to determine suitability to perform the job duties (such as physical examination reports),

2. drug and alcohol tests obtained in the course of employment,

3. doctor's excuses provided in accordance with the attendance policy,

4. work-related injury and occupational exposure reports, and

5. medical and laboratory reports related to such injuries or exposures, especially to the extent necessary to determine worker's compensation coverage.

With respect to Company employees, only health information that is obtained about staff in the course of providing ambulance or other medical services directly to them is considered PHI under HIPAA. These protections are subject to HIPAA exceptions, such as a situation in which the staff member is involved in a work-related injury and utilizes the Company for personal ambulance transport while on duty.

XXIV. EMPLOYEE TRAINING

All employees, independent contractors, students, trainees, an leased (temporary) employees (collectively referred to as "staff") who have access to patient information shall be trained in the Company's policies and procedures regarding PHI.

1. All current staff must be trained regarding the Company's HIPAA Compliance Program.

2. All new staff members are required to undergo privacy training within 30 days of hire.

3. All staff members will also be required to undergo privacy training within a reasonable time after there is a material change to the Company's policies and procedures on privacy practices.

4. All staff will receive copies of the Company's policies and procedures regarding privacy.

5. All attendees must personally complete the training and verify completion and agree to adhere to the Company's policies and procedures on privacy practices. The signed acknowledgement will be kept in the employee file in Human Resources.

6. Training will consist of a comprehensive self-review of the Company's HIPAA Privacy Policies and Procedures. Staff must complete the Company's on-line HIPAA training. The on-line HIPAA training program supersedes any previous video or live training programs.

XXV. MONITORING AND AUDITING

The Compliance Department will have the responsibility to monitor compliance with this policy. Changes, amendments or additions to this policy are not permitted without the approval of the Corporate Compliance Committee.

The Compliance Department will conduct routine audits for compliance to this policy; which may include, but are not limited to routine monthly audits of patient records as well as on-site audits of billing centers and ambulance operations.

XXVI. EMPLOYEE CONFIDENTIALITY AGREEMENT

In consideration of their employment or compensation from the Company, all employees must read and understand the Company's policies and procedures regarding PHI, as mandated by HIPAA. Every employee must sign the Company's Employee Confidentiality Agreement (See Exhibit N), which verifies they have read and understand the Company's policies and procedures regarding HIPAA.

XXVII. CORRECTIVE ACTION

Any breach of Company policy is very serious, failure to comply with the Company's HIPAA Privacy Policies and Procedures may result in disciplinary action up to and including termination. Not only does the law require that we appropriately sanction staff members for privacy violations, our patients and he public expect us to do just that.

This policy applies to all Company staff members who have any degree of access to patient information, including those staff members who may learn of patient information indirectly, and even if use of this information is not part of the staff member's responsibilities with the Company. The type of corrective action will 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 other contractor should be aware that violations of a severe nature may result in notification to law enforcement officers as well as regulatory, accreditation, and/or licensure organizations and civil and/or criminal penalties may apply.

Any sanctions under this policy or any other policy will not apply to staff members who:

- file a complaint with the federal government about potential privacy violations,
- testify, assist, or participate in an investigation or compliance review proceeding or official government proceeding investigating privacy issues, and
- oppose any actions by the Company that are unlawful under the HIPAA Privacy Rule or the HIPAA Security Rule, when that opposition is mad e with the good faith belief that the Company was violating privacy or security regulations (as long as any opposition or filing of a complaint did not result in improper disclosure of PHI or e-PHI).

The Compliance Department and appropriate management in conjunction with Human Resources is responsible for determining the severity of corrective action necessary. The following apply when determining corrective action:

1. The Compliance Department and Human Resources will appropriately investigate and document any allegations of wrongful actions and determine whether an act requiring corrective action has occurred and what corrective action is appropriate.

2. Management and Human Resources will generally follow the progressive discipline steps set forth below for failure to comply with HIPAA privacy policies, however instances where blatant disregard for Company policy has been confirmed the Company may determine that immediate termination is appropriate.

3. All corrective actions of employees will be documented and retained for a period of at least six (6) years from the date of its creation or the date when it was last in effect, whichever is later

Progressive sanctions will include the following (in accordance with collective bargaining agreements, where applicable):

1. Remedial training and education

2. Informal verbal counseling

3. Formal verbal counseling with written documentation of the counseling

4. Written warning

5. Suspension

6. Termination or expulsion

The Corporate Legal Department will notify law enforcement, regulatory accreditation and/or licensure agencies of wrongful actions as appropriate.

