HIPPA PRIVACY POLICY

Radiology Consultants of Little Rock, P.A.

Last Revision Date

November 20, 2015

HIPAA Privacy Policy for Radiology Consultants

Table of Contents

Section I: Privacy

4. Privacy Notice
    - Notice of Privacy Practices
    - Policy - Providing Patient with the Notice of Privacy Practices
    - Procedure – Providing the Patient with the Notice of Privacy Practices
    - Receipt of Notice of Privacy Practices Form
    - Policy – Documentation Patient Received Privacy Notice and Retention of Notice
    - Procedure – Documentation Patient Received Privacy Notice and Retention of Notice
    - Procedure - Revising/Updating Privacy Notice
    - Procedure - Revising the Electronic Notice
    - Policy - Statement of Right to Change Privacy Notice and Policy and Procedures
    - Procedure - Electronic Notice
    - Procedure - Explaining to Patient How to Access Electronic Notice
    - Policy – Electronic Mail
    - Policy - Employee E-mail Usage

5. Patient Rights
    - Policy - Individual's Right to Access/Inspect or Obtain a Copy of PHI
    - Procedure - Individual's Right to Access/Inspect or Obtain a Copy of PHI
    - Policy - Verifying the Identity of the Person Requesting Information
    - Procedure - Verifying the Identity of the Person Requesting Information
    - Policy - Entity's Right to Deny Access
    - Procedure - Entity's Right to Deny Access
    - Policy -Timely Action to Respond to Request for PHI
    - Procedure - Timely Action to Respond to Request for PHI:
        - Providing Access
        - Amendments
        - Denials
    - Policy - Handling Requests for PHI:
    - Procedure - Handling Requests for:
        - PHI
        - Access to PHI
        - Amendments to PHI
        - Restrictions to PHI and Terminating Restrictions
        - Request to Restrict Disclosures of PHI
    - Procedure – Denial Process for:
        - Amendments to PHI
        - Access to PHI
        - Restrictions to PHI and Terminating Restrictions
    - Procedure – Documentation of Requests, Denials, and Other Actions
    - Policy – Individual's Rights to Request Restriction and Entity's Rights to Deny
    - Policy – Confidential Communications, Including Alternative means or Locations
    - Procedure - Confidential Communications, Including Alternative Means or Locations
    - Policy – Individual's Rights to Request Amendment to PHI; Entity's Rights to Deny
    - Policy – Individual's Rights to Disagree with Denial for Amendment
    - Procedure - Individual's Rights to Disagree with Denial for Amendment

- Policy – Entity's Right to Rebuttal
- Procedure – Entity's Right to Rebuttal
- Policy – Individual's Right to Have Review of Denial
- Procedure - Individual's Right to Have Review of Denial
- Policy – Designation of Outside Resource
- Procedure – Designation of Outside Resource
- Policy – De-Identification of PHI
- Procedure - De-Identification of PHI
- Policy – Use of PHI for Marketing Purposes
- Procedure – Use of PHI for Marketing Purposes
- Policy – Communicating With Patients About Their Rights
- Procedure - Communicating With Patients About Their Rights
- Procedure – Handling Confidential Communications
- Policy - Individual's Right to Access/Obtain an Accounting of Disclosures of PHI
- Procedure - Individual's Right to Access/Obtain an Accounting of Disclosures of PHI
- Form – Request for an Accounting of Disclosures
- Policy – Entity's right to suspend accounting of PHI
- Procedure – Entity's right to suspend accounting of PHI
- Policy – Timely Action for Accounting for Disclosures of PHI
- Procedure – Timely Action for Accounting for Disclosures of PHI
- Policy – Cost-based Fees for Multiple Accountings Within a 12-month Period
- Procedure - Cost-based Fees for Multiple Accountings Within a 12-month Period
- Policy - Documentation for Requests and Restrictions of PHI
- Procedure – Documentation for Requests and Restrictions of PHI
- Procedure – Processing Requests for an Accounting of Disclosures of PHI

6. Breaches

    - Sample Breach Notification Letter to Patient
    - Sample Policy on Notification of Breaches of Unsecured Protected Health Information

Section II: Training and Education

1. Training Policy
2. Training Procedure
3. Employee E-mail Usage Policy
4. Confidentiality Agreement

HIPAA Privacy and Security Standards

Policies and Procedures

Section I: Privacy Standards

Section I: Privacy Standards

1. Privacy Standards

Effective Date: April 14, 2003
Revised Date: November 20, 2015

Who Has Access to Patient PHI/ Minimum Necessary Information Based on Job Function

Policy:

1. For uses of protected health information, the Company will identify those persons or classes of persons in its workforce who need access to the information to carry out their duties. For each such person or classes of persons, it will identify the category or categories of access they need to perform their jobs and any conditions appropriate to such access. The Company will make reasonable efforts to limit the access of protected health information in accordance with these designations.

2. The Company finds that all physicians and medical personnel involved in the treatment of an individual need access to the individual's entire medical record, as do transcription, billing and coding personnel.

3. Front desk personnel who receive patients into the office will have access to patient medical records and will create a new electronic chart for the treating physician, check for the completion of patient forms used by the Company, organize charts or file materials for others in the chart, or to perform other delegated specific tasks.

Effective Date: April 14, 2003

Minimum Necessary Requirements

Policy:

1. Unless an exception listed below applies, the Company will make reasonable efforts not to use, disclose or request more than the minimum amount of protected health information necessary to accomplish the intended purpose of a use, disclosure or request.

2. The Company does not need to make a minimum necessary determination in the following circumstances:

    - Disclosures to or requests by a health care provider for treatment purposes.
    - Disclosures to the individual who is the subject of the information.
    - Uses or disclosures made pursuant to an authorization requested by the individual.
    - Uses or disclosures required for compliance with the standardized Health Insurance Portability and Accountability Act (HIPAA) transactions.
    - Disclosures to the Department of Health and Human Services (HHS) when disclosure of information is required under the rule for enforcement purposes.
    - Uses or disclosures that are required by other law.

Effective Date: April 14, 2003
Revised Date: November 20, 2015

Procedure for Minimum Necessary Information Based on Job Function

Procedure:

1. All personnel of the Company will be given passwords to access the PHI they need to perform their job.

2. Depending on the access rights attributed to a password, personnel will be permitted to view the fields they need to perform their basic job functions on our computer system.

3. The entire medical file, if necessary, may be accessed by our Physicians, x-ray techs, and front desk/medical record file personnel checking films and reports in and out to physician offices, etc.

Effective Date: April 14, 2003
Revised Date: November 20, 2015

Level of Information that can be Released to the Business Associate

Policy:

1. The Company will not disclose protected health information to a business associate unless it has first executed a written contract with the business associate which contains all of the provisions contained in the example found in the Business Associate Agreement. The Privacy Officer will be responsible for securing the appropriate contract from all of the Company's business associates and overseeing their duties.

2. If the Company becomes aware of a pattern of activity or practice of a business associate that constitutes a material breach or violation of the business associate's obligations under its contract, it will take reasonable steps to cure the breach or end the violation.

3. If the Company is unable to correct or cure the business associate violation, it will terminate the agreement, where feasible. The Privacy Officer will have the authority to terminate a business associate contract, subject to the approval of the Company's management. Where there are no feasible alternatives to the business associate or terminating would be unreasonably burdensome on the Company, the Company may choose not to terminate. If the Company finds that it is not practical to terminate, it must notify the Secretary of Health and Human Services of its decision.

4. The company may continue operating under certain existing written contracts with their Business Associates until April 14, 2004 without amending the contracts to include the Business Associate contract provisions. To qualify for the extension, the contract between the Business Associate and the Company must: (1) exist before the effective date of the HIPAA modifications and (2) not be modified or renewed between that date and April 14, 2003 (the Privacy Standards' compliance date). By April 14, 2004, all of the Company's Business Associate arrangements must be in conformance with the Privacy Rule.

5. Business Associate has been updated to reflect the HITECH Act / Omnibus Rule.

Effective Date: April 14, 2003
Revised Date: November 20, 2015

Procedure for Level of Information that can be Released to a Business Associate

Procedure:

1. What is a Business Associate?

Business associate:

(1) Except as provided in paragraph (4) of this definition, business associate means, with respect to a covered entity, a person who:

> (i) On behalf of such covered entity or of an organized health care arrangement (as defined in this section) in which the covered entity participates, but other than in the capacity of a member of the workforce of such covered entity or arrangement, creates, receives, maintains, or transmits protected health information for a function or activity regulated by this subchapter, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, patient safety activities listed at 42 CFR 3.20, billing, benefit management, practice management, and repricing; or
>
> (ii) Provides, other than in the capacity of a member of the workforce of such covered entity, legal, actuarial, accounting, consulting, data aggregation (as defined in § 164.501 of this subchapter), management, administrative, accreditation, or financial services to or for such covered entity, or to or for an organized health care arrangement in which the covered entity participates, where the provision of the service involves the disclosure of protected health information from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the person.

(2) A covered entity may be a business associate of another covered entity.

(3) Business associate includes:

> (i) A Health Information Organization, E-prescribing Gateway, or other person that provides data transmission services with respect to protected health information to a covered entity and that requires access on a routine basis to such protected health information.
>
> (ii) A person that offers a personal health record to one or more individuals on behalf of a covered entity.

(iii) A subcontractor that creates, receives, maintains, or transmits protected health information on behalf of the business associate.

(4) Business associate does not include:

(i) A health care provider, with respect to disclosures by a covered entity to the health care provider concerning the treatment of the individual.

(ii) A plan sponsor, with respect to disclosures by a group health plan (or by a health insurance issuer or HMO with respect to a group health plan) to the plan sponsor, to the extent that the requirements of § 164.504(f) of this subchapter apply and are met.

(iii) A government agency, with respect to determining eligibility for, or enrollment in, a government health plan that provides public benefits and is administered by another government agency, or collecting protected health information for such purposes, to the extent such activities are authorized by law.

(iv) A covered entity participating in an organized health care arrangement that performs a function or activity as described by paragraph (1)(i) of this definition for or on behalf of such organized health care arrangement, or that provides a service as described in paragraph (1)(ii) of this definition to or for such organized health care arrangement by virtue of such activities or services.

2. We will initiate a Business Associate Agreement with the following types of business that provide services such as the ones listed below:

Level I – This is the highest level of PHI given out for in order to get claims paid by the insurance companies and satisfy any attorney requesting information for lawsuits. The type of information that may be distributed will be name, address, telephone and fax numbers, social security numbers, date of birth, date of service, medical record numbers, Insurance numbers, account numbers, referring physician, diagnosis, CPT codes and insurance response. This information is given out by mail, electronic mail, and fax.

- Claims processing or administration
- Billing
- Legal
- Accounting

Level II – People with access to our computer system and reports.

- Computer support
- Data analysis, processing or administration

Level III – These people are not given any PHI, but may come in contact with information when in the office providing services in various areas.

- Equipment maintenance on x-ray machines
- Service to Dictaphone and transcription equipment, printers and fax machines, etc.
- Shredding service and mail pickup

HIPAA BUSINESS ASSOCIATE AGREEMENT

This Business Associate Agreement ("BAA") is entered into by and between Radiology Consultants of Little Rock, P.A. ("Covered Entity") and _____ ("Business Associate") as of the____day of_____, 20 (the "Effective Date").

RECITALS

A. WHEREAS, Radiology Consultants of Little Rock, P.A. is a "Covered Entity" as defined under the Health Insurance Portability and Accountability Act of 1996 (Pub. L. No. 104-191) and its implementing regulations (collectively, "HIPAA"), as amended by the regulations promulgated pursuant to the Health Information Technology for Economic and Clinical Health ("HITECH") Act (Division A, Title XIII and Division B, Title IV of Pub. L. No. 111–5) (which was part of the American Recovery and Reinvestment Act of 2009), and _____ is a "Business Associate" as defined under HIPAA; and

B. WHEREAS, in connection with the Agreement for Access to Web Portal between Covered Entity and Business Associate (the "Agreement"), Covered Entity may provide Business Associate with Protected Health Information ("PHI") (defined below); and

C. WHEREAS, Covered Entity and Business Associate intend to protect the privacy and provide for the security of PHI disclosed to Business Associate pursuant to this BAA, which is drafted to satisfy specific components of HIPAA, including the Privacy Rule (defined below), the Security Rule (defined below) and the Breach Notification Rule (defined below).

NOW, THEREFORE, in consideration of the mutual promises below and the exchange of information pursuant to this BAA, the parties agree as follows:

1. DEFINITIONS

a. "Breach" shall have the meaning given to such term at 45 C.F.R. § 164.402 and applicable State data breach notification law.

b. "Breach Notification Rule" shall mean the rule related to breach notification for Unsecured Protected Health Information at 45 C.F.R. Parts 160 and 164.

c. "Designated Record Set" shall have the meaning given to such term under the Privacy Rule at 45 C.F.R. § 164.501.

d. "Electronic Protected Health Information" or "EPHI" shall have the same meaning given to such term under the Security Rule, including, but not limited to, 45 C.F.R. § 160.103, limited to the information created or received by Business Associate from or on behalf of Covered Entity.

e. "Privacy Rule" shall mean the Standards for Privacy of Individually Identifiable Health Information, codified at 45 C.F.R. Parts 160 and Part 164, Subparts A and E.

f. "Protected Health Information" or "PHI" shall have the meaning given to such term under the Privacy and Security Rules at 45 C.F.R. § 160.103, limited to the information created or received by Business Associate from or on behalf of Covered Entity.

g. "Security Rule" shall mean the Security Standards for the Protection of Electronic Protected Health Information, codified at 45 C.F.R. § 164, Subparts A and C.

h. Other terms used, but not otherwise defined, in this BAA shall have the same meaning as those terms in the Privacy, Security or Breach Notification Rules.

2. PRIVACY RULE PERMITTED USES AND DISCLOSURES OF BUSINESS ASSOCIATE

a. Permitted Uses and Disclosures of PHI. Except as provided in Paragraphs (b), (c), and (d), below, Business Associate may only use or disclose PHI to perform functions, activities or services for, or on behalf of Covered Entity, as specified in the Agreement.

b. Use for Management and Administration. Except as otherwise limited in this BAA, Business Associate may, consistent with 45 C.F.R. 164.504(e)(4), use PHI if necessary (i) for the proper management and administration of Business Associate, or (ii) to carry out the legal responsibilities of Business Associate.

c. Disclosure for Management and Administration. Except as otherwise limited in this BAA, Business Associate may, consistent with 45 C.F.R. 164.504(e)(4), disclose PHI for the proper management and administration of Business Associate, provided (i) the disclosure is Required by Law, or (ii) Business Associate obtains reasonable assurances from the person to whom the PHI is disclosed ("Person") that it will be held confidentially and will be used or further disclosed only as Required by Law or for the purpose for which it was disclosed to the Person, and that the Person agrees to immediately notify Business Associate in writing of any instances of which it becomes aware in which the confidentiality of the information has been breached or is suspected to have been breached.

d. Reporting Violations. Business Associate may use PHI to report violations of law to appropriate Federal and State authorities, consistent with 45 C.F.R. § 164.502(j)(1).

