Kenosha Radiology Center, LLC's Policy for Safeguarding PHI

I. Background

A. Privacy Rules.

The Health Insurance Portability and Accountability Act (HIPAA) mandated that the Department of Health and Human Services create federal regulations to set standards for the use, disclosure, safeguarding, tracking and disposal of Protected Health Information (PHI). In order to assure adherence to those regulations KRC has adopted the following policies and procedures.

B. Privacy Rules Summary

1. Identify what information and entities are covered
2. Define which health information may be used and disclosed with and without the patient's consent
3. Requires providing written notice to the patient describing the covered entity's privacy policies
4. Requires a good faith effort to secure the patient signature on the privacy rights notice
5. Authorizes patients to request a restricted use and disclosure of certain health information
6. Gives patients the rights to review their health records
7. Requires covered entities to track and log certain disclosures of health information
8. Requires the appointment of a privacy officer
9. Requires covered entities to establish written agreements with their business associates
10. Mandates reasonable safeguards for the handling of patients' records
11. Allows the States to adopt and enforce privacy rules if they are more stringent than Federal rules

C. KRC has adopted the following policies and procedures to assure compliance with the federal privacy rules.

II. Privacy Rules - Definitions

A. Covered Entity - Defined. The Privacy Rules apply to all covered entities and their business associates. A covered entity is defined as a health care provider, and health plan or a health care clearing House.

1. A health care provider is "…a provider of medical or health services…or any other person or organization who furnishes, bills, or is paid for health care in the normal course of business."
2. A health plan is - "…an individual or group plan that provides, or pays the cost of medical care…"

3. A health plan clearing house is -"…a public or private entity including a billing service…that processes or facilitates the processing of health information."

B. Protected Health Information (PHI) defined. PHI is defined by the Privacy rules as information (including demographics) collected from an individual by a health care provider, employer or health plan which relates to past, present, or future physical or mental health care or conditions of an individual or the provision of health care to an individual and which identifies the individual or could be reasonably believed to allow the identification of the individual.

C. Business Associate - defined. A business associate, a "…person who…performs, or assists in the performance of…A function or activity involving the use or disclosure of individually identifiable health information, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing or benefits management.

III. Permitted Uses of PHI

A. Uses of PHI - Without patient authorization. A covered entity may use PHI without the prior consent of the patient for: (1) the treatment of the patient; (2) to obtain payment for the care; (3) or for certain health care operations.

B. Uses of PHI - With patient authorization. PHI may also be used for any purpose authorized in writing in advance by the patient. If KRC intends to use the PHI for any purpose other than that described above, a written authorization signed by the patient is required. The authorization must identify all uses to which KRC intends or expects the PHI may be used and to whom the PHI may be disclosed. A signed copy of the authorization will be kept in the patient's medical record.

1. Refusal to sign - use of PHI. If the patient declines to sign the authorization form, KRC is nevertheless permitted to make disclosures of PHI consistent with the privacy policy. 2. Refusal to sign - documented. If the patient declines to sign an authorization form, that refusal to sign will be noted on the form and a copy of the form will be placed in the patients file. If a patient declines to sign an authorization, the PHI can only be used for limited purposes described above.

C. Minors. The federal privacy rules permit the disclosure of PHI to the parents of a minor patient, with or without the consent of the patient, unless specific state laws restrict such disclosures.

IV. Authorization Policies and Procedures

A. General Policy.

1. Uses. It is KRC's policy that a signed authorization must be obtained before any PHI is used or disclosed for any purpose other than that permitted by the privacy regulations. Any use or disclosure

requiring an authorization shall only be made to the extent and in the manner authorized.

2. Conditional Authorizations. KRC will not require a patient to sign any authorization as a condition of the provision of treatment or service, the third party payment for that treatment or service, the enrollment in any health plan or to be eligible for benefits.

B. Authorizations - Content. As required by the privacy regulations, all authorizations will contain (1) detailed description of what PHI is to be released, (2) purpose for the PHI authorization, (3) person(s) or entity(ies) to which the PHI is to be released by KRC, and (4) Signature and date line for the authorizing patient. KRC's approved authorization form is entitled, 'HIPAA COMPLIANT AUTHORIZATION FOR THE RELEASE OF PROTECTED HEALTH INFORMATION.'

C. Authorizations - Reliance on Third Parties. If a third party provides KRC any PHI for the purposes other than permitted in the privacy rule, KRC shall require that third party to provide it with a current valid authorization, signed by the patient, which expressly permits the intended use of the PHI.

V. Safeguarding PHI

A. KRC employees.
Employees are not permitted to access or attempt to access PHI unless required as a part of their employment duties and only if expressly informed of their right to access the PHI by management. The privacy officer shall maintain a list of all employees authorized to have such access and the dates that access began and ended.