Staff members have an affirmative duty to report immediately to management or the Privacy Officer or Representative any suspected violation of Company privacy/security policies and procedures.

Staff members shall be educated about this policy and the serious nature of violating Company privacy/security policies. Staff members will be made aware of the potential sanctions that may occur, and will be made aware of any changes to this sanction policy.

XXVIII. QUESTIONS AND REPORTING

Questions or comments regarding this policy should be directed to the Privacy Officer or the Compliance Department.

Reports of alleged non-compliance to this or any of Rural/Metro's HIPAA or Compliance Policies may be made to the anonymous Rural/Metro Employee Hotline at **1-877-631-5722**.

Approved by: _____ Date: 10/30/13
President and Chief Executive Officer

EXHIBIT A

NOTICE OF PRIVACY PRACTICES REGARDING PROTECTED HEALTH INFORMATION

THE RURAL/METRO FAMILY OF COMPANIES NOTICE OF PRIVACY PRACTICES REGARDING PROTECTED HEALTH INFORMATION

THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.

Rural/Metro Corporation, through its subsidiaries and affiliates, provides medical transportation, fire protection services and related services. These subsidiaries and affiliates providing such services are hereinafter referred to as "The Company," "we," "our," or "us." Due to the nature of these services, we are required by law to maintain the privacy of certain confidential health care information, known as Protected Health Information (PHI), and to provide you with a notice of our legal duties and privacy practices with respect to your PHI. We are also required to abide by the terms of the version of this Notice currently in effect.

Uses and Disclosures of PHI: We may use PHI for the purposes of treatment, payment and health care operations, in most cases without your written permission. Examples of our use of your PHI:

For Treatment. This includes such things as obtaining verbal and written information about your medical condition and treatment from you as well as from others, such as doctors and nurses who give orders to allow us to provide treatment to you. We may give your PHI to other health care providers involved in your treatment, and may transfer your PHI via radio or telephone to the hospital or dispatch center.

For Payment. This includes any activities we must undertake in order to get reimbursed for the services we provide to you, including such things as submitting bills to insurance companies, making medical necessity determinations and collecting outstanding accounts.

For Health Care Operations. This includes quality assurance activities, licensing and training programs to ensure that our personnel meet our standards of care and follow established policies and procedures, as well as certain other management functions.

Reminders for Scheduled Transports and Information on Other Services. We may also contact you with a reminder of any scheduled appointments for non-emergency ambulance and medical transportation, or to inform you about other services we provide.

Use and Disclosure of PHI Without Your Authorization. We are permitted to use PHI *without* your written authorization, or opportunity to object, in certain situations, and unless prohibited by a more stringent state law, including:

- For the treatment, payment or health care operations activities of another health care provider who treats you;
- For health care and legal compliance activities;
- To a family member, other relative, or close personal friend or other individual involved in your care if we obtain your verbal agreement to do so or if we give you an opportunity to object to such a disclosure and you do not raise an objection, and in certain other circumstances where we are unable to obtain your agreement and believe the disclosure is in your best interests;
- To a public health authority in certain situations as required by law (such as to report abuse, neglect or domestic violence;
- For health oversight activities including audits or government investigations, inspections, disciplinary proceedings, and other administrative or judicial actions undertaken by the government (or their contractors) by law to oversee the health care system;
- For judicial and administrative proceedings as required by a court or administrative order, or in some cases in response to a subpoena or other legal process;
- For law enforcement activities in limited situations, such as when responding to a warrant;
- For military, national defense and security and other special government functions;
- To avert a serious threat to the health and safety of a person or the public at large;
- For workers' compensation purposes, and in compliance with workers' compensation laws;
- To coroners, medical examiners, and funeral directors for identifying a deceased person, determining cause of death, or carrying on their duties as authorized by law;
- If you are an organ donor, we may release health information to organizations that handle organ procurement or organ, eye or tissue transplantation or to an organ donation bank, as necessary to facilitate organ donation and transplantation;
- For research projects, but this will be subject to strict oversight and approvals;
- Use or disclose health information about you in a way that does not personally identify you or reveal who you are.