3. PRIVACY RULE OBLIGATIONS AND ACTIVITIES OF BUSINESS ASSOCIATE

a. Limitations on Disclosure. Business Associate shall not use or disclose PHI other than as permitted or required by this BAA, the Agreement, or as Required by Law. Business Associate shall not use or disclose PHI in a manner that would violate the Privacy Rule if done by Covered Entity, unless expressly permitted to do so pursuant to the Privacy Rule, the Agreement, and this BAA.

b. Appropriate Safeguards. Business Associate shall use appropriate safeguards to prevent the use or disclosure of PHI other than as permitted by the Agreement, this BAA, or as Required by Law.

c. Obligations on Behalf of Covered Entity. To the extent Business Associate carries out an obligation for which Covered Entity is responsible under the Privacy Rule, Business Associate must comply with the requirements of the Privacy Rule that apply to Covered Entity in the performance of such obligation.

d. Mitigation. Business Associate shall mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of PHI by Business Associate in violation of the requirements of HIPAA, the Agreement, or this BAA.

e. Reporting of Improper Use or Disclosure. Business Associate shall report to Covered Entity in writing any use or disclosure of PHI not permitted by this BAA within five (5) days of becoming aware of such use or disclosure.

f. Business Associate's Subcontractors. Business Associate shall ensure, consistent with 45 C.F.R. § 164.502(e)(1)(ii), that any Subcontractor that creates, receives, maintains, or transmits PHI on behalf of Business Associate agrees in writing to the same restrictions and conditions that apply through this BAA to Business Associate with respect to such PHI.

f. Access to PHI. Business Associate shall provide access, at the request of Covered Entity, and in the time and manner reasonably designated by Covered Entity, to PHI in a Designated Record Set, to Covered Entity or, as directed by Covered Entity, to an Individual or a third party designated by the Individual, in order to meet the requirements under the Privacy Rule at 45 C.F.R. § 164.524.

g. Amendment of PHI. Business Associate shall make any PHI contained in a Designated Record Set available to Covered Entity (or an Individual as directed by Covered Entity) for purposes of amendment per 45 C.F.R. § 164.526. Business Associate shall make any amendment(s) to PHI in a Designated Record Set that Covered Entity directs or agrees to pursuant to the Privacy Rule, at the request of Covered Entity, and in the time and manner reasonably designated by Covered Entity. If an Individual requests an amendment of PHI directly from Business Associate or its Subcontractors, Business Associate shall notify Covered Entity in writing within five (5) days of receiving such request. Any denial of amendment of PHI maintained by Business Associate or its Subcontractors shall be the responsibility of Covered Entity.

h. Accounting of Disclosures. Business Associate shall provide to Covered Entity in the time and manner designated by Covered Entity, information collected in accordance with Section 3(i) of this BAA, to permit Covered Entity to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 C.F.R. § 164.528. In the event that the request for an accounting is delivered directly to Business Associate or its Subcontractors, Business Associate shall provide a copy of such request to Covered Entity, in writing, within five (5) days of Business Associate's receipt of such request.

i. Documentation of Disclosures. Business Associate shall document disclosures of PHI and information related to such disclosures as would be required for Covered Entity to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 C.F.R. § 164.528. At a minimum, such information shall include: (i) the date of disclosure; (ii) the name of the entity or person who received PHI and, if known, the address of the entity or person; (iii) a brief description of the PHI disclosed; and (iv) a brief statement of the purpose of the disclosure that reasonably informs the Individual of the basis for the disclosure, or a copy of the Individual's authorization, or a copy of the written request for disclosure.

j. Retention of PHI. Notwithstanding Section 6(c) of this BAA, Business Associate and its Subcontractors shall retain all PHI throughout the term of the Agreement and shall continue to maintain

the information required under Section 3(i) of this BAA for a period of six (6) years after termination of the Agreement.

k. Governmental Access to Records. Business Associate shall make its internal practices, books and records, including policies and procedures and PHI, relating to the use and disclosure of PHI received from, or created or received by Business Associate on behalf of Covered Entity available to the Secretary and Covered Entity for purposes of determining Covered Entity's compliance with the Privacy Rule as applicable.

l. Minimum Necessary. Business Associate shall only request, use and disclose the Minimum Necessary amount of PHI necessary to accomplish the purpose of the request, use or disclosure.

4. SECURITY RULE OBLIGATIONS OF BUSINESS ASSOCIATE

a. Compliance with the Security Rule. Business Associate agrees to comply with the Security Rule with respect to Electronic Protected Health Information and have in place reasonable and appropriate Administrative, Physical, and Technical Safeguards to protect the Confidentiality, Integrity, and Availability of EPHI and to prevent the use or disclosure of EPHI other than as permitted by the Agreement, this BAA, and as Required by Law.

b. Subcontractors. Business Associate shall ensure that any Subcontractor that creates, receives, maintains, or transmits EPHI on behalf of Business Associate agrees in writing to comply with the Security Rule with respect to such EPHI.

c. Security Incident/Breach Notification Reporting. Business Associate shall report any Security Incident promptly upon becoming aware of such incident. Separate from the requirements related to Security Incident reporting, Business Associate shall also make the reports set forth below in Section 5, related to a Breach of Unsecured PHI.

5. BREACH NOTIFICATION (FEDERAL AND STATE) RULE OBLIGATIONS OF BUSINESS ASSOCIATE

a. Notification Requirement. Immediately following Business Associate's discovery of a Breach, or upon Business Associate's reasonable belief that a Breach has occurred, Business Associate shall provide written notification of such Breach to Covered Entity.

b. Discovery of Breach. For purposes of reporting a Breach to Covered Entity, the discovery of a Breach shall occur on the first day on which such Breach is known to Business Associate or, by exercising reasonable diligence, would have been known to or suspected by Business Associate. Business Associate will be considered to have had knowledge of a Breach if the Breach is known, or by exercising reasonable diligence would have been known to any person (other than the person committing the Breach) who is an employee, officer or agent of the Business Associate.

c. Content of Notification. Any notice referenced above in Section 5(a) of this BAA will include, to the extent known to Business Associate, the identification of each individual whose Unsecured PHI has been, or is reasonably believed by Business Associate to have been accessed, acquired, or disclosed during such Breach, as well as the information, to the extent known by Business Associate, that Covered Entity is required to include in its notification to the individual pursuant to the

Breach Notification Rule or applicable State data breach notification laws. Business Associate will also provide (on a continuing basis as information is discovered) to Covered Entity other available information that Covered Entity is required to include in its notification to the individual pursuant to the Breach Notification Rule or applicable State data breach notification laws.

d. Cooperation with Covered Entity. Business Associate shall:

(i) Cooperate and assist Covered Entity with any investigation into any Breach or alleged Breach, including those conducted by any Federal agency, State Attorney General, or State agency (or their respective agents);

(ii) Comply with Covered Entity's determinations regarding Covered Entity's and Business Associate's obligations to mitigate to the extent practicable any potential harm to the individuals impacted by the Breach; and

(iii) As directed by the Covered Entity, assist with the implementation of any decision by Covered Entity or any Federal agency, State agency, including any State Attorney General, or their respective agents, to notify and provide mitigation to individuals impacted or potentially impacted by a Breach.

6. TERM AND TERMINATION

a. Term. The term of this BAA shall commence as of the Effective Date, and shall terminate when all of the PHI provided by Covered Entity to Business Associate, or created or received by Business Associate on behalf of Covered Entity, is destroyed or returned to Covered Entity or, if it is infeasible to return or destroy PHI, protections are extended to such information, in accordance with the provisions of this Section 6.

b. Termination for Cause. Upon Covered Entity's knowledge of a material breach of the terms of this BAA by Business Associate, Covered Entity shall:

(i) Provide an opportunity for Business Associate to cure, and, if Business Associate does not cure the breach within thirty (30) days, Covered Entity may immediately terminate this BAA and the Agreement;

(ii) Immediately terminate this BAA and the Agreement if Covered Entity has determined that (a) Business Associate has breached a material term of this BAA, and (b) cure is not possible; or

(iii) Immediately terminate this BAA if the Agreement has been terminated.

c. Effect of Termination.

(i) Except as provided in paragraph (ii) of this Section 6(c), upon termination of this BAA for any reason, Business Associate shall return or destroy all PHI received from Covered Entity, or created or received by Business Associate on behalf of Covered Entity, and shall retain no copies of the PHI except as required by the Agreement. This provision shall apply to PHI that is in the possession of Subcontractors of Business Associate.

(ii) In the event that Business Associate determines that returning or destroying the PHI is infeasible, Business Associate shall provide to Covered Entity notification of the conditions that make return or destruction infeasible. Upon mutual agreement of the parties that return or destruction of PHI is infeasible, Business Associate shall extend the protections of this BAA to such PHI and limit further uses and disclosures of such PHI to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains such PHI.

7. MISCELLANEOUS

a. Regulatory References. A reference in this BAA to a section in the Privacy, Security, or Breach Notification Rule means the section as in effect or as amended, and for which compliance is required.

b. Survival. The respective rights and obligations of Business Associate under Section 6(c) of this BAA shall survive the termination of the BAA.

c. No Third Party Beneficiaries. Nothing express or implied in this BAA is intended to confer, nor shall anything herein confer, upon any person other than Covered Entity, Business Associate and their respective successors or assigns, any rights, remedies, obligations or liabilities whatsoever.

d. Amendment. This Agreement replaces all prior understandings or agreements, written or oral, regarding the subject matter hereof. The parties agree to take such action as is necessary to amend this BAA in writing from time to time as is necessary for Covered Entity to comply with the requirements of the Privacy, Security or Breach Notification Rules, as well as HIPAA and HITECH.

e. Effect on Agreement. Except as specifically required to implement the purposes of this BAA, or to the extent inconsistent with this BAA, all other terms of the Agreement shall remain in force and effect.

f. Interpretation. The provisions of this BAA shall prevail over any provisions in the Agreement that may conflict or appear inconsistent with any provision in this BAA. Any ambiguity in this BAA shall be resolved to permit Covered Entity to comply with the Privacy, Security, and Breach Notification Rules, as well as HIPAA and HITECH.

g. Disclaimer. Covered Entity makes no warranty or representation that compliance by Business Associate with this BAA is satisfactory for Business Associate to comply with any obligations it may have under HIPAA, the Privacy Rule, or any other applicable law or regulation pertaining to the confidentiality, use or safeguarding of health information. Business Associate is solely responsible for all decisions it makes regarding the use, disclosure or safeguarding of PHI.

h. Indemnification.

(i) Business Associate shall indemnify, defend and hold Covered Entity and its officers, directors, employees, agents, successors and assigns ("Covered Entity Indemnitees") harmless, from and against any and all losses, claims, actions, demands, liabilities, damages, costs and expenses (including, but not limited to, costs of providing notifications and credit monitoring services to individuals pursuant to the Breach Notification Rule and State data breach notification laws, administrative costs associated with Covered Entity's and Business Associate's compliance with Breach

Notification Rule and State data breach notification laws, judgments, settlements, court costs and reasonable attorneys' fees actually incurred) (collectively, "Information Disclosure Costs") arising from or related to: (1) any breach of this BAA by Business Associate, including but not limited to the use or disclosure by Business Associate of Individually Identifiable Information (including PHI) in violation of the terms of this BAA or applicable law; and (2) whether in oral, paper or electronic media, any Breach caused, directly or indirectly, by Business Associate.

i. Counterparts. This BAA may be executed in multiple counterparts, each of which shall be deemed an original but all of which together shall constitute one and the same instrument. Facsimile or electronic (PDF) signatures shall be treated as original signatures. This BAA shall be binding when one or more counterparts hereof, individually or taken together, shall bear the signatures of all of the parties reflected on this BAA as the signatories thereto.

IN WITNESS WHEREOF, the parties hereto have duly executed this BAA as of the Effective Date.

Covered Entity	Business Associate
Sign_____	Sign_____
Print_____	Print_____
Title_____	Title_____

Effective Date: April 14, 2003

Privacy Policy

1. The Company will use and disclose protected health information only as permitted by the HIPAA Privacy Standards and this Compliance Program. Protected health information means individually identifiable health information[1] transmitted or maintained in any format (written, electronic, or oral), whether relating to a living or a deceased individual.

2. The Company is required to disclose protected health information when an individual requests access to certain health information in accordance with the Providing the Patient With the Notice of Privacy Practices policy or an accounting of disclosures in accordance with the Individual's Right to Access/Obtain an Accounting of Disclosures of PHI policy. The Company must also disclose protected health information when the Secretary of Health and Human Services (the "Secretary") requests information to determine the Company's compliance with the HIPAA Privacy Standards. Any request for access or an accounting, or a request from the Secretary will be forwarded immediately to the Privacy Officer who will coordinate the Company's efforts. The Privacy Officer shall log each such request as well as the Company's follow-up to each such request.

3. The Company may use or disclose protected health information without patient permission only in certain, public policy-related circumstances.

4. It may also use and disclose protected health information for treatment, payment and health care operation purposes without patient permission, unless another law requires it.

5. In general, for all other purposes, the Company must obtain the individual's permission before it uses or discloses the individual's protected health information. There are two forms of permission under the HIPAA Privacy Standards: oral agreement and authorization.

6. The Company will obtain the patient's verbal agreement before disclosing protected health information to persons assisting in a patient's care. The agreement does not have to be in writing and may be inferred from the circumstances. See the Uses and Disclosures Pursuant to Individual Agreement policy.

---

[1] Individually identifiable health information is that subset of health information that:

- Is created by or received by a health care provider, health plan, employer, or health care clearinghouse;
- Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and
- Which identifies the individual or which provides a reasonable basis to believe that it could probably be used to identify the individual who is the subject of the information.

Effective Date: April 14, 2003
Revised Date: November 20, 2015

Disciplinary Actions for Unauthorized Access, Use Or Disclosure

Policy:

1. Any unauthorized access, use or disclosure of PHI will be brought to the attention of the Privacy Officer. The Privacy Officer will be responsible for all reports of issues and will conduct any necessary investigation into those reports.

2. An unauthorized access, use or disclosure of PHI will be dealt with on a case by case basis depending on the severity of the access, use or disclosure.

3. Examples of behavior on the part of individuals that could require remedial actions that are done to correct mistakes might include:

    - Failure of an individual to understand and carry out required procedures and policies
    - Inappropriate or Improper implementation of the policies and procedures
    - Negligent behavior

4. In cases of intentional misconduct, repeated violations, or after documented remedial actions have failed to correct the problem disciplinary action will be imposed that may include:

    - Verbal or written warnings
    - Placing the individual in a different position
    - Probation
    - Termination of employment
    - Other disciplinary action felt to be appropriate for the specific misconduct

5. The initiation of corrective or disciplinary action by Radiology Consultants does not preclude or replace any criminal proceedings that may be taken by the Department of Human Services.

Effective Date: April 14, 2003
Revised Date: November 20, 2015

Procedure for Disciplinary Actions for Unauthorized Access, Use or Disclosure

Procedure:

1. After the Privacy Officer conducts the necessary investigation into the unauthorized access, use or disclosure of PHI and determines the nature of the incident, they will meet with the employee and the supervisor or manager.