1. Disclosure to Third Parties. No Employee is permitted to disclose PHI to any third party unless such disclosures are required in order to carry out the employee's job and only in accordance with these policies.

B. On-site Access by others. Any subcontractors, consultants, auditors, counsel, temporary employees, custodians or others with authorized access to KRC property will be permitted access to PHI only as required to carry out their duties and only after signing either a Confidentiality Agreement, Business Associated Agreement or similar agreement, whichever is most appropriate.

C. Electronic PHI

1. Storage. Access to all PHI created or stored in electronic format shall be protected by commercially appropriate anti-hacker and anti-virus software. The data shall be backed up per KRC policy and stored in a secure off site location. All archived PHI shall be maintained at a site with appropriate security to prevent unauthorized access.

2. Access. All PHI access shall be exclusively through the use of Pre-assigned controls solely to authorized employees. Temporary access may be granted to consultants and others as deemed necessary. Unique passwords will be given and then removed after completion of assigned work.

D. Non-electric PHI

1. Storage of all PHI shall be in locked file cabinets or locked Rooms which are secured to prevent access by unauthorized Access.

E. Copying and or Removal of PHI. No one is permitted to copy or remove PHI unless such copying is a permitted disclosure to a third party or patient in accordance with the privacy rule. No one is permitted to remove any PHI from the premises except to make a permitted disclosure.

F. Destruction and Disposal. When KRC no longer requires PHI in whatever form, it shall be returned to the appropriate party as may be called for in a written agreement. Otherwise, all PHI whether paper or electronic or copies shall be destroyed in a commercially reasonable fashion designed to assure that it cannot be read or accessed.

VI. Disclosing PHI

A. General Policy. KRC shall only disclose PHI to third parties in accordance with the privacy rule.

B. Accounting for Disclosures. KRC shall maintain a written record of all disclosures of PHI using a disclosure log, (except for those described in the privacy policy, permitted incidental disclosures and disclosures made in accordance with a valid 'Business Associate Agreement')

1. Reporting Disclosures to patients. By regulation, each patient is permitted a single accounting of PHI disclosures once a year. All accountings to patients shall be made in writing and only if the request is received in writing and signed by the patient.

VII. Amending PHI

A. General Policy. KRC will not alter, correct or delete PHI unless fully satisfied that the change is warranted and will result in the correction of a material error in the PHI.

B. Patient Request. Patients have a right to request their PHI be corrected. However, KRC is required to make corrections requested by a patient only if the request is necessary to correct a material error in the PHI.

1. In writing. Any patient request to change PHI shall be in writing signed and dated by the patient and must state with clarity the reason for the requested changed. If KRC declines to make the requested change, the patient will be informed of the decision and the reason for the action.

2. Decisions. Any decision to approve or refuse a patient's request shall be made to the security officer. The patient shall also be advised that KRC reserves the right to inform all third parties to whom the inaccurate PHI was previously provided.

VIII. Effect of the State Privacy Laws

A. In General. The Federal Privacy Rules create certain authorized Uses and Restrictions on the use of PHI. The Federal rules expressly defer to State privacy laws where those laws are more stringent than the Federal privacy rules.

IX. Privacy Officer

A. Appointment. The privacy rules require that all covered entities appoint a privacy officer responsible for assuring that the entity's privacy policies are kept current and are being followed. KRC has appointed Carol Pilger to serve as its privacy officer.

X. Violation of Privacy Policies

A. General. The privacy rules impose substantial civil and criminal Penalties, including fines and imprisonment, on individuals and entities which make uses or disclosures of PHI in violation of the rules.

B. KRC Policy. Under some circumstances, KRC can be held liable for the actions of its employees who violate the privacy rules. KRC has therefore established specific internal discipline for employees.

XII. KRC Discipline for Privacy Violations

KRC has adopted the above policies and procedures regarding the uses and safeguarding of PHI and EPHI. In order to increase the likelihood of adherence to these policies and procedures, KRC has included the following specific forms of discipline for employees who violate those policies.

A. Employees - Non Disclosure. A violation of an internal policy or procedure which does not result in a prohibited use or disclosure of PHI. First Offense - Letter of reprimand. Second Offense - punishment up to but not including termination. Third Offense - Termination

B. Disclosure. A violation of an internal policy or procedure which does result in a disclosure of PHI: Negligent disclosure - first offense: up to suspension.
Second offense: Termination. Reckless or intentional disclosure - First offense: up to and including Termination. Second offense: Termination. Disclosure for profit. First offense: Termination. Disclosure that results in embarrassment or ridicule to the patient or was intended to have such a result - First offense: Termination. Disclosure to the Media with the intent or expectation that it would be published - First offense: Termination.