Any other use or disclosure of PHI, other than those listed above will only be made with your written authorization. You may revoke your authorization at any time, in writing, except to the extent that we have already used or disclosed medical information in reliance on that authorization.

Patient Rights: As a patient, you have a number of rights with respect to your PHI, including:

The right to access, copy or inspect your PHI. This means you may inspect and copy most of the medical information about you that we maintain. We will normally provide you with access to this information within 30 days of your request. We may also charge you a reasonable fee, as state law permits, to provide a copy of any medical information you have the right to access. In limited circumstances, we may deny you access to your medical information, and you may appeal certain types of denials. We have forms available to request access to your PHI and we

will provide a written response if we deny you access and let you know your appeal rights. You also have the right to receive confidential communications of your PHI. If you wish to inspect or obtain a copy of your medical information, you should contact our local privacy representative.

Right to Copy of PHI Maintained in an Electronic Format. If we use or maintains an electronic health record with respect to your PHI you have a right to obtain a copy of that PHI in an electronic format and, if you choose, to have us transmit a copy directly to an entity or person you clearly, conspicuously, and specifically designate. Additionally, any fee that we may charge you for providing a copy of your PHI (or a summary or explanation of the information), if the copy (or summary or explanation) is in an electronic form, will not be greater than our labor costs in responding to your request for the copy (or summary or explanation).

The Right to Amend Your PHI. You have the right to ask us to amend written medical information we may have about you. We will generally amend your information within 60 days of your request and will notify you when we have amended the information. We are permitted by law to deny your request to amend your medical information only in certain circumstances, like when we believe the information you have asked us to amend is correct. If you wish to request an amendment of the medical information we have about you, please contact our local privacy representative to obtain an amendment request form.

The Right to Request an Accounting. You may request an accounting from us of certain disclosures of your medical information we have made in the six years prior to the date of your request. However, your requests for an accounting of disclosures cannot precede the implementation date of HIPAA April 14, 2003. We are not required to give you an accounting of information we have used or disclosed for purposes of treatment, payment or health care operations, or when we share your health information with our business associates, such as our billing company or a medical facility from/to which we have transported you. We are also not required to give you an accounting of our uses of PHI for which you have already given us written authorization. If you wish to request an accounting, contact our local privacy representative.

The Right to Request That We Restrict the Uses and Disclosures of Your PHI. You have the right to request that we restrict how we use and disclose your medical information we have about you. We are not required to agree to any restrictions you request, but any restrictions agreed to by us in writing are binding on us.

Right to Opt Out of Fundraising. In the event that Rural/Metro would contact you to request your participation in fund raising efforts, you have the right to opt out of receiving such communications.

Right to Pay Out of Pocket. You have the right to request restrictions of disclosures of your PHI to health plans if you consent to pay the balance for services in full.

Restrictions on Disclosures to Health Plans for Services Paid In Full Out of Pocket. Except as otherwise required by law, at your request we will not disclose your PHI to a health plan for purposes of carrying out payment or health care operations (and is not for the purpose of

carrying out treatment), if the PHI pertains solely to a health care item or service for which we have been paid out of pocket in full.

Right to Request Alternative Communications. You have the right to request that we communicate with you about medical matters in a certain way or at a certain location. For example, you can ask that we only contact you at work or by mail. To request confidential alternative communications, you must make your request in writing on the form provided by the Practice. We will not ask you the reason for your request. We will accommodate all reasonable requests. Your request must specify how or where you wish to be contacted.

Internet and the Right to Obtain a Paper Copy of the Notice on Request. If we maintain a web site, we will prominently post a copy of this Notice for your review. We will always provide you a paper copy of the Notice upon request.

Revisions to the Notice: We reserve the right to change the terms of this Notice at any time, and the changes will be effective immediately and will apply to all PHI we maintain. Any material changes to the Notice will be promptly posted in our facilities and posted to our web site, if we maintain one. You can get a copy of the latest version of this Notice by contacting our privacy official.

Your Legal Rights and Complaints: You also have the right to complain to us, or to the Secretary of the United States Department of Health and Human Services if you believe your privacy rights have been violated. You will not be retaliated against in any way for filing a complaint with us or to the government. Should you have any questions, comments or complaints you may direct all inquiries to our privacy official.