2. The disciplinary action imposed will depend on the nature, severity and frequency of the violation and may include one or more of the following:

    - The individual may be required to take part in retraining focused on the problem area
    - The individual may be reassigned or there may be a change of duty
    - Verbal and/or written warnings
    - Probation
    - Termination of employment
    - Other disciplinary action felt to be appropriate for the specific misconduct

Effective Date: April 14, 2003
Revised Date: November 20, 2015

Reporting Incidents of Unauthorized Access, Use Or Disclosure

Policy:

1. We encourage any individual to report instances of suspected misuse or report incidents of unauthorized access, use or disclosure of PHI to their supervisor or the Privacy Officer.

2. This office will not tolerate retaliation against personnel who report suspected violations.

Effective Date: April 14, 2003
Revised Date: November 20, 2015

Procedure for Reporting Incidents of Unauthorized Access, Use or Disclosure

Procedure:

1. The individual may report to their immediate Supervisor any concerns of unauthorized access, use or disclosure.

2. The individual will be asked to put their concern in writing and it will be submitted to the Privacy Officer.

3. The Privacy Officer will conduct an investigation and determine if disciplinary action will be required.

Effective Date: April 14, 2003

Whistleblower Policy

Policy:

1. All Radiology Consultants personnel are strongly encouraged to report issues, concerns or suspected violations of HIPAA in writing to the Privacy Officer.

2. Radiology Consultants will not tolerate retaliation against any personnel who report suspected violations.

Section I: Privacy Standards

2. Privacy Administrative Tasks

Effective Date: April 14, 2003

Sanctions for Failing to Comply With Privacy Policies and Procedures

Policy:

1. As a condition of employment or other affiliation with the Company, all Company personnel are required to follow the Company's policies and procedures concerning the use and disclosure of protected health information. The Company shall impose appropriate disciplinary action upon any personnel who fail to comply with applicable laws or this Compliance Program.

2. Officers and managers are responsible for disciplining personnel in an appropriate and consistent manner. The type of disciplinary action shall be determined on a case-by-case basis, and where appropriate, in consultation with the Privacy Officer and the Company's management.

3. The range of sanctions shall include oral warnings, written warnings, oral reprimands, written reprimands, demotion, probation, or termination.

4. Punishment for serious violations may subject an individual to immediate termination.

5. Nothing in this policy shall be interpreted as granting employees of the Company any right to challenge or seek further review of the disciplinary action imposed upon them by their supervisor or by any other officer or agent of the Company. The review processes are for the sole benefit of the Company to enhance the effectiveness of its Compliance Program.

Effective Date: April 14, 2003

Procedure for Sanctions for Failing to Comply with Privacy Policies and Procedures

Procedure:

1. Any personnel found not following the policies and procedures of HIPAA will face disciplinary action by their Supervisor or the Privacy Officer.

2. The type of disciplinary action shall be determined on a case-by-case basis, and may include one or more of the following:

    - The individual may be required to take part in retraining focused on the problem area
    - The individual may be reassigned or there may be a change of duty
    - Verbal and/or written warnings
    - Probation
    - Termination of employment
    - Other disciplinary action felt to be appropriate for the specific misconduct

Effective Date: April 14, 2003

Non-retaliation Policy

Policy:

1. The Company will not require individuals to waive their rights to file a complaint with the Secretary of the Department of Health and Human Services or their other rights under the HIPAA Privacy Standards as a condition to receiving treatment. Personnel are also prohibited from retaliating against any person who files a complaint with the Secretary or testifies, assists, or participates in certain investigations, compliance reviews, proceedings and hearings under the Administrative Simplification provisions of HIPAA.

2. All personnel are prohibited from retaliating against patients for exercising their rights granted under HIPAA or participating in any process established by the HIPAA Privacy Standards, such as filing a complaint against the Company

Effective Date: April 14, 2003

Processing Complaints

Policy:

1. The Company will provide a process for any individual to raise issues to the Company regarding the Company's policies and procedures concerning the use and disclosure of protected health information and its compliance with those policies and procedures and the requirements of HIPAA.

2. The Privacy Officer will be responsible for all reports of issues, will conduct any necessary investigation into those reports, and will attempt to resolve complaints and take corrective measures, if necessary.

3. The Privacy Officer will routinely report the outcome of investigations to the Company's management. Individuals who file a report will be notified of the disposition as soon as justification is complete. The Privacy Officer will document all reports received and dispositions of such reports.

Effective Date: April 14, 2003

Procedure for Processing Complaints

Procedure:

1. Any individual may discuss issues with his or her supervisor, manager, or team leader regarding the use and disclosure of protected health information. If the individual is not comfortable speaking with a direct supervisor or manager, he or she can contact the Administrator/Privacy Officer.

2. The individual will be required to submit their concerns in writing.

3. The Privacy Officer will conduct an investigation and attempt to resolve the complaint and take corrective measures that may be needed.

4. The Privacy Officer will maintain documentation of the complaints received and their disposition.

5. The Privacy Officer will report the outcome of investigations to the Administrator or Security Officer.

6. Complaints may also be made with the Secretary of the Department of Health and Human Services (HHS).

Section I: Privacy Standards

3. Authorization

Effective Date: April 14, 2003
Revised Date: November 20, 2015

Obtaining Authorization

Policy:

1. Radiology Consultants will obtain an authorization from an individual to use and disclose the individual's protected health information where an individual's permission is required, but consents and oral agreement are not appropriate.

2. In other words, Radiology Consultants will obtain an authorization from an individual when it seeks to use or disclose the individual's protected health information for any purpose other than treatment, payment, health care operations or to make disclosures to persons assisting in an individual's care as discussed in the Uses and Disclosures Pursuant to Individual Agreement policy or for the public policy-related purposes.

3. Authorizations obtained by Radiology Consultants will contain all necessary elements.

4. Radiology Consultants will not use or disclose protected health information as outlined in an authorization if the authorization is not appropriate to use for any reason. The reasons include:

    - The expiration date has passed or the expiration event has occurred.
    - It has been revoked.
    - It has not been filled out completely, with respected to a required element.
    - Any material information contained in the authorization is known to be false.
    - The authorization is combined with another document in a way which inappropriately creates a compound authorization or the Company inappropriately conditioned treatment on the signature of the authorization.

5. Radiology Consultants will maintain an authorization for six (6) years from the date it became effective.

Effective Date: April 14, 2003

Procedure for Obtaining Authorization

Procedure for Diagnostic and CT Front Desk:

1. The front desk personnel will provide an Authorization form at the time of service for any patient to sign giving permission for a specific relative, person assisting in their care, guardian, or legal counsel to be able to obtain their PHI. Not all patients will need to sign this form at the time of service.

2. The form will be scanned into the patient's medical record and maintained for six years.

Procedure for Attorney Requests:

1. If the patient or attorney requests for PHI to be released, a signed Authorization form must be obtained with the patient's signature.

2. It can be mailed or faxed to the patient or attorney for the patient to sign.

3. Documentation will be made by putting a comment on the patient's file of receipt of the form and the name of the individual the PHI may be released.

4. The form will be scanned in the Correspondence File by the date the comment is placed on the account in the computer.

Radiology Consultants of Little Rock, P.A.

Authorization for the Use or Disclose Of Protected Health Information

I, _____ hereby authorize Radiology Consultants of Little Rock, P.A. to use or disclose Protected Health Information in the following manner:

_____Release to _____

(name of entity to receive information)

_____Release to _____

(name of physician office requesting information)

The following Protected Health Information_____

_____

_____

(Describe the information to be used or disclosed, including descriptors such as date of service, type of service, level of detail to be released or other specific information)

The Protected Health Information is being used or disclosed for the following purpose(s):_____

_____

(List specific purposes for the Protected Health Information)

This authorization is in full force and effect until _____*date*__ or ___*event that relates to patient or disclosure*, at which time this authorization to use or disclose Protected Health Information expires.

I understand that I have the right to revoke this authorization in writing by sending notification to Radiology Consultants of Little Rock, P.A. at 9601 Lile Drive, Suite 1100, Little Rock, AR 72205.

I understand when I revoke this authorization, it is not effective to the extent that Radiology Consultants of Little Rock, P.A. has already relied on the use or disclose of the Protected Health Information.

I also understand Protected Health Information released pursuant to this authorization may be re-disclosed by the party who received that information and may no longer be protected by federal or state law.

Radiology Consultants of Little Rock, P.A. will not condition my treatment or payment on whether I provide an authorization for the requested use or disclose.

I understand I have the following rights:

- To inspect or copy the Protected Health Information to be used or disclosed
- To refuse to sign this authorization (information will not be disclosed)

_____ _____

Signature Date

(Patient or Personal Representative)

_____

Name of Patient or Personal Representative

_____

Description of Personal Representative's Authority

Effective Date: April 14, 2002

Disciplinary Actions for Failure to Adhere to Process

Policy:

1. Anyone not following the procedures in obtaining, documenting, or retaining the authorization form will be brought to the attention of the Privacy Officer.

2. Examples of behavior on the part of individuals that could require remedial actions that are done to correct mistakes might include:

    - Failure of an individual to understand and carry out required procedures and policies
    - Inappropriate or Improper implementation of the policies and procedures
    - Negligent behavior

3. In cases of intentional misconduct, repeated violations, or after documented remedial actions have failed to correct the problem disciplinary action will be imposed that may include:

4. The initiation of corrective or disciplinary action by Radiology Consultants does not preclude or replace any criminal proceedings that may be taken by the Department of Human Services.

Effective Date: April 14, 2003

Procedure for Disciplinary Actions for Failure to Adhere to the Process (or errors in the process)

Procedure:

1. Any employee not adhering to the process for obtaining, documenting and storing the Authorization will face disciplinary action by the Supervisor and/or Privacy Officer.

2. The disciplinary action imposed will depend on the nature, severity and frequency of the violation and may include one or more of the following:

    - The individual may be required to take part in retraining focused on the problem area
    - The individual may be reassigned or there may be a change of duty
    - Verbal and/or written warnings
    - Probation
    - Termination of employment
    - Other disciplinary action felt to be appropriate for the specific misconduct

Effective Date: April 14, 2003

Documentation, Retention and Destruction of Authorization Forms

Policy:

In accordance with HIPAA regulations, Radiology Consultants will document the receipt of signed Authorization Forms in their computer system and maintain the form for a period of six years before destroying the form.

Effective Date: April 14, 2003
Revised Date: November 20, 2015

Procedure for Documentation, Retention and Destruction of Authorization Forms

Procedure:

1. All signed Authorization Forms received from a patient at either Front Desk or Patient Accounts will be documented on the patient's account in the computer by adding a comment of the expiration date and to whom the PHI may be released.

2. The Front Desk will file the form in the patient's demographics and the Patient Accounts Department will scan into the Correspondence File by the date the comment is placed on the account in the computer.

Effective Date: April 14, 2003
Revised Date: November 20, 2015

Determining Uses and Disclosures Allowed Under Authorization

All personnel will verify who they are speaking to, the patient or their representative, which they chose on their Authorization Form, by asking any of the following questions:

1. Social Security Number – last 4 digits
2. Date of Birth

Effective Date: April 14, 2003

How Patient Can Revoke Authorization

Policy:

1. The Company will permit patients to revoke their authorizations except to the extent that the Company has taken action in reliance on the authorization.

2. We will only permit patients of Radiology Consultants or HealthScreen Arkansas to revoke their authorization. If it is a patient from any hospital, private practice (such as Ortho Arkansas), LRDC, etc., we will direct them to the facility where their service was performed.

3. All revocations must be in writing to be effective by mail or fax.

4. Notification of revocations will be disseminated to all persons who handle the individual's protected health information on behalf of the company.

Effective Date: April 14, 2003
Revised Date: November 20, 2015

Procedure for How Patient Can Revoke Authorization

Procedure:

1. All revocations must be in writing to be effective by mail or fax to the Privacy Officer.

2. Notification of revocations will be disseminated to all persons who handle the individual's protected health information on behalf of the company.

3. A comment will be placed in the computer on the patient's account.

The request will be scanned in the patient's demographics by the Front Desk if it is an office patient and scanned into the Correspondence File by Patient Accounts if the patient is from another place of service

Effective Date: April 14, 2003
Revised Date: November 20, 2015

Procedure for Documenting Written Revocations

Procedure:

1. When a letter from an individual revoking authorization is received, a comment will be placed in the computer on the patient's account.

2. The letter will be scanned into the patient's demographics by the Front Desk if it is a Radiology Consultants' patient and scanned into the Correspondence File in the Patient Accounts Department if it from some other place

Effective Date: April 14, 2003

Procedure for Documentation of Validity/Term

Procedure:

1. All requests for PHI released will be verified with the patients recorded release forms.

2. The validity of such requests will be determined based on the information listed on the request form by the patient and checked against the expiration date on the form.

3. If the patient does not list an expiration date, a standard expiration date will be issued and recorded on the form of one year.

Section I: Privacy Standards

4. Privacy Notice

RADIOLOGY CONSULTANTS OF LITTLE ROCK, PA
9601 BAPTIST HEALTH DRIVE, SUITE 1100
LITTLE ROCK, AR 72205

NOTICE OF PRIVACY PRACTICES

Effective Date: April 14, 2003.
This Notice was most recently revised on November 20, 2015.

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

IF YOU HAVE ANY QUESTIONS ABOUT THIS NOTICE OR IF YOU NEED MORE INFORMATION, PLEASE CONTACT OUR PRIVACY OFFICER:

Privacy Officer: Lucille Whitlow
Mailing Address: 900 South Shackleford, #110, Little Rock, AR 72211
Telephone: 501-227-5130
Fax: 501-978-5417
E-mail: Lucille.whitlow@radconLR.com

About This Notice

We are required by law to maintain the privacy of Protected Health Information (PHI) and to give you this Notice explaining our privacy practices with regard to that information. You have certain rights – and we have certain legal obligations – regarding the privacy of your PHI, and this Notice also explains your rights and our obligations. We are required to abide by the terms of the current version of this Notice.

What is Protected Health Information (PHI)?

Protected Health Information (PHI) is information that individually identifies you and that we create or get from you or from another health care provider, a health plan, your employer, or a health care clearinghouse and that relates to (1) your past, present, or future physical or mental health or conditions, (2) the provision of health care to you, or (3) the past, present, or future payment for your health care.

How We May Use and Disclose Your PHI

We may use and disclose your PHI in the following circumstances:

For Treatment. We may use PHI to give you medical treatment or services and to manage and coordinate your medical care. For example, we may disclose PHI to

doctors, nurses, technicians, or other personnel who are involved in taking care of you, including people outside our practice, such as referring or specialist physicians.

For Payment. We may use and disclose PHI so that we can bill for the treatment and services you get from us and can collect payment from you, an insurance company, or another third party. For example, we may need to give your health plan information about your treatment in order for your health plan to pay for that treatment. We also may tell your health plan about a treatment you are going to receive to find out if your plan will cover the treatment. If a bill is overdue we may need to give PHI to a collection agency to the extent necessary to help collect the bill, and we may disclose an outstanding debt to credit reporting agencies.

For Health Care Operations. We may use and disclose PHI for our health care operations. For example, we may use PHI for our general business management activities, for checking on the performance of our staff in caring for you, for our cost-management activities, for audits, or to get legal services. We may give PHI to other health care entities for their health care operations, for example, to your health insurer for its quality review purposes.