Privacy Officer Contact Information:

Privacy Officer
Rural/Metro
9221 E. Via De Ventura,
Scottsdale AZ 85258
(480) 606-3886

Effective Date of the Notice: November 1, 2010

EXHIBIT B

Rural/Metro Corporation
Roles Based Access Matrix

Job Title	Accessible PHI	Conditions to Access PHI
Executive Management	All PHI	May access only to the extent necessary to monitor compliance and to accomplish appropriate supervision and management of personnel. May access any the Company facility necessary to monitor compliance and to accomplish company related functions without being accompanied by other The Company personnel.
Corporate Management	All PHI	May access only to the extent necessary to monitor compliance and to accomplish appropriate supervision and management of personnel.
Corporate Auditors	All PHI	May access only to the extent necessary to monitor compliance and to accomplish appropriate auditing functions.
Operational Management (Division General Managers. Billing Managers, etc.)	All PHI	May access only to the extent necessary to monitor compliance and to accomplish appropriate supervision and management of personnel.
Training Coordinators/Quality Assurance Auditors	Electronic and paper intake forms from dispatch, patient care reports, physician certification statements, other documents related to patient care.	May access only as part of training and quality assurance activities. All individually identification PHI should be redacted prior to use in training and quality assurance activities.
EMT	Electronic and paper intake forms from dispatch, patient care reports, physician certification statements, other documents related to patient care.	May access only as part of completion of a patient event and post-event activities and only while actually on duty.

Job Title	Accessible PHI	Conditions to Access PHI
Paramedic	Electronic and paper intake forms from dispatch, patient care reports, physician certification statements, other documents related to patient care.	May access only as part of completion of a patient event and post-event activities and only while actually on duty.
Billing/Collection Personnel	Electronic and paper intake forms from dispatch, patient care reports, physician's certification statements, billing claims, remittance advice statements, and other patient records from facilities.	May access only as part of duties necessary to complete patient billing and collection follow up and only while on an actual working shift.
Field Supervisors	Electronic and paper intake forms from dispatch, patient care reports, physician certification statements, other documents related to patient care.	May access only as part of completion of a patient event and post-event activities, as well as for quality assurance checks and corrective counseling of staff.
Dispatcher	Electronic and paper intake forms, scheduled transport information and CAD information regarding patient addresses.	May access only as part of completion of an incident, from receipt of information necessary to dispatch a call, to the closing out of the incident and only while on duty.
Administrative	No access to PHI	No access to PHI
Consultant	Limited Access to PHI	May access only to the extent necessary to perform their assigned tasks, and as dictated by a confidentiality agreement.
Technical Support	All PHI	May access only to the extent necessary to monitor compliance and to accomplish appropriate supervision and management of personnel.

EXHIBIT C

Rural/Metro Corporation
Accounting Log for Non-TPO Disclosures of Protected Health Information

Patient Name: _____

Date of Disclosure	Requestor Name/Company/ Title	Purpose of Disclosure	Requested PHI (list all)	Authorization from Patient (Yes/No/NA)	PHI Disclosed	Reviewed by Privacy Official or Representative

Comments:

_____
_____
_____
_____
_____

Log Completed by: _____ Title: _____

Date: _____

EXHIBIT D

Rural/Metro Corporation

Patient Request for an Accounting of Non-TPO Disclosures

Patient Name: _____ Date: _____

Address: _____

City: _____State: _____ Zip Code: _____

Social Security #: _____

Patient Rights: As a patient, you have the right to access, copy or inspect your PHI, amend your PHI, request an accounting of certain uses and disclosures of PHI for the last six (6) years beginning April 14, 2003, prior to the date of the request, from The Company.

NOTE: Rural/Metro is not required to provide you with an accounting of uses and disclosures associated with your treatment, payment or health care operations.

Signature: _____ Request Date: _____

EXHIBIT E

Rural/Metro
Patient Request for Access Form

Patient Name: _____ Date: _____

Address: _____

City: _____State: _____ Zip Code: _____

Social Security No.: _____ Last Date of Service: _____

Patient Rights: **As a patient, you have the right to access, copy or inspect your protected health information (PHI), in accordance with federal and state laws, rules and regulations. You may also have the right to request an amendment to your PHI, or request that we restrict the use and disclosure of it. These rights are further described in our Notice of Privacy Practices.**

To better allow us to process your request, please indicate the type of request you are making on this form: [check all that apply]

_____ Access to simply review my health information.
_____ Access to obtain copies of my health information. (There may be a fee for this service).
_____ Access to review and potentially request amendment of my health information.
_____ Access to review and potentially request an accounting of how my PHI has been used and disclosed to others.
_____ Access to review and potentially request restrictions on the use and disclosure of my health information.