Appointment Reminders/Treatment Alternatives/Health-Related Benefits and Services. We may use and disclose PHI to contact you to remind you that you have an appointment for medical care, or to contact you to tell you about possible treatment options or alternatives or health related benefits and services that may be of interest to you.

Minors. We may disclose the PHI of minor children to their parents or guardians unless such disclosure is otherwise prohibited by law.

Personal Representative. If you have a personal representative, such as a legal guardian (or an executor or administrator of your estate after your death), we will treat that person as if that person is you with respect to disclosures of your PHI.

As Required by Law. We will disclose PHI about you when required to do so by international, federal, state, or local law.

To Avert a Serious Threat to Health or Safety. We may use and disclose PHI when necessary to prevent a serious threat to your health or safety or to the health or safety of others. But we will only disclosure the information to someone who may be able to help prevent the threat.

Business Associates. We may disclose PHI to our business associates who perform functions on our behalf or provide us with services if the PHI is necessary for those functions or services. For example, we may use another company to do our billing, or to provide transcription or consulting services for us. All of our business associates are obligated, under contract with us, to protect the privacy of your PHI.

Organ and Tissue Donation. If you are an organ or tissue donor, we may use or disclose your PHI to organizations that handle organ procurement or transplantation – such as an organ donation bank – as necessary to facilitate organ or tissue donation and transplantation.

Military and Veterans. If you are a member of the armed forces, we may release PHI as required by military command authorities. We also may release PHI to the appropriate foreign military authority if you are a member of a foreign military.

Workers' Compensation. We may use or disclose PHI for workers' compensation or similar programs that provide benefits for work-related injuries or illness.

Public Health Risks. We may disclose PHI for public health activities. This includes disclosures to: (1) a person subject to the jurisdiction of the Food and Drug Administration ("FDA") for purposes related to the quality, safety or effectiveness of an FDA-regulated product or activity; (2) prevent or control disease, injury or disability; (3) report births and deaths; (4) report child abuse or neglect; (5) report reactions to medications or problems with products; (6) notify people of recalls of products they may be using; (7) a person who may have been exposed to a disease or may be at risk for contracting or spreading a disease or condition; and (8) the appropriate government authority if we believe a patient has been the victim of abuse, neglect, or domestic violence and the patient agrees or we are required or authorized by law to make that disclosure.

Health Oversight Activities. We may disclose PHI to a health oversight agency for activities authorized by law. These oversight activities include, for example, audits, investigations, inspections, licensure, and similar activities that are necessary for the government to monitor the health care system, government programs, and compliance with civil rights laws.

Lawsuits and Disputes. If you are involved in a lawsuit or a dispute, we may disclose PHI in response to a court or administrative order. We also may disclose PHI in response to a subpoena, discovery request, or other legal process from someone else involved in the dispute, but only if efforts have been made to tell you about the request or to get an order protecting the information requested. We may also use or disclose your PHI to defend ourselves if you sue us.

Law Enforcement. We may release PHI if asked by a law enforcement official for the following reasons: in response to a court order, subpoena, warrant, summons or similar process; to identify or locate a suspect, fugitive, material witness, or missing person; about the victim of a crime if; about a death we believe may be the result of criminal conduct; about criminal conduct on our premises; and in emergency circumstances to report a crime, the location of the crime or victims, or the identity, description, or location of the person who committed the crime.

National Security. We may release PHI to authorized federal officials for national security activities authorized by law. For example, we may disclose PHI to those officials so they may protect the President.

Coroners, Medical Examiners, and Funeral Directors. We may release PHI to a coroner, medical examiner, or funeral director so that they can carry out their duties.

Inmates. If you are an inmate of a correctional institution or under the custody of a law enforcement official, we may disclose PHI to the correctional institution or law enforcement official if the disclosure is necessary (1) for the institution to provide you with health care; (2) to protect your health and safety or the health and safety of others; or (3) the safety and security of the correctional institution.

Uses and Disclosures That Require Us to Give You an Opportunity to Object and Opt Out

Individuals Involved in Your Care or Payment for Your Care. We may disclose PHI to a person who is involved in your medical care or helps pay for your care, such as a family member or friend, to the extent it is relevant to that person's involvement in your care or payment related to your care. We will provide you with an opportunity to object to and opt out of such a disclosure whenever we practicably can do so.

Disaster Relief. We may disclose your PHI to disaster relief organizations that seek your PHI to coordinate your care, or notify family and friends of your location or condition in a disaster. We will provide you with an opportunity to agree or object to such a disclosure whenever we practicably can do so.

Your Written Authorization is Required for Other Uses and Disclosures

Uses and disclosures for marketing purposes and disclosures that constitute a sale of PHI can only be made with your written authorization. Other uses and disclosures of PHI not covered by this Notice or the laws that apply to us will be made only with your written authorization. If you do give us an authorization, you may revoke it at any time by submitting a written revocation to our Privacy Officer and we will no longer disclose PHI under the authorization. Disclosures that we made in reliance on your authorization before you revoked it will not be affected by the revocation.

Special Protections for HIV, Alcohol and Substance Abuse, Mental Health, and Genetic Information

Special privacy protections apply to HIV-related information, alcohol and substance abuse, mental health, and genetic information. Some parts of this general Notice of Privacy Practices may not apply to these kinds of PHI. Please check with our Privacy Officer for information about the special protections that do apply. For example, if we give you a test to determine if you have been exposed to HIV, we will not disclose the fact that you have taken the test to anyone without your written consent unless otherwise required by law.

Your Rights Regarding Your PHI

You have the following rights, subject to certain limitations, regarding your PHI:

Right to Inspect and Copy. You have the right to inspect and/or receive a copy of PHI that may be used to make decisions about your care or payment for your care. But you do not have a right to inspect or copy psychotherapy notes. We may charge you a fee for the costs of copying, mailing or other supplies associated with your request. We may not charge you a fee if you need the information for a claim for benefits under the Social Security Act or any other state or federal needs-based benefit program. We may deny your request in certain limited circumstances. If we do deny your request, you have the right to have the denial reviewed by a licensed healthcare professional who was not directly involved in the denial of your request, and we will comply with the outcome of the review.

Right to an Electronic Copy of Electronic Medical Records. If your PHI is maintained in one or more designated record sets electronically (for example an electronic medical record or an electronic health record), you have the right to request that an electronic copy of your record be given to you or transmitted to another individual or entity. We may charge you a reasonable, cost-based fee for the labor associated with copying or transmitting the electronic PHI. If you chose to have your PHI transmitted electronically, you will need to provide a written request to this office listing the contact information of the individual or entity who should receive your electronic PHI.

Right to Receive Notice of a Breach. We are required to notify you by first class mail or by e-mail (if you have indicated a preference to receive information by e-mail), of any breach of your Unsecured PHI.

Right to Request Amendments. If you feel that PHI we have is incorrect or incomplete, you may ask us to amend the information. You have the right to request an amendment for as long as the information is kept by or for us. A request for amendment must be made in writing to the Privacy Officer at the address provided at the beginning of this Notice and it must tell us the reason for your request. We may deny your request if it is not in writing or does not include a reason to support the request. In addition, we may deny your request if you ask us to amend information that (1) was not created by us, (2) is not part of the medical information kept by or for us, (3) is not information that you would be permitted to inspect and copy, or (2) is accurate and complete. If we deny your request, you may submit a written statement of disagreement of reasonable length. Your statement of disagreement will be included in your medical record, but we may also include a rebuttal statement.

Right to an Accounting of Disclosures. You have the right to ask for an "accounting of disclosures," which is a list of the disclosures we made of your PHI. We are <u>not</u> required to list certain disclosures, including (1) disclosures made for treatment, payment, and health care operations purposes, (2) disclosures made with your authorization, (3) disclosures made to create a limited data set, and (4) disclosures made directly to you. You must submit your request in writing to our Privacy Officer.

Your request must state a time period which may not be longer than 6 years before your request. Your request should indicate in what form you would like the accounting (for example, on paper or by e-mail). The first accounting of disclosures you request within any 12-month period will be free. For additional requests within the same period, we may charge you for the reasonable costs of providing the accounting. We will tell you what the costs are, and you may choose to withdraw or modify your request before the costs are incurred.

Right to Request Restrictions. You have the right to request a restriction or limitation on the PHI we use or disclose for treatment, payment, or health care operations. You also have the right to request a limit on the PHI we disclose about you to someone who is involved in your care or the payment for your care, like a family member or friend. We are not required to agree to your request. If we agree, we will comply with your request unless we terminate our agreement or the information is needed to provide you with emergency treatment.

Right to Restrict Certain Disclosures to Your Health Plan. You have the right to restrict certain disclosures of PHI to a health plan if the disclosure is for payment or health care operations and pertains to a health care item or service for which you have paid out of pocket in full. We will honor this request unless we are otherwise required by law to disclose this information. This request must be made at the time of service.

Right to Request Confidential Communications. You have the right to request that we communicate with you only in certain ways to preserve your privacy. For example, you may request that we contact you by mail at a special address or call you only at your work number. Your must make any such request in writing and you must specify how or where we are to contact you. We will accommodate all reasonable requests. We will not ask you the reason for your request.

Right to a Paper Copy of This Notice. You have the right to a paper copy of this Notice, even if you have agreed to receive this Notice electronically. You may request a copy of this Notice at any time. You can get a copy of this Notice at our website: http://www.radconlr.com.

How to Exercise Your Rights

To exercise your rights described in this Notice, send your request, in writing, to our Privacy Officer at the address listed at the beginning of this Notice. We may ask you to fill out a form that we will supply. To get a paper copy of this Notice, contact our Privacy Officer by phone or mail.

Changes To This Notice

The effective date of the Notice is stated at the beginning. We reserve the right to change this Notice. We reserve the right to make the changed Notice effective for PHI we already have as well as for any PHI we create or receive in the future. A copy of our current Notice is posted in our office and on our website.

Complaints

If you believe your privacy rights have been violated, you may file a complaint with us or with the Secretary of the Department of Health and Human Services. To file a complaint with us, contact our Privacy Officer at the address listed at the beginning of this Notice. All complaints must be made in writing and should be submitted within 180 days of when you knew or should have known of the suspected violation. There will be no retaliation against you for filing a complaint.

Optional Provisions to be included as applicable:

Foreign Language Version. If you have difficulty reading or understanding English, you may request a copy of this Notice in Spanish.

[Note: Foreign language versions are not required by HIPAA, but federal law requires a provider to make material distributed to the public, such as a Notice of Privacy Practices, available in the languages of persons with limited English proficiency in the provider's service area.]

Medical Residents and Medical Students. Medical residents or medical students may observe or participate in your treatment or use your PHI to assist in their training. You have the right to refuse to be examined, observed, or treated by medical residents or medical students.

Newsletters and Other Communications. We may use your PHI to communicate to you by newsletters, mailings, or other means regarding treatment options, health related information, disease management programs, wellness programs, or other community based initiatives or activities in which our practice is participating.

Effective Date: April 14, 2003
Revised Date: November 2015

Providing the Patient with the Notice of Privacy Practices

Policy:

1. The Company will adhere to its Notice of Privacy Practices (the "Notice"). The Privacy Officer shall be responsible for developing and maintaining the Company's Notice. The Notice currently adopted by the Company is attached as Exhibit A, Receipt of Notice of Privacy Practices.

2. The Privacy Officer will be listed on the Notice and serve as the contact person for individuals who have complaints about how the Company has used or disclosed their protected health information or who have questions about the Company's Notice.

3. A copy of the Notice shall be distributed to each patient at the patient's first visit after HIPAA's compliance date of April 14, 2003. It shall be the responsibility of the front desk personnel to ensure that this is accomplished. Additional copies will be provided individuals, including members of the public, upon request. A copy of the Notice will be prominently displayed in the patient waiting room. The notice will be prominently displayed on the company website.

4. The Notice will be promptly revised whenever there is a material change to the Company's practices described in the Notice.[2] Unless required by law, material revisions will not be implemented prior to the effective date of the revised Notice.[3] Revised Notices will be made available upon request and posted prominently in the patient waiting room.

5. The Company's Notice will be retained for six (6) years from its last effective date. The Company will likewise retain acknowledgements and documentation of good faith efforts to obtain written acknowledgements for a duration of six (6) years.

[2] A covered entity may not apply a revision to information received or maintained prior to the revision unless it has reserved the right to do so in its Notice.

[3] The effective date of the Notice is the date it is printed or otherwise published.

Effective Date: April 14, 2002
Revised Date: November 20, 2015

Procedure for Providing the Patient with the Notice of Privacy Practices

Procedure:

1. During the registration process at the Diagnostic/Ultrasound front desk or the CT front desk the patient will be handed the Notice of Privacy Practices brochure.

2. The patient will be asked to sign the Receipt of Notice of Privacy Practices form stating that they received the brochure.

3. This form will be sent back with the patient's paperwork and scanned with the report in the patient's demographics.

4. This form is to be kept in the patient's demographics for six years and updated as necessary.

Radiology Consultants of Little Rock, P.A.
Acknowledgement of Receipt of Notice of Privacy Practices

I, _____ have received a copy of the Notice of Privacy Practices from Radiology Consultants of Little Rock, P.A. concerning how the use or disclosure of Protected Health Information will be handled by the practice.

_____ _____

Patient Signature Date

Effective Date: April 14, 2002
Revised Date: November 20, 2015

Documentation Patient Received Privacy Notice and Retention of the Notice

Policy:

1. A copy of the Notice shall be distributed to each patient at the patient's first visit after HIPAA's compliance date of April 14, 2003. It shall be the responsibility of the front desk personnel to ensure that this is accomplished. Additional copies will be provided individuals, including members of the public, upon request. A copy of the Notice will be prominently displayed in the patient waiting room. The notice will be prominently displayed on the company website.

.2. The Notice will be promptly revised whenever there is a material change to the Company's practices described in the Notice. Unless required by law, material revisions will not be implemented prior to the effective date of the revised Notice. Revised Notices will be made available upon request and posted prominently in the patient waiting room.

3. The Company's Notice will be retained for six (6) years from its last effective date. The Company will likewise retain acknowledgements and documentation of good faith efforts to obtain written acknowledgements for a duration of six (6) years.

Effective Date: April 14, 2002
Revised Date: November 20, 2015

Procedure for Documentation Patient Received Privacy Notice and Retention of the Notice

Procedure:

1. During the registration process at the Diagnostic/Ultrasound front desk or the CT front desk the patient will be handed the Notice of Privacy Practices brochure.

2. The patient will be asked to sign the Receipt of Notice of Privacy Practices form stating that they received the brochure.

3. This form will be sent back with the patient's paperwork and scanned with the report in the patient's demographics.

4. This form is to be kept in the patient's file for six years and updated as necessary.

Effective Date: April 14, 2003
Revised Date: November 20, 2015

Procedure for Revising/Updating Privacy Notice

Procedure:

1. The Notice of Privacy Practices will be distributed in the following ways:

    - Brochure form given to the patient at the time of service.
    - Posted in the waiting room
    - Posted on our Website at www.radconlr.com

2. As soon as we are informed that there are material changes to the uses or disclosures, the individual's rights, the covered entity's legal duties or other privacy practices stated in the notice, a revised brochure will be printed to be available upon request on or after the effective date of the revision. It may not be given out before the effective date of the change.

3. A revised copy of the Notice will be posted in the waiting room the date the revision is effective.

4. The secretary maintaining the Website will e-mail the revised Notice to VCMM Creative Media to be posted the effective date of the change or shortly after.

Effective Date: April 14, 2003
Revised Date: November 2015

Procedure for Revising the Electronic Notice

Procedure:

1. The Notice of Privacy Practices will be posted on the Website at www.radconlr.com by VCMM Creative Media.

2. When we are informed that there are material changes to the uses or disclosures, the individual's rights, the covered entity's legal duties or other privacy practices stated in the Notice, the secretary maintaining the HIPAA Policy and Procedures will make the necessary changes.

3. The revised Notice will be e-mailed to sharter@vcmm-media.com, with instructions for the Notice to be posted on or shortly after the effective date of the revision. It may not be posted before the revision date.

Effective Date: April 14, 2003

Statement of the Right to Change
Privacy Notice and Policy and Procedures

Policy:

The Notice of Privacy Practices (the, "Notice") has the following paragraph regarding the right to change the Notice and policy and procedures:

CHANGES TO THIS NOTICE

We reserve the right to make changes to this notice at any time. We reserve the right to make the revised notice effective for personal health information we have about you as well as any information we receive in the future. In the event there is a material change to this Notice, the revised Notice will be posted. In addition, you may request a copy of the revised Notice at any time.

Effective Date: April 14, 2003
Revised Date: November 20, 2015

Procedure for Electronic Notices

Procedure:

1. Radiology Consultants will maintain the Notice of Privacy Practices (the, "Notice") on the Website, www.radconlr.com. It will not be our policy to e-mail the Notice.

2. Our Website is maintained by:

   VCMM Creative Media
   14922 Gorgeous View Trail
   Little Rock, AR 72210
   (501) 837-2769

3. We will e-mail the Notice to VCMM Creative Media and they will post it on the Website.

4. Any revisions to the Notice will be made in our office and then e-mailed VCMM Creative Media to be posted on the effective date of the change or shortly after.

Effective Date: April 14, 2003
Revised Date: November 20, 2015

Procedure Explaining to Patient
How to Access Electronic Notice

Procedure:

1. The Notice of Privacy Practices (the, "Notice") will be maintained on our Website at www.radconlr.com by VCMM Creative Media.

2. The Website address is in the Notice brochure given out at the time of service.

3. Anyone may call into the Radiology Consultants office to ask for the Website address in order to access the Notice.

4. It will not be the policy of Radiology Consultants to e-mail the Notice.

Effective Date: April 14, 2003

Electronic Mail Policy

Purpose:

The purpose of this policy is to define appropriate standards for secure and effective use of Radiology Consultants electronic mail system.

Policy:

Electronic mail has become an integrated tool in Radiology Consultants business processes. This policy applies to all usage of Radiology Consultants electronic mail systems where the mail is either originated from or is received into a Radiology Consultants computer or network. It applies to all users including, but not limited to, employees, medical staff, contractors, students, and volunteers.

User Responsibilities:

The user is any person who has been authorized to read, enter, or update information created or transmitted via Radiology Consultants electronic mail system.

Electronic mail is intended to be used as a business tool to facilitate communications and the exchange of information needed to perform an employee's job. Incidental personal use is permissible so long as:

1. It does not consume more than a trivial amount of resources.
2. Does not interfere with worker productivity.
3. Does not preempt any business activity.

Users have an obligation to use e-mail appropriately, effectively, and efficiently.

Users must be aware that electronic communications can, depending on the technology, be forwarded, intercepted, printed and stored by others. Therefore, users must utilize discretion and confidentiality protections equal to or exceeding that which is applied to written documents.

E-mail should not be used for urgent or time-sensitive communications.

Business e-mail accounts and passwords should not be shared or revealed to anyone else besides the authorized user(s).

Prohibited Uses:

Use of electronic mail is to be in compliance with all applicable state and federal statutes and Radiology Consultants policies and procedures. Prohibited usage of Radiology Consultants electronic mail system includes, but is not limited to:

1. Copying or transmission of any document, software or other information protected by copyright and/or patent law, without proper authorization by the copyright or patent owner.
2. Engaging in any communication that is threatening, defamatory, obscene, offensive, or harassing.
3. Use of e-mail system for solicitation of funds, political messages, gambling, commercial or illegal activities.
4. Disclosure of an individual's personal information without appropriate authorization.
5. Transmission of information to individuals inside or outside the company without a legitimate business need for the information.
6. Use of e-mail addresses for marketing purposes without explicit permission from the target recipient.
7. Transmission of highly confidential or sensitive information, e.g., HIV status, mental illness.
8. Forwarding of e-mail from in-house or outside legal counsel, or the contents of that mail, to individuals outside of the company without the express authorization of counsel.
9. Misrepresenting, obscuring, suppressing, or replacing a user's identity on an electronic communication.
10. Obtaining access to the files or communications of others with no substantial company business purpose.
11. Attempting unauthorized access to data or attempting to breach any security measure on any electronic communication system, or attempting to intercept any electronic communication transmissions without proper authorization.

This list is not considered all-inclusive. Further questions regarding appropriate use of electronic mail should be directed to the employee's supervisor or the Security Officer.

Ownership and User Privacy of E-mail:

Use of electronic mail is a part of Radiology Consultants business processes. All messages originated or transported within or received into Radiology Consultants electronic mail system are considered to be the property of Radiology Consultants.

All users of e-mail systems do so within the understanding that they have no expectation of privacy related to that use. Radiology Consultants reserves the right to access the electronic mail system for the purpose of ensuring the protection of legitimate business interests and proper utilization of its property. Such purposes may include, but are not limited to:

1. Locating and retrieving lost messages.
2. Performing duties when an employee is out of the office or otherwise unavailable.
3. Maintaining control of the system by analyzing message patterns and implementing revisions as needed.
4. Collecting or monitoring electronic communications in order to ensure the ongoing availability and reliability of the system.
5. Recovering from systems failures and other unexpected emergencies.
6. Investigating suspected breaches of security or violations of policy with probable cause.
7. Electronic mail information is occasionally visible to staff and contractors engaged in routine testing, maintenance, and problem resolution. Staff and contractors assigned to perform such assignments will not intentionally seek out and read, or disclose to others, the content of e-mail.

Workforce members must advise and receive approval from the Security Officer of their intent to review an employee's messages prior to accessing employee files.

Confidentiality of Electronic Mail:

Users of Radiology Consultants electronic mail system may have the capacity to forward, print and circulate any message transmitted through the system. Therefore:

1. Users should utilize discretion and confidentiality protections equal to or exceeding that which is applied to written documents.
2. When e-mail is used for communication of confidential or sensitive information, specific measures must be taken to safeguard the confidentiality of the information. These safeguards are as follows:
    a. Information considered confidential or sensitive must be protected during transmission of the data utilizing encryption or some other system of access controls that ensure the information is not accessed by anyone other than the intended recipient.
    b. A notation referring to the confidential or sensitive nature of the information should be made in the subject line.
    c. Confidential or sensitive information may be distributed to multiple recipients; however, the use of distribution lists is prohibited.
    d. Confidential or sensitive information is to be distributed only to those with a legitimate need to know.

Retention of Electronic Mail:

Generally, e-mail messages constitute temporary communications, which are non-vital and may be discarded routinely. However, depending on the content of an e-mail message, it may be considered a more formal record and should be retained pursuant to Radiology Consultants record retention schedules.

Provider/Patient Use of E-mail:

Use of provider/patient e-mail can facilitate improved communication between an individual and his or her provider. However, due to the inherent risks involved in e-mail use, the following policy considerations must be clearly addressed prior to using e-mail for provider/patient communications.

Patient informed consent and agreement to guidelines for use of e-mail must be documented. Informed consent should address the following:

1. E-mail communication is a convenience and not appropriate for emergencies or time-sensitive issues.
2. No one can guarantee the security and privacy of e-mail messages. Employees generally have the right to access any e-mail received or sent by a person at work.
3. Highly sensitive or personal information should not be communicated via e-mail.
4. Communication guidelines defined, including:
    a. How often e-mail will be checked.
    b. Instructions for when and how to escalate to phone calls and office visits.
    c. The types of transactions that are appropriate for e-mail.
5. Staff other than the health care provider may read and process the mail.

6. Clinically relevant messages and responses will be documented in the medical record.
7. E-mail message content must include:
    a. The category of the communication in the subject line, i.e., prescription refill, appointment request, etc.
    b. Clear patient identification including patient name, telephone number and patient identification number in the body of the message.
8. Indemnify Radiology Consultants for information loss due to technical failures.

Technical Security Practices:

9. Restriction of access to the professional e-mail account in the same way access to medial records is restricted.
10. Use of password protected programs and screen-savers for all workstations
11. Firewalls
12. Prohibition on use of unsecured wireless e-mail communication when sending patient identifiable information.

Compliance:

Employees and users of Radiology Consultants electronic mail system(s) who are found to be in violation of any part of this policy are subject to disciplinary action up to and including dismissal.

Effective Date: April 14, 2003

Employee E-mail Usage Policy

E-mail is to be used for Radiology Consultants business and should not be overused or misused. Personal e-mail use is allowed before 8:00 a.m. and after 5:00 p.m. E-mail is an efficient way to send urgent messages or those designed to communicate with multiple people simultaneously. Use extreme caution to ensure that the correct e-mail address is used for the intended recipient(s).

Radiology Consultants may access and monitor e-mail at any time for any reason without notice. You should not expect or treat e-mail as confidential or private. E-mail users must provide the network administrator with passwords. Except for authorized Company personnel, no one is permitted to access another person's e-mail without consent.

System users should exercise extreme judgment and common sense when distributing messages. Confidential information should never be disseminated to unauthorized sources. This includes the transmission of documents containing financial information or Social Security numbers. Patient-related messages should be carefully guarded and protected, like any other written materials. You must also abide by copyright laws, ethics rules and other applicable laws.

Sending harassing, abusive, intimidating, discriminatory, or other offensive e-mails is strictly prohibited. The use of the system to solicit for any purpose without the consent of the human resources director is strictly prohibited. If you receive a message containing defamatory, obscene, offensive or harassing information, or that discloses personal information without permission, you must delete it immediately and not forward it. Chain-type messages and executable graphics files should also be deleted and not forwarded because they cause overload on our system. Anyone engaging in the transmission of inappropriate emails, as determined by the Company, will be subject to discipline, up to and including termination.

I have read the Company's e-mail policy and agree to abide by it as consideration for my continued employment. I understand that violation of any of the above policies may result in my termination.

_____ _____

User Signature Date

Section I: Privacy Standards

5. Patient Rights

Effective Date: April 14, 2003

Policy for Individual's Right to Access/Inspect or Obtain a Copy of PHI

Policy:

1. The Company will give individuals access to their protected health information contained in designated record sets. Designated record sets include a patient's medical record, billing record, and any other document or record used to make decisions about the patient. The Privacy Officer or Supervisor shall be responsible for receiving and processing requests for access.

2. Oral request will be accepted for PHI being sent to patient (except Medical Report). Written request will be required for Medical Reports as well as PHI being sent to address other than patient's address.

3. The Company will arrange for review by the patient at a convenient time and location or mail the information to the patient, upon the patient's request, unless an exception that permits the denial of the request is present. The Company shall provide the requested access or send the individual a written notice of denial within thirty (30) days of the request. If the information is not maintained or accessible by the Company on-site, the Company must take action on the request within sixty (60) days. If the Company is unable to take the action required by this paragraph within the applicable timeframe, the Company may exercise a one time thirty (30) day extension, if the Company provides the individual with a written explanation for the delay and the date by which the Company will take final action on the request.

4. The Company will provide the patient with access to the protected health information in the form or format requested by the individual, if it is readily producible in such form or format. If not, the information will be produced in a readable hard copy form.

5. If the Company denies a request for access, and is subject to review, the Company will provide a timely, written denial to the individual. The denial must contain the basis for the denial and a description of how to complain to the Company or the Secretary of Health and Human Services. If access to the information was denied, the denial must also state that the individual has a right to have the Company's decision reviewed by a licensed health care professional designated by the Company who did not participate in the original decision regarding access and explain how to exercise this right. Any such request will be promptly referred to such licensed health care professional. The review determination must be made within a reasonable period of time and the Company shall promptly provide notice of the determination. The Company must follow the determination made by the reviewer.

6. The Company will maintain the designated record sets and the titles of the person(s) in charge of receiving and processing requests for access for six (6) years.

Effective Date: April 14, 2003
Revised Date: November 20, 2015

Procedure for Individual's Right to Access/Inspect or Obtain a Copy of PHI

Procedure for Patient Accounts:

1. Patients may call into our Patient Accounts Department for an inspection or accounting of disclosures of their PHI from any insurance clerk.

2. The clerk will verify that they are speaking with the patient by asking for some type of personal identifiable information such as their name, address, phone number, social security number, or date of birth. After the clerk is satisfied they are speaking to the patient, they may proceed in helping the patient with their request.

3. The clerk may go ahead help the patient by phone if they are requesting information such as:

   - Balance of the account
   - Help filing insurance or obtaining insurance information
   - Asking for a copy of their bill, etc.

4. If the patient is requesting copies of their reports or x-rays to be sent to a physician, the call will be transferred to the front desk. The front desk will document the physician they are checked out to in the film tracking program in the computer and will require these x-rays be returned to us.

5. If the patient is wanting to obtain copies of their PHI where research is required on our part, the following steps will be taken:

   - The request must be made in writing and when received it must be stamped with the date the request was received.
   - The clerk will work with the Privacy Officer or Supervisor and will provide a formal response to the patient, either denial of the request or that the request was accepted, within 30 days--60 days if off site retrieval is required.
   - The patient will be mailed, faxed or emailed the information, or informed when they may pick it up from our office.
   - The clerk will place a comment in the computer on the account and scan the written request and response in the patient's demographics if it is an office patient and scanned into the Correspondence File if it a patient from another place of service.
   - The request and response will be maintained for six years before being destroyed.

Effective Date: April 14, 2003
Revised Date: November 20, 2015

Procedure for Individual's Right to Access/Inspect or Obtain a Copy of PHI

Procedure for the Front Desk Areas:

1. Office patients may call into our CT Front Desk or Diagnostic/Ultrasound Front Desk and ask for an inspection or accounting of disclosures of their PHI.

2. The front desk personnel will verify that they are speaking with the patient by asking for some type of personal identifiable information such as their name, address, phone number, date of birth, or social security number. After they are satisfied they are speaking to the patient, they may proceed in helping the patient with their request.

3. If the patient is requesting billing information regarding their account, they will be transferred to Patient Accounts.

4. If the patient is requesting copies of their reports or x-rays to be sent to a physician, we will make a copy of the report and check the films out to that physician, or let the patient pick it up and take it to that physician. We will document the physician they are checked out to in our film tracking program on the computer and will require these x-rays be returned to us.

5. If the patient is requesting a copy of their x-rays to keep for themselves or information where research is required, the following procedures will be taken:

    - The request must be made in writing and when received it must be stamped with the date the request was received. Oral and written requests will be documented in the computer by the date the request is made.

    - The front desk clerk will work with the Privacy Officer or Supervisor and will provide a formal response to the patient, either denial of the request or that the request was accepted, within 30 days--60 days if off site retrieval is required.