Signature:_____ Request Date: _____

∗You must provide a photocopy of a legal ID listed in Section 1 and return with the completed form.

Office Use Only

Select the type of photo identification provided:

Driver's License/State ID __ Military ID __ Other Photo ID__ Passport ___

Update to Patient Accounting Log _____ Yes _____ No _____ N/A

Patient Information/Documentation Released and Purpose:

_____
_____
_____
_____

EXHIBIT F

Rural/Metro Corporation
Patient/Representative Request for Access Form

I understand that it is the policy of Rural/Metro to keep all patient records and patient information confidential. In addition, I understand that Rural/Metro is providing patient information to me as required by state law or because I have produced legal documentation giving me the ability to receive such information. I attest that any documentation I have provided to Rural/Metro, giving me the authority to receive the requested patient information is a legally operative and effective document. Rural/Metro will not be held responsible for any defects in the legal document that may render it inoperative.

Name of Requestor: _____ Date: _____

Signature: _____

Title (*if applicable*): _____ Relationship to Patient: _____

Name of Patient: _____

Please indicate the type of request you are making on behalf of the patient:
_____Access to simply review my health information.
_____Access to obtain copies of my health information. (There may be a fee for this service).
_____ Access to review and potentially request amendment of my health information.
_____ Access to review and potentially request an accounting of how my PHI has been used and disclosed to others.
_____ Access to review and potentially request restrictions on the use and disclosure of my health information.

∗To receive the requested PHI on behalf of the patient, the requestor must provide, with this access form, a copy of one each of the legal documents and forms of legal identification listed below.

Office Use Only

Copy of legal document attached _____ Yes _____ No

Type of legal document attached: Power of Attorney ___ Patient Written Authorization ___

Estate/Executor Document ___ Other _____

Type of Photo ID Driver's License/State ID ___ Military ID ___ Passport ___
Other_____

Update to Patient Accounting Log _____ Yes _____ No _____ N/A

List of Patient Information/Documentation Released and Purpose:
_____
_____
_____

EXHIBIT G

Rural/Metro Corporation
Denial of Request for Access to Protected Health Information

Date: _____
Dear_____

We have carefully reviewed your request to have access to certain protected health information (PHI) that Rural/Metro Corporation and its subsidiaries has in its possession about you. Unfortunately, we are unable to grant your request for access to this information.
The basis for this denial is that:

1. _____ The information you requested was compiled in reasonable anticipation of, or use in, a civil, criminal or administrative action or proceeding;
2. _____ The information you requested was obtained from someone other than a health care provider under a promise of confidentiality and the access requested would be reasonably likely to reveal the source of the information.

The denials for reasons #1 or #2 are final and you may not appeal the decision to deny access to the information.

3. _____ 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;
4. _____ The protected health information makes reference to another person (other than a health care provider) and a licensed health professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to cause substantial harm to that person;
5. _____ The request for access is made by you as a personal representative of the individual about whom you are requesting the information, and a licensed health professional has determined, in the exercise of professional judgment, that access by you is reasonably likely to cause harm to the individual or another person.

Denials of access for reasons #3, #4, or #5 may be reviewed in accordance with the review procedures described below:

Review Procedures
If the denial of your request for access to PHI is for reasons #3, 4 or 5, you may request a review of the denial of access by sending a written request to:

Rural/Metro Corporation
Corporate Compliance
9221 E. Via De Ventura
Scottsdale AZ 85258

We will designate a licensed health professional, who was not directly involved in the denial, to review the decision to deny you access. We will promptly refer your request to this designated review official. The review official will determine within a reasonable period of time whether the denial is appropriate. We will provide you with written notice of the determination of the designated review official.

You may also file a complaint in accordance with our complaint procedures (available upon request) if you are not satisfied with our determination.

Sincerely,

Rural/Metro

EXHIBIT H

Rural/Metro Corporation
Request for Amendment of Protected Health Information

Patient Name: _____

Address: _____

City: _____ State: _____ Zip Code: _____

Date of Service: _____

Customer Number: _____

Please note: A separate Request for Amendment of Protected Health Information form must be completed for each date of service you wish to amend.