    - The patient will be mailed, faxed or emailed the information, or informed when they may pick it up from our office.

    - The front desk clerk will put a comment in the computer on the account when the request was received, stamp the date on it and scan it in the patient's demographics if it is an office account. Patient Accounts will scan other places of service in the Correspondence File to be maintained for six years.

    - A charge may be made for the copies of the x-rays, but not for the reports the first time. We may charge for copies if the request is made by the patient again.

Effective Date: April 14, 2003

Verifying the Identity of the Person Requesting Information

Policy:

1. HIPAA requires a covered practice to verify the identity and authority of an individual requesting PHI, to the extent these are not known to the practice, and to develop policies and procedures to implement this requirement.

2. Before making any disclosure the Company personnel must verify that the individual's oral agreement was obtained and it must be documented in the computer. The verification process is considered to be met when the healthcare entity exercises "professional judgment" in making a disclosure.

Effective Date: April 14, 2003
Revised Date: November 20, 2015

Procedure for Verifying the Identify of the Person Requesting Information

Procedure:

1. Before making any disclosure the Company personnel must verify that the individual's oral agreement was obtained by asking the patient for the following information:

    - Date of Birth
    - Social Security number – last 4 digits

2. After professional judgment is made and you are satisfied that you are speaking to the patient you may assist the patient with their request.

3. A comment will be documented in the computer on the account of the nature and date of the call.

Effective Date: April 14, 2003

Entity's Right to Deny Access

Policy:

The Company may deny a person access to his or her protected health information for any of the following reasons:

1. The information is not contained within a designated record set;
2. The information qualifies as psychotherapy notes;
3. The records are being compiled in anticipation of litigation;
4. The records are exempt from disclosure under the Clinical Laboratory Improvements Amendments ("CLIA");
5. The information is created or obtained by the Company for clinical research, assuming the patient agreed to such a restriction;
6. The information was obtained from someone other than a health care provider under a promise of confidentiality and access would be reasonably likely to reveal the source of the information;
7. A licensed health care professional has determined that the access requested is reasonably likely to endanger the life or physical safety of the individual or another person;
8. The information references another person and a licensed health professional has determined that the access is reasonably likely to cause harm to such other person; or
9. The request is made by the patient's personal representative and a licensed health professional has determined that the provision of access to the personal representative is reasonably likely to cause substantial harm to the patient or another person.

Effective Date: April 14, 2003
Revised Date: November 20, 2015

Procedure for Entity's Right to Deny Access

Procedure:

If access is denied on a ground permitted by the policy the Privacy Officer or Supervisor will use the following procedure:

1. Provide access to other information after excluding PHI to which the individual has been denied access.

2. Written notice will be provided within 30 days including the basis for the denial, a statement of the individual's review rights, if applicable, and a description of how the individual may complain to the organization or to the Secretary. The description will include the name, title and telephone number of the contact person.

3. If we do not maintain the PHI requested and know where the information is maintained, we will inform the individual of were to direct the request.

4. If the individual has requested a review of the denial and the denial is subject to review, we will designate another healthcare professional not involved with the original decision to conduct a review and follow that person's decision.

5. We will document this process in the computer on the account and scan it in the patient's demographics if it is an office account it will be scanned into the Correspondence File if it is a patient from another place of service. The information will be maintained for six years.

Effective Date: April 14, 2003
Revised Date: Novemer 20, 2015

Timely Action to Respond to Request for PHI

Policy:

1. Radiology Consultants will provide a formal response to the patient within 30 days after written receipt of the request for PHI.

2. If the requested information is stored in an archived file, we will have 60 days to take action after receiving the request.

3. If we are unable to deny or provide access within the allowable time frames, we will be allowed a one-time 30 day extension. We will provide the patient with a written statement explaining the reasons for the delay and the date by which action on the request will be completed.

4. Any request for information that is readily available may be handled at that time after verification that we are speaking to the patient.

Effective Date: April 14, 2003
Revised Date: November 20, 2015

Procedure for Timely Action to Respond to Request for PHI

Procedure:

1 Any patient calling into the office wishing to discuss their account, asking for or providing insurance information, etc. will be helped immediately after the clerk has verified they are speaking with the patient.

2 If the patient is requesting information that requires research, we will ask for the request in writing and it will go to the Supervisor or Privacy Officer.

3 The response time by the Privacy Officer will be made in writing within 30 days after receipt of the request for PHI. The response will:

- Provide a written denial of the request,
- Inform the individual the request was accepted and explain how and where the information can be accessed, or
- Will provide the information.

4 If the requested information is stored in an off-site location, we will have 60 days to take action after receiving the request.

5 If we are unable to deny or provide access within the allowable time frames, we will be allowed a one-time 30 day extension. We will provide the patient with a written statement explaining the reasons for the delay and the date by which action on the request will be completed.

6 The request will be stamped with the date received, a comment placed in the computer on the account, and the request and response scanned in the patient's demographics if it is an office patient will be scanned into the Correspondence File in Patient Accounts of it is a patient from another place of service and maintained for six years.

Effective Date: April 14, 2003
Revised Date: November 20, 2015

Procedure for Timely Action to Respond to Request for PHI -- Providing Access

Procedure:

1. Any patient calling into the office to discuss their account, asking for or providing insurance information, etc. will be helped immediately by phone after the clerk has verified they are speaking with the patient or appropriate representative.

2. If the patient's request has to be researched or approved, we will ask for the request in writing. When received, the request will go to Supervisor or Privacy Officer. Access must be provided within 30 days. Access may be obtained in the following manner:

- The patient will be provided written response with a date and time to pickup the information or view the information in our office.

- We will mail, fax or email the PHI requested in order to facilitate providing the information in a timely manner.

- We may provide a summary of PHI or an explanation of the PHI as long as the individual agrees in advance to the summary report or explanation, along with payment of any fees imposed for creating the summary.

3. The request and response will be documented in the computer on the account and scanned in the patient's demographics if this is an office patient will be scanned into the Correspondence File it the patient is from another place of service. The information will be maintained for six years.

Effective Date: April 14, 2003
Revised Date: November 20, 2015

Procedure for Timely Action to Respond to Request for PHI Amendments

Procedure:

1. The individual has the right to request that we amend PHI or a record about the individual in a designated record set for as long as the information remains in that record set.

2. The Administrator or Privacy Officer must respond to the request making the amendment or at a minimum, identifying the record set within 60 days.

3. If we are unable to act on the amendment within the required 60 days, we may extend the response time by no more than 30 days. This 30 day extension is allowed on a one-time basis and the individual will be informed in writing of:

    a. The reason for the delay.
    b. The date by which the amendment will be completed.

4. If the request for amended PHI is denied, the denial will be made in writing from the Privacy Officer with the required 60 day time frame.

5. The request and response will be documented in the computer on the account and scanned in the patient's demogrpahics if this is an office patient will be scanned into the Correspondence File it the patient is from another place of service. The information will be maintained for six years.

Effective Date: April 14, 2003
Revised Date: November 20, 2015

Procedure for Timely Action to Respond to Request for PHI Denials

Procedure:

1. After the written request for PHI is received and researched, the Administrator or Privacy Officer will provide a written denial of the request in 30 days. If the information requested is stored in an off-site location, the practice has 60 days to take action after receiving the request.

2. If we are unable to deny or provide access to the information, we will be allowed a one-time 30 day extension. The patient will be provided with a written statement explaining the reasons for the delay and the date by which action on the request will be completed.

3. The request and response will be documented in the computer on the account and scanned in the patient's demographics if this is an office patient will be scanned into the Correspondence File it the patient is from another place of service. The information will be maintained for six years.

Effective Date: April 14, 2003
Revised Date; November 20, 2015

Handling Requests for Access, Amendments, Restrictions and Terminating Restrictions to PHI

Policy:

1. Radiology Consultants will give the patient the right to access, amend, restrict and terminate restrictions to PHI to include medical record, billing record, films and medical reports or records used to make decisions about the patient.

2. Oral requests will be accepted when the patient is calling for access to current billing information or help filing insurance, etc., from Patient Accounts.

3. If the patient is in need of films and reports, the request will be handled by the front desk.

4. If the request is in need of research, we will ask the patient to send a written request for the PHI access, amendment, or restriction.

5. The Supervisor or Privacy Officer will provide the requested access or send the individual a written notice of denial within 30 days of the request. If the information is not accessible on site, we will respond within 60 days of the request.

Effective Date: April 14, 2003

Procedure for Handling Requests for PHI

Procedure:

1. Oral requests will be accepted when the patient is calling for current billing information or help filing insurance, etc., from Patient Accounts. Patient Accounts will also handle requests from other places of service. If the patient is in need of films and reports, the request will be handled by the front desk.

2. If the request is in need of research, we will ask the patient to send a written request for the PHI and the Supervisor or Privacy Officer will provide the requested access or send the individual a written notice of denial within 30 days of the request. If the information is not accessible on site, we will respond within 60 days of the request.

3. The response may:

   - Provide a written denial of the request,
   - Inform the individual the request was accepted and explain how and where the information can be accessed, or
   - Provide the requested information.

4. The request will be stamped with the date received. A comment will be placed on the account and the request and response scanned in the patient's demographics if it is a Radiology Consultants' patient will be scanned into the Correspondence File in Patient Accounts if it is from another place of service.

Effective Date: April 14, 2003
Revised Date: November 20, 2015

Procedure for Handling Requests for Access to PHI

Procedure:

1. Oral requests will be accepted when the patient is calling for current billing information or help filing insurance, etc., from Patient Accounts. Documentation of the call will be placed in the computer on the account. If the patient is in need of films and reports, the request will be handled by the front desk. Any films checked out will be documented in the film tracking program on the computer.

2. If the request is in need of research, we will ask the patient to send a written request for the PHI, however, oral requests may also be accepted.

3. The Supervisor or Privacy Officer will provide the requested access within 30 days of the request. If the information is not accessible on site, we will respond within 60 days of the request.

4. The PHI may be accessed in the following ways:

    - The requested information will be mailed, faxed or emailed to the individual or it may be picked up by the patient.

    - A summary or explanation as long as the individual requesting the information agrees in advance to the summary report or explanation may be provided.

    - The individual will be informed that the request was accepted and explain how and where the information can be accessed, including on site inspection and/or allowing the patient to obtain a copy of the records.

5. The request will be stamped with the date received. A comment will be placed in the computer on the account and the request and response scanned in the patient's demographics if it is an office patient and scanned into the Correspondence File in Patient Accounts if the patient is from another place of service.

Effective Date: April 14, 2003

Procedure for Handling Request for Amendments to PHI

Procedure:

1. The individual has the right to request that we amend PHI or a record about the individual in a designated record set for as long as the information remains in that record set. Our requirements for PHI other than medical reports are:

- The request may be made in writing from the patient.
- A reason to support the amendment must be given.

2. When a request to amend medical reports (PHI) is received, we will have the physician on the floor and/or the reading physician if it is regarding a report, aware of the situation and solution for the amendment. **(We would not need their agreement to notify a referring physician of a change in a report, we would automatically send an amended report.)** All requests to change medical reports will be:

- Required to make the request in writing.
- The physician on the floor or the reading physician will make the decision to accept the amendment or not.
- If accepted, the physician will make the amendment and send a copy to the referring physician, patient and/or collection agency.

4. We must act on the request within 60 days. If we are unable to act within the 60 day time frame, we may extend the response time by no more than 30 additional days and the patient must be informed in writing.

5. Once a request to amend PHI has been accepted:

- A letter will be sent by the Supervisor or Privacy Officer to the individual that the amendment has been accepted.
- We will make the amendment to the PHI.
- We obtain the individual's identification and agreement to have the practice notify relevant persons such as business associates identified by the individual as having received the affected PHI who might have relied on or might foreseeably rely on such information to the detriment of the individual.

6. If the request for amended PHI is denied, the denial will be made in writing from the Supervisor or Privacy Officer with the required 60 day time frame.

7. We will place a comment in the computer on the account of the request for change of PHI, and the request and our response will be filed it the patient's x-ray jacket if it is an office patient or the Correspondence File in Patient Accounts if the patient is from another place of service and maintained for six years.

8. Future disclosures of medical reports (PHI) to which an individual has requested amendment are affected in the following way::

    - If a statement of disagreement has been submitted, the covered practice must include the appended materials or an accurate summary of the appended information in any future disclosures of the PHI.

9. If we receive notice of amendment to PHI from other entities, we are required to make those amendments in the appropriate record sets.

Effective Date: April 14, 2003
Revised Date: November 20, 2015

Procedure for Handling Requests for Restrictions to PHI and Terminating Restrictions

Procedure for Handling Requests for Restrictions to PHI:

Patients have the right to restrict uses and disclosures of his/her PHI to carry out treatment, payment, or healthcare operations, along with any uses and disclosures for involvement in the individual's care and notification purposes. While the patient has the right to request that information be restricted, the healthcare entity does not have to comply with that request. The procedures for denial should be followed in order to deny the request.

1. The individual should request restriction of PHI in writing to the Privacy Officer.

2. The Privacy Officer or Supervisor will research the request to restrict the information and respond as quickly as possible with denial or acceptance.

3. If we accept the request to restrict information, we must comply with that restriction unless needed to provide emergency treatment. In case of an emergency which requires disclosure to another healthcare provider, the covered practice must ask the healthcare provider to not further disclose the PHI. The restriction, even if agreed upon by the healthcare entity, is not effective if it prevents uses and disclosures to permitted or required PHI by other provisions in the HIPAA privacy standards.

4. We will document in the computer on the account the restriction and scan the request, the response and any rebuttal in the patient's demographics if it is an office patient or in the Correspondence File in Patient Accounts if the patient is from another place of service on the date of the comment on the account.

5. We will have the front desk put a colored tab on the folder to help identify the restriction or any further restriction of PHI necessary.

Procedure for Handling Requests for Terminating Restrictions:

We are allowed to terminate an agreement to a restriction as long as the following occur:

1. The patient agrees to or requests the termination in writing.

2. We will place a comment in the computer on the account of the termination of restriction and scan this written notice and any response in the patient's demographics if it is an office patient or in the Correspondence File in the Patient Accounts if the patient is from another place of service.

Request to Restrict Disclosures of Protected Health Information to a Health Plan

Patient's Name: _____ Date of Birth: _____

Current Health Plan: _____

I request that Radiology Consultants of Little Rock, PA restrict disclosures of my protected health information (PHI), outlined below, to my current health plan, for purposes of carrying out payment or for healthcare operations, if the following criteria have been met:

- Healthcare item or service must be paid for, out of pocket, in full, at the time of service
- Disclosure regarding this healthcare item or service is not otherwise required by law
- Request must be made prior to care being initiated

Description of PHI to be restricted:

☐ Healthcare information relating to the following treatment, condition, or date of service:
_____
☐ Lab test(s): (Please specify) _____
☐ Other: _____

By signing this form, I understand the following:

- I am responsible for payment, out of pocket, in full, at the time of service for the healthcare items or services listed above.
- If I wish to restrict PHI for a follow-up visit related to a previously restricted healthcare item or service, I must pay for the follow-up visit, out of pocket, in full, at the time of service, as well.
    - If I do not restrict disclosure to my health plan for a follow-up visit pertaining to a previously restricted healthcare item or service, Radiology Consultants of Little Rock, PA is permitted to disclose minimum necessary information pertaining to the previously restricted visit in order to receive payment for my follow-up care from my health plan.
- It is my responsibility to request restrictions from other healthcare providers, such as my pharmacy, other physicians or a hospital/outpatient surgery center.
- This restriction only applies to disclosures to my current health plan for payment or healthcare operation purposes. The PHI listed above may still be used or disclosed for treatment purposes or as otherwise required by law.
- I may terminate this restriction at any time, by notifying, Radiology Consultants of Little Rock, PA in writing.