Information to Amend:
Please check the field(s) that represents the type of information you would like to amend of the Designated Record Set (DRS).

____ Name
____ Marital Status
____ Billing Address
____ Mailing Address
____ Current Medical Condition*
____ Past Medical History*
____ Allergies*
____ Current Medications*
____ Responsible Party/Next of Kin
____ Other:
_____

Please specifically describe the information you are requesting to be amended. Attach a separate sheet if necessary.

Rural/Metro Corporation and its subsidiaries, in its capacity as a health care provider, is entitled to perform and bill for services based on all protected health information in its current form or upon which it has already relied until such time as the amended information becomes effective. Rural/Metro Corporation is not required to accept your request for amendment and will notify you in writing as to the decision on your request.

Your signature below indicates that you have agreed to accept these terms as they have been listed and to provide payment, if required, to The Company based on existing protected health information until such time that the amendments you have made are effective.

_____ _____
Patient Signature Date

*Any amendment request regarding patient current medical conditions, past medical history, current medications, allergies or any other medical information must be supported by documentation from the patient's physician or facility.

EXHIBIT I

Rural/Metro Corporation
Acceptance of Request for Amendment of Protected Health Information

DATE:

Dear:_____

We have reviewed your request for amendment to the protected health information (PHI) of _____. Please be advised that we have made the appropriate amendment to the PHI or record that was the subject of your request.

We are now requesting that you grant us permission to allow us to notify the person(s) with which the amendments need to be shared. We will provide to those individual(s) you identify to us as having received the PHI that has been amended as well as those persons or business associates that have such information and who may have relied on or could be reasonably expected to rely on the amended PHI.

Identify to us any individuals you know of who may need the amended PHI about you and sign the statement below giving us permission to provide them with the updated PHI.

If you have any questions, please contact _____, Privacy Representative at ( ) _____.

Sincerely,

Rural/Metro Corporation

By my signature below, I hereby agree to allow Rural/Metro Corporation to provide amended PHI that it may have about me to the following persons, and to others who Rural/Metro Corporation has identified have a need for such information, provided such information is furnished in accordance with federal and state laws, rules and regulations.

Contact information for persons I know need the amended PHI about me:

☐ Please check if none, sign and date form below and return to Rural/Metro

_____

_____

_____

_____ _____
Patient Signature Date

EXHIBIT J

Rural/Metro Corporation
Denial of Request for Amendment to Protected Health Information

Date: _____

Dear _____,

We have reviewed your request for amendment to the protected health information (PHI) of _____. Please be advised that we must deny your request to amend this information at this time.

The basis for this denial is:

- ☐ It has been determined information is complete and accurate as written
- ☐ The record was not created by Rural/Metro Corporation or its subsidiaries
- ☐ The record is not a part of the "Designated Record Set"
- ☐ Other: _____

You have the right to submit a written statement to us if you disagree with our denial of your request. You may file your statement directly to our privacy representative, _____at the address listed.

If you do not submit a statement disagreeing with our decision to deny your amendment request, you may request that we provide your initial request for amendment, and a copy of our denial of your request with any future disclosures of the protected health information (PHI) that was the subject of your request for denial.

You also have the right to file a complaint with us or with the federal government if you disagree with our decision to deny your request to amend your PHI. We have enclosed a copy of our Complaint Procedure, which outlines the steps you need to take to file either a complaint with us, or a complaint with the federal government.

Sincerely,

Privacy Representative
Rural/Metro Corporation

EXHIBIT K

Rural/Metro Corporation
Request for Restriction of Protected Health Information

Date: _____

Social Security #: _____

Patient Name: _____

Address: _____

City: _____ State: _____ Zip Code: _____

Date of Service: _____

Customer ID#: _____

Patient Rights: As a patient, you have the right to request restrictions to the uses and disclosures of your PHI. **Rural/Metro Corporation is not required to agree to any restrictions requested by the patient, however any restrictions agreed to by Rural/Metro Corporation are binding on Rural/Metro Corporation.**

Please indicate your request for restricted uses and disclosures of your PHI**.**

_____

_____

_____

_____ _____
Patient Signature Date

FOR AMBULANCE SERVICE USE ONLY

DATE RECEIVED _____

REQUEST ACCEPTED _____

REQUEST DENIED _____

DATE _____

REVIEWING OFFICIAL _____

NOTICE TO PATIENT _____

COMMENTS: _____

EXHIBIT L

Rural/Metro Corporation
Log for Processing External Complaints about Privacy Practices

DATE COMPLAINT RECEIVED	PATIENT NAME	DESCRIPTION OF COMPLAINT	DISPOSITION OF COMPLAINT

EXHIBIT M

Rural/Metro Corporation
Patient Procedure for Filing Complaints about Privacy Practices

YOU MAY MAKE A COMPLAINT DIRECTLY TO US

You have the right to make a complaint directly to the Privacy Official of Rural/Metro Corporation concerning our policies and procedures with respect to the use and disclosure of Protected Health Information ("PHI"), as defined by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). You may also make a complaint about concerns you have regarding our compliance with any of our established policies and procedures concerning the confidentiality and use or disclosure of your PHI or about the requirements of the HIPAA Privacy Rule.

All written complaints should be directed to our Privacy Official at the following address:

Corporate Compliance
Rural/Metro Corporation
9221 E. Via De Ventura
Scottsdale AZ 85258

Upon notification of a complaint, Rural/Metro Corporation will instruct the complainant of their rights under the HIPAA Privacy Rule.

YOU MAY ALSO MAKE A COMPLAINT TO THE GOVERNMENT

If you believe Rural/Metro Corporation is not complying with the applicable requirements of the Federal Privacy Rule, you may file a complaint with the Secretary of the U.S. Department of Health and Human Services. The HIPAA Privacy Rule states the following:

Requirements for filing complaints. Complaints under this section must meet the following requirements.

1. A complaint must be filed in writing, either on paper or electronically.
2. A complaint must name the entity that is the subject of the complaint and describe the acts or omissions believed to be in violation of the applicable requirements of the Federal Privacy Rule or the applicable standards, requirements and implementation specifications of subpart E of part 164 of the Federal Privacy Rule.
3. A complaint must be filed within 180 days of when the complainant knew or should have known that the act or omission complained of occurred, unless the Secretary waives this time limitation for good cause.
4. The Secretary may prescribe additional procedures for the filing of complaints, as well as the place and manner of filing, by notice in the Federal Register.

Investigation. The Secretary may investigate complaints. Such investigations may include a review of the pertinent policies, procedures or practices of the covered entity and of the circumstances regarding any alleged acts or omissions concerning compliance.

EXHIBIT N

EMPLOYEE CONFIDENTIALITY AGREEMENT OF THE COMPANY AND ITS SUBSIDIARIES (R/M)

I _____, have read and understand Rural/Metro Corporation's policies regarding the privacy of individually identifiable protected health information (PHI), as mandated by the Health Insurance Portability and Accountability Act of 1996 (HIPAA). In addition, I acknowledge that I have received training in R/M policies concerning PHI access, use, disclosure, storage and destruction as required by HIPAA.

In consideration of my employment or compensation from Rural/Metro Corporation, I hereby agree that I will not, at any time, during my employment or association with Rural/Metro Corporation, use, access or disclose PHI to any person or entity, internally or externally, except as required or permitted in the course of my duties and responsibilities with Rural/Metro Corporation, as set forth in Rural/Metro Corporation's privacy policies and procedures or as permitted under HIPAA. I understand that this obligation extends to any PHI that I may acquire during the course of my employment or association with Rural/Metro Corporation, whether in oral, written or electronic form and regardless of the manner in which access was obtained.

I understand and acknowledge my responsibility to apply Rural/Metro Corporation's policies and procedures during the course of my employment or association. I also understand that unauthorized use or disclosure of PHI will result in disciplinary action, up to and including termination of employment or association with Rural/Metro Corporation and the imposition of civil penalties and criminal penalties under applicable federal and state law as well as professional disciplinary action as appropriate.
I understand that this obligation will survive the termination of my employment or end of my association with Rural/Metro Corporation, regardless of the reason for such termination.

Signature _____ Date: _____

**Please sign and return Employee Confidentiality Agreement to the Human Resources Representative.*

**********For Human Resources Management Only**********

Date of Hire: _____

*ENTER VERIFICATION OF SIGNED EMPLOYEE CONFIDENTIALITY AGREEMENT (TRACKING # **710008**)*

Employee ID#: _____

Location: _____