Signature of Patient: _____ Date: _____

Name of Personal Representative (if applicable): _____

Signature of Personal Representative: _____ Date: _____

Relationship to Patient: _____

For Office Use Only

☐ Approved
- ☐ Payment received
- ☐ Placed restriction in patient record
- ☐ Notified appropriate personnel

☐ Denied
- ☐ Non-payment or dishonored payment
- ☐ Disclosure of PHI to health plan is required by law
- ☐ Patient made the request after care had been initiated

Additional Notes: _____

_____ _____
Privacy Officer Signature Date

Effective Date: April 14, 2003
Revised Date: November 20, 2015

Procedure for Denial of Amendment of PHI

Procedure:

1. The individual has the right to have a covered practice amend PHI about the individual in a designated record set for as long as the information remains in that record set.

2. However, we have the right to deny request for amendment in any of the following instances:

   - The information was not created by our practice (unless the individual can reasonably provide a basis to believe that the healthcare entity that originally created the information no longer exists or cannot act on this request).
   - The information is not part of a designated record set.
   - The individual would not have the right to access the information.
   - We determine the record to be accurate and complete.

3. The Privacy Officer will send a written denial with the following information:

   a. The reason for the denial.
   b. The individual's right to submit a written statement disagreeing with the denial, including how the individual may file that statement
   c. A statement that if the individual does not disagree with the denial in writing, he/she can ask that the request for amendment and denial be included with future disclosures of the PHI subject to the amendment.
   d. A description of how the individual can file a complaint with the organization or the Secretary, including the name or title and telephone number of the contact person.

4. The individual will be allowed to submit a written statement disagreeing with the denial stating the basis of the disagreement

5. We will be allowed to prepare a written rebuttal to the individual's statement of disagreement, but we will have to provide a copy of the rebuttal to the individual.

6. A comment will be placed in the computer on the account regarding the request and the response for the denial.

7. The request and response for denial will be scanned in the patient's demographics if it is an office patient and the Correspondence file in Patient Accounts if the patient is from another place of service.

8. The information will be maintained for six years.

Effective Date: April 14, 2003
Revised Date: November 20, 2015

Procedure for Denial Process for Access to PHI

Procedure:

1. Not only does the individual have the right to request copies of PHI contained in a designated record set, but a covered practice is required to provide formal response to the patient within 30 days after receipt of the request or 60 days if the information is stored off site. The response can inform the individual the request was accepted or provide a written denial of the request.

2. If the request for access to PHI is denied, the Privacy Officer or Supervisor will send a letter including under the following circumstances:

    - We determine, using professional judgment, that releasing the information is reasonably likely to endanger the life or physical safety of the individual or another person.
    - The PHI references another person and the licensed healthcare professional using professional judgment determines that access to the information is reasonably likely to cause substantial harm to the other person.
    - The request for access is made by an individual's personal representative and using professional judgment we determine that access given to the personal representative is reasonably likely to cause substantial harm to the individual or another person.

3. If access is denied on any of the above grounds, the individual requesting access has the right to have another licensed healthcare professional who did not participate in the original decision to deny, review the request and determine whether it is appropriate to grant or deny access. We have the right to designate the reviewing official, but must follow that person's decision.

4. We may deny access to healthcare information and the individual does <u>not</u> have the right to request a review of this action in the following circumstances:

    - Request for psychotherapy notes.
    - A request from a correctional facility inmate if obtaining such copy would jeopardize the health, safety, security, custody, or rehabilitation of the individual or other inmates, or the safety of any officer, employee or other person at the correctional institution or responsible for the transporting of the inmate.
    - The request applies to PHI created or obtained as a part of a research project involving treatment if that access during the project has been temporarily suspended, providing the patient agreed to denial of access, and the provider informed the patients that access would again be granted when the research project was completed.
    - The individual's access to PHI is contained in records subject to the Privacy Act.

- The PHI was obtained from someone other than a healthcare provider under a promise of confidentiality where the requested access would be likely to reveal the source.

5. If we deny access to PHI we must do the following:

   - Alternative Access. Provide access to other information, to the extent possible, after excluding the PHI to which the individual has been denied.
   - Form of Denial. Provide a timely written denial in plain language containing the following elements:
     - The basis for the denial
     - A statement of the individual's review rights including how to exercise the review rights (if applicable); and
     - A description of how the individual may complain to the organization or to the Secretary. The description must include the name, title and telephone number of the contact person.
   - Other Responsibility. If we do not maintained the PHI requested and know where the information is maintained, we must inform the individual of where to appropriately direct the request.
   - Review of Denial. If the individual has requested a review of the denial and the denial is subject to review, the practice must designate a licensed healthcare professional (not involved in the original decision) to conduct a review. We must then promptly refer a request for the review to that reviewing official.
   - Documentation. We are required to document the types of record sets that are subject to access by individuals, along with the titles of the person responsible for receiving and processing these requests.

6. A comment will be placed in the computer on the patient's account.

7. The request and response will be scanned in the patient's demogrpahics if it is an office patient and in Correspondence File in Patient Accounts if it is a patient from another place of service.

8. The date of the request stamped on it and it will be maintained for six years.

Effective Date: April 14, 2003
Revised Date: November 20, 2015

Procedure for Denial Process for Restrictions to PHI and Terminating Restrictions

Procedure for Denial Process for Restrictions to PHI:

The individual has the right to restrict uses and disclosures of his/her PHI to carry out treatment, payment, or healthcare operations, along with any uses and disclosures for involvement in the individual's care and notification purposes. However, we do not have to comply with the request.

1. The individual should make the request for restriction to PHI in writing to the Privacy Officer. The Privacy Officer or Supervisor will research the request to restrict as soon as possible.

2. Denial will be made in writing to the individual with the reason for the denial and a description of how they may complain to the organization or to the Secretary to include name, title, and telephone number of the contact person.

3. We will place a comment regarding the request and response in computer on the patient's account.

4. The written request and the response will be stamped with the date of the request and filed in the patient's demographics if it is an office account or in the Correspondence File in Patient Accounts by the date of the comment if the patient is from another place of service.

Procedure for Denial Process for Terminating Restrictions:

1. The individual should make the request for termination of restrictions in writing to the Privacy Officer. The Privacy Officer or Supervisor will research the request to terminate restriction as soon as possible.

2. The Privacy Officer will respond with the denial to terminate restriction with a reason why the denial is being made and how the individual may complain to the organization or to the Sectary to include name, title, and telephone number of the contact person.

3. We will place a comment in the computer on the account of the written request for termination of restriction and the response and file it in the patient's demographics if it is an office patient or in the Correspondence File in Patient Accounts by the date of the comment if the patient is from another place of service.

Effective Date: April 14, 2003
Revised Date: November 20, 2015

Procedure for Documentation of Requests, Denials and Other Actions

Procedure:

A covered practice is required to document the following:

1. Records or PHI within the record set that is the subject of a disputed amendment.

2. Append or otherwise link

    a. The individual's request for amendment
    b. The covered entity's denial of the request
    c. The individual's statement of disagreement, if any
    d. The covered entity's rebuttal, if any

3. The request for PHI access, amendment, restriction, or termination of restriction will be handled in the following manner:

    a. The request will be stamped with the date received.
    b. A comment will be placed in the computer on the patient's account.
    c. The request and response will be filled in the patient's demographics if it is an office patient and in the Correspondence File in Patient Accounts if the patient is from another place of service.

Effective Date: April 14, 2003
Revised Date: November 20, 2015

Individual's Rights to Request Restriction and Entity's Right to Deny

Policy:

1. The Company will permit patients to make requests to restrict the Company's use and disclosure of protected health information for treatment, payment, health care operations, or to persons assisting in a patient's care.

2. If the Company wishes to agree to requests for additional protections, then:

    - The Company will permit patients to make requests to restrict the Company's use and disclosure of protected health information for treatment, payment, health care operations or to persons assisting in a patient's care. Any such request will be directed to the Privacy Officer. The Privacy Officer may agree to the restriction, with the approval, or subject to the instructions of the Company's management.
    - A restriction may not be imposed to prevent the use or disclosure of protected health information for the public policy-related uses and disclosures.
    - Information subject to the restriction will be marked, stamped or maintained in a separate file to notify Company personnel of the agreed upon restriction.
    - If the Company agrees to a restriction, it will not use or disclose protected health information in violation of that restriction. However, it is permissible for the Company to use or disclose the information where the information is needed for emergency treatment of the individual. If a disclosure is made to another provider in the event of an emergency, the Company must request that the provider not further use or disclose the information.
    - The Company may terminate an agreement to a restriction if the individual agrees to or requests the termination in writing, the individual orally agrees to the termination and the oral agreement is documented, or the Company informs the individual that it is terminating its agreement to a restriction, except that such termination is only effective with respect to protected health information created or received after it has so informed the individual.
    - Restrictions agreed to by the Company will be documented in written form and maintained for six (6) years from its last effective date.

Effective Date: April 14, 2003

Confidential Communications, Including Alternative Means or Locations

Policy:

1. The Company will permit individuals to request that it provide confidential communications involving protected health information to the individual.

2. The Company will accommodate reasonable requests by individuals to receive communications of protected health information from the Company by alternative means or at alternative locations. For example, if a patient would like to receive communications from the Company at her place of employment instead of her home, the Company will accommodate this request.

3. The Company may require the individual to make a request for a confidential communication in writing.

4. Requiring an explanation from the individual as to the basis for the request for confidential communications is prohibited.

Effective Date: April 14, 2003
Revised Date: November 20, 2015

Procedure for Confidential Communications, Including Alternative Means or Locations

Procedure:

Any individual requesting confidential communications of PHI by alternative means or at alternative locations will be requested to:

1. Make the request in writing. The individuals do not have to explain their reasons for requesting delivery of the information at an alternative address.

2. We may condition the provision of an accommodation as to how payment, if any, will be handled and specification of an alternative address or other method of contact.

3. We will change the address on the statement to the alternative address.

4. A comment will be placed in the computer on the account as to the request for change and the request will be stamped with the date of receipt of the request.

5. The request will be filed in the patient's demographics if it is an office patient and in the Correspondence File if the patient is from another place of service and maintained for a period or six years.

Effective Date: April 14, 2003

Individual's right to Request Amendment to PHI; Entity's Right to Deny

Policy:

1. Patients have a right to request an amendment to their protected health information that is contained in designated record sets. The Privacy Officer will receive and process these requests.

2. The Company may deny a patient's request if the information:

    - is accurate and complete;
    - is not contained in a designated record set;
    - would not be subject to the right of access; or
    - was not created by the Company, unless the patient provides a reasonable basis to believe the entity which created the information is no longer available to act on the request.

3. The Company may require the patient to put the request for amendment in writing and to give a reason for the request (e.g., the patient feels the information is incorrect) provided that the Company informs a patient of these requirements in advance. All requests will be stamped with the date it was received.

4. All requests for amendment will be subject to approval by the Privacy Officer who shall consult with the Company's Medical Director. The Privacy Officer will maintain this documentation, along with requests for amendment, statements of denial, statements of disagreement, and rebuttals for a period of six (6) years.

5. The Company must act on a request for an amendment no later than sixty (60) days from receipt of the request. All written requests will be stamped with the date it was received. If the Company accepts the request, it must make the amendment and notify the patient that the amendment was accepted within sixty (60) days. Amendment may be made by identifying the records in the designated record set that are affected and appending or otherwise providing a link to the location of the amendment. The Company must make reasonable efforts to provide the amendment within a reasonable amount of time to persons identified by the patient as having received protected health information needing the amendment. It must also notify persons, including business associates, that the covered entity knows to have the information and that may have relied on the information to the detriment of the patient.

6. If the Company denies the requested amendment, in whole or part, it must provide the patient with a written denial within sixty (60) days of the request. The written denial must contain the following: (1) the basis for the denial; (2) a statement that the patient has a right to submit a statement of disagreement and describe how the patient may file such a statement; and (3) an explanation that the patient may request that the Company provide the patient's request for amendment and its denial with any further disclosures of the patient's protected

7. health information in lieu of a statement of disagreement. Finally, the denial must describe how the patient may complain to the Company or the Secretary of Health and Human Services about the denial. The description must include the name or title, and telephone number of the contact person or office within the Company who will receive complaints.

8. The Company may prepare a written rebuttal to a patient's statement of disagreement, a copy of which must be provided to the patient.

9. When informed by another covered entity of amendment to protected health information in its possession, the Company will make the amendment in the manner described in this section

Effective Date: April 14, 2003

Individual's right to Disagree With Denial for Amendment

Policy:

1. If the Company denies a patient's request for amendment, in whole or part, it must provide the patient with a written denial within sixty (60) days of the request.
2. The individual must be allowed to submit a written statement disagreeing with the denial stating the basis of the disagreement.
3. The covered practice is allowed to prepare a written rebuttal to the individual's statement of disagreement, but must provide a copy of the rebuttal to the individual.

Effective Date: April 14, 2003
Revised Date: November 20, 2015

Procedure for Individual's right to Disagree With Denial for Amendment

Procedure:

1. Any individual submitting a written statement disagreeing with a denial of amendment will be forwarded to the Supervisor or Privacy Officer.
2. The Privacy Officer will decide if a rebuttal statement to the individual is required.
3. We will put a comment in the computer on the patient's account of the PHI that is the subject of a disputed amendment.
4. We will file the request for amendment, the denial, the statement of disagreement and rebuttal, if any, in the patient's demographics if it is an office account and in the Correspondence File in Patient Accounts if the patient is from another place of service.
5. We must include the appended materials listed above or an accurate summary of the appended information in any further disclosures of the PHI.
6. If the individual has not submitted a statement of disagreement, we must include the individual's request for amendment and its denial or a summary of this information with future disclosures of PHI.

Effective Date: April 14, 2003

Entity's Right to Rebuttal

Policy:

If the Company denies a patient's request for amendment and the individual submits a written statement disagreeing with that denial, the covered practice is allowed to:

- Prepare a written rebuttal to the individual's statement of disagreement
- Must provide a copy of the rebuttal to the individual.

Effective Date: April 14, 2003
Revised Date: November 20, 2015

Procedure for Entity's Right to Rebuttal

Procedure:

1. Any individual submitting a written statement disagreeing with a denial of amendment will be forwarded to the Supervisor or Privacy Officer.

2. The Privacy Officer will decide if a rebuttal statement to the individual is required. If so, he will render a written statement to the individual.

3. We will put a comment in the computer on the patient's account of the PHI that is the subject of a disputed amendment.
4. We will file the request for amendment, the denial, the statement of disagreement and rebuttal, if any, in the patient's demographics if it is an office account and in the Correspondence File in Patient Accounts if the patient is from another place of service. This will be maintained for a period of six years.
5. We must include the appended materials listed above or an accurate summary of the appended information in any further disclosures of the PHI.
6. If the individual has not submitted a statement of disagreement, we must include the individual's request for amendment and its denial or a summary of this information with future disclosures of PHI.

Effective Date: April 14, 2003

Individual's Right to Have Review of Denial

Policy:

If the request for access to PHI is denied, the individual must be allowed to submit a written statement disagreeing with the denial stating the basis of the disagreement. The Company is allowed to prepare a written rebuttal to the individual's statement of disagreement provided a copy is sent to the individual.

The individual is allowed to request a review of the denial if the denial is subject to review, the practice must designate a licensed healthcare professional not involved in the original decision to conduct a review. The organization must promptly refer a request for review to that reviewing official.

The organization is required to document the types of record sets that are subject to access by individuals, along with the titles of the person responsible for receiving and processing these requests.

Effective Date: April 14, 2003
Revised Date: November 20, 2015

Procedure for Individual's Right to Have Review of Denial

Procedure:

The individual is allowed to request a review of the denial of access if the denial is subject to review.

1. We will ask that the request for review of denial be submitted in writing to our Privacy Officer.
2. The Privacy Officer will promptly designate a licensed healthcare professional not involved in the original decision to conduct a review.
3. The organization is required to document the types of record sets that are subject to access by individuals, along with the titles of the person responsible for receiving and processing these requests.
4. A comment will be placed in the computer on the patient's account.
5. Documentation of the procedure will be scanned in the patient's demographics if it is an office patient and in the Correspondence File in Patient Accounts if the patient is from another place of service.
6. This information will be maintained for six years.

Effective Date: April 14, 2003

Designation of Outside Resource

Policy:

1. The individual is allowed to request a review of the denial if the denial is subject to review.
2. The practice must promptly designate a licensed healthcare professional not involved in the original decision to conduct a review.
3. The organization is required to document the types of record sets that are subject to access by individuals, along with the titles of the person responsible for receiving and processing these requests.

Effective Date: April 14, 2003
Revised Date: November 20, 2015

Procedure for Designation of Outside Resource

Procedure:

1. The request for a review of the denial will be forwarded to the Privacy Officer.
2. The Privacy Officer will designate a licensed healthcare professional not involved in the original decision to conduct a review as soon as possible.
3. We will abide by the decision of that healthcare professional.
4. We will document the types of record sets that are subject to access by individuals, along with the titles of the person responsible for receiving and processing these requests in the computer system on the patient's account.
5. The patient's request and response will be scanned in the patient's demographics if it is an office account and in the Correspondence File if the patient is from another place of service and maintained for six years.

Effective Date: April 14, 2003

De-Identification of PHI

Policy:

1. The Privacy Standards apply to health information that identifies or could reasonably be expected to identify an individual. They do not restrict the use or disclosure of information that has been de-identified.

2. To create de-identified information, the Company may use one of three methods. First, it may remove all of the following are identifiers:
    - Names
    - All geographic subdivisions smaller than a state, including street address and zip codes (except for the initial three digits of a zip code if, according to current data available from the Bureau of the Census, the geographic unit formed by combining all zip codes with the same initial three digits contains more than 20,000 people, and the initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000)
    - All elements of dates (except year), for dates directly related to an individual, including birth date; and all ages over 89 and all elements of dates (including year), (except that ages may be aggregated into a category of age 90 or older)
    - Telephone numbers, fax numbers, e-mail addresses
    - Social security numbers, medical record numbers, health plan beneficiary numbers, account numbers, certificate /license numbers
    - Vehicle identification and serial numbers, including license plate numbers, device identifiers and serial numbers
    - Web Universal Resource Identifiers, Internet Protocol address numbers, biometric identifiers,
    - Full face photographic images and comparable images, and
    - Any other identifier from the record which could be used to identify an individual.

    Second, the Company may remove fewer identifiers, if a person with appropriate statistical and scientific knowledge determines that the risk of identification is very small.

    Third, if the information is to be used for research or public health purposes, the Company may create a more limited data set, that does not include directly identifiable information but in which certain identifiers, such as admission, discharge and service dates, date of death, age and five-digit zip code remain. The Company must condition disclosure of the limited data set upon the recipient signing a data use or similar agreement, in which the recipient agrees to limit its use of the data to the original reasons for the disclosure and to refrain from attempting to re-identify the information or use it to contact the subjects of the information.

Effective Date: April 14, 2003

Procedure for De-Identification of PHI

Procedure:

1. This company will not intentionally give out information that would identify anyone with their PHI outside of treatment, payment, or health care operation or as required by law.

2. We will remove all of the identifiers in order to protect PHI.

3. We do not use our patient information for research purposes.

Effective Date: April 14, 2003
Revised Date: November 20, 2015

Use of PHI for Marketing Purposes

Policy:

1. Marketing is making a communication about a product or service for the purpose of encouraging someone to buy or use that product or service.

2. Disclosure of PHI for marketing purposes is limited to disclosure to business associates that undertake marketing activities on behalf of the covered entity. No other disclosure for marketing is permitted. Covered entities may not give away or sell lists of patients or enrollees without obtaining authorization from each person on the list. As with any disclosure to a business associate, the covered entity must obtain the business associate's agreement to use the PHI only for the covered entity's marketing activities. A covered entity may not give PHI to a business associate for the business associate's own purposes.

3. If the Company engages in marketing and it does not fit one of the three exceptions listed below, the Company will need to get authorization from a patent before using or disclosing the patient's PHI.

    - Face to Face encounters such as during an office visit. This exception allows a health care provider to give patients samples of goods and products.

    - Products and services of nominal value. PHI may be used or disclosed without authorization when they involve products and service of only nominal value. This exception allows the provider to send his patients pens, refrigerator magnets, toothbrushes, calendars, or similar items with the provider's or health care organization's name on them.

    - Certain health-related products and services. PHI may be used or disclosed without authorization for marketing communications when they involve health-related products or services by the health care organization or by a third party. This could cover a broad range of communications, but for the exception to apply, a marketing communication must meet several additional requirements. It must:

        - Identity the health care organization making the communication so that patient's know the source of the marketing communication.
        - Clearly state that the health care organization is being compensated for making the communication, if that's the case.
        - Tell patients how to opt out of further marketing communications (with some exceptions, such as a general health care newsletter). Make reasonable efforts to ensure that individuals who opt out of receiving communications are not sent such communications.
        - If the marketing communication targets patients with a specific health status or condition (such as diabetics and smokers), the health care organization must have made a determination before using the PHI, that the product or service may be of benefit to individuals with that health status or condition. The marketing communication must tell patient's why they've been targeted and how the product or service relates to their health.

Effective Date: April 14, 2003
Revised Date: November 20, 2015

Procedure for Use of PHI for Marketing Purposes

Procedure:

1. Radiology Consultants has a marketing consultant that works with the Privacy Officer and our Physicians in marketing for our organization. We do have a business associate agreement in place.

2. We will make sure in all our communications that we tell patients how to opt out of future marketing communications. According to the final HIPAA privacy regulations, a marketing communication won't fall into the "no patient authorization" exception for "certain health-related products and services" unless it describes how the patient may opt out of getting any further marketing communications from the sender. So, for example, in each letter or brochure you send to a patient about your health-related products and services, you should include a statement telling the patient that they may opt out of receiving any future marketing communications from you. One way to do that is to have patient's initial and return the marketing communication to you. Below is Model Language we can adapt and use for this statement.

Model Language.

Periodically, we send communications to friends and neighbors in our health care community that describe the health care services and products we offer. If you would prefer not to receive communications like this from our organization in the future, please indicate this by placing your initials on the line provided below and returning this (letter/brochure/card/whatever this is) to the following address for processing: Radiology Consultants, 9601Baptist Health Drive, Suite 1100, Little Rock, AR 72205. Please note that it will take approximately six weeks to process your request.

☐ I do not wish to receive future communications from Radiology Consultants that describe the health care services and products it offers. Please remove my name, address and phone number from your mailing lists.

Initial here: _____

Effective Date: April 14, 2003

Communicating With Patients About Their Rights

Policy:

1. Patients have several rights in terms of their PHI. These include the right to:

    - Request special restrictions on otherwise permissible uses and disclosures of PHI
    - Confidential communications.
    - Have access to inspect and obtain a copy of their PHI
    - Amend their PHI
    - Receive an accounting of certain disclosures of PHI.

2. Our patients will be provided with a copy of our Notice of Privacy Practices at the time of service that will describe how medical information about them may be used and disclosed and how they can get access to that information.

3. The Notice will be displayed in the waiting room as well as on the company website at www.radconlr.com.

Effective Date: April 14, 2003
Revised Date: November 20, 2015

Procedure for Communicating With Patients About Their Rights

Procedure:

1. At the time of service we will provide the patient with a copy of our Notice of Privacy Practices that will describe how medical information about them may be used and disclosed and how they can get access to that information.

2. The Notice will be posted on our company website at www.radconlr.com as well as displayed in the waiting room.

3. The patient will be asked to sign an acknowledgment that they received the Notice.

4. We will document on our computer that the patient was given a copy of the Notice and the Receipt of Notice of Privacy Practices form will be filed in the patient's folder.

5. Our office will be glad to answer any questions the patient may have.

Effective Date: April 14, 2002

Procedure for Handling Confidential Communications

Procedure:

1. We will require the request for confidential communication to be made in writing.

2. If we agree the request is reasonable, we will place a comment in the computer on the account as to how and when the delivery of the confidential information is to be given out and an alternative address or other method of contact.

3. The request and response will be filed in the patient's account if it is an office patient and in the Correspondence File in Patient Accounts if the patient is from another place of service.

Effective Date: April 14, 2003

Individual's Right to Access/Obtain an Accounting of Disclosures of PHI

Policy:

1. Patients have the right to an accounting of disclosures made by the Company and its business associates for disclosures other than these:

    - For treatment, payment or health care operations
    - To a patient concerning the patient's protected health information
    - Pursuant to an authorization
    - To persons assisting in a patient's care (made pursuant to their agreement)
    - For national security or intelligence purposes
    - For correctional institutions or law enforcement officials as provided for under the Privacy Standards
    - Disclosures that occurred prior to the compliance date, which is currently April 14, 2003

2. Patients have a right to an accounting of the applicable disclosures that have been made by the Company and its business associates in the six (6) year period following the HIPAA compliance deadline of April 14, 2003 and prior to the date of the request for an accounting.

3. An accounting of a disclosure must include all required information. Required information includes the date of the disclosure; the name of the entity or person who received the protected health information; and, if known, their last known address; and a brief description of the protected health information disclosed. The accounting must also contain a brief statement of the purpose or reason for the disclosure or, in lieu of the statement, a copy of the patient's written authorization, or a written request for disclosure from the Secretary of Health and Human Services or other appropriate party made pursuant to one of the public policy-related purposes discussed in the Privacy Standards.

    The Company will document and maintain:

    - The information required to be included in accountings
    - Accountings provided patients
    - The titles of the persons or offices responsible for receiving and processing requests for an accounting
    - Statements by health care oversight agencies or law enforcement officials regarding the need to temporarily suspend a patient's right to an accounting. It will maintain this documentation for a period of six (6) years from the date they are created.

Effective Date: April 14, 2003
Revised Date: November 20, 2015

Procedure for Individual's Right to Access/Obtain an Accounting of Disclosures of PHI

Procedure:

1. Patients have a right to an accounting of the applicable disclosures that have been made by the Company and its business associates in the six (6) year period following the HIPAA compliance deadline of April 14, 2003 and prior to the date of the request for an accounting.

2. There is a Request for an Accounting of Disclosures form that the patient may fill out and return to the Privacy Officer. This request explains that the first request is free in a 12 month period but for subsequent requests in the same 12 month period, the charge is $20.00.

3. The response time by the Privacy Officer will be made in writing within 60 days after receipt. If we are unable to provide the requested information within the allowable time frame, we will be allowed a one-time 30 day extension.

4. We will provide the patient with a written statement explaining the reasons for the delay and the date by which action on the request will be completed during the initial 60 day time period.

5. Documentation will be scanned in the computer on the patient's account and the form and response will be scanned in the patient's demographics if it is an office account or in the Correspondence File in Patient Accounts if the patient is from another place of service.

Request for an Accounting of Disclosures

I. PATIENT INFORMATION.

Date of Request: _____

Name: _____ Date of birth: _____

Address: _____
_____

Address to send disclosure accounting (if different from above): _____
_____

II. DATES REQUESTED

I would like an accounting of all disclosures for the following time frame. Please note: the maximum time frame that can be requested is six years prior to the date of your request.

From: _____ To: _____

III. FEES

There is no charge for the first request for an accounting in a 12-month period. For subsequent requests in the same 12-month period, the charge is $20.00. I understand that there is (check one):

____ No fee for this request:

____ A fee for this request in the amount of $20.00, and I wish to proceed.

IV. RESPONSE TIME

I understand that the account I have requested will be provided to me within 60 days unless I am notified in writing that an extension of up to 30 days is needed.

Signature of patient or legal representative: _____

Date: _____

V. THIS SECTION IS FOR RADIOLOGY CONSULTANTS USE ONLY

Date request was received: _____ Date accounts sent: _____

Extension requested (circle one): Yes / No. If yes, give reason. _____
_____

Patient notified in writing on this date: _____

Staff member processing request: _____

Effective Date: April 14, 2003

Entity's Right to Suspend Accounting of PHI

Policy:

1. The covered entity must temporarily suspend an individual's right to receive an accounting of disclosures to a health oversight agency or law enforcement official, respectively, for the time specified by such agency or official, if such agency or official provides the covered entity with a written statement that such an accounting to the individual would be reasonably likely to impede the agency's activities and specifying the time for which such a suspension is required.

2. The request must be made in writing and we will:

    - Document the statement, including the identity of the agency or official making the statement.

    - Temporarily suspend the individual's right to an accounting of disclosures subject to the statement.

    - Limit the temporary suspension to no longer than 30 days from the date of the written statement, unless a written statement is submitted during that time.

2. An individual may request an accounting of disclosures for a period of time less than six years from the date of the request.

Effective Date: April 14, 2003
Revised Date: November 20, 2015

Procedure for Entity's Right to Suspend Accounting of PHI

Procedure:

1. We are required to temporarily suspend an individual's right to receive an accounting of disclosures on records that have been requested from a health oversight agency or law enforcement official, respectively, for the time specified by such agency or official. The agency's written statement should specify the time for which the suspension is required.

2. We will require the request to be made in writing. The procedure will be as follows:

   - We will place a comment in the computer on the account documenting the request including the identity of the agency or official making the statement.

   - The comment will temporarily suspend the individual's right to an accounting of disclosures subject to the statement.

   - Limit the temporary suspension to no longer than 30 days from the date of the oral statement, unless a written statement is submitted during that time.

   - We scan a copy of the request in the patient's x-ray demographics if it is an office account and in the Correspondence File by the date of the comment if it is a patient from another place of service.

   - An individual may request an accounting of disclosures for a period of time less than six years from the date of the request.

Effective Date: April 14, 2003

Timely Action for Accounting for Disclosures of PHI

Policy:

The Company will provide an accounting within sixty (60) days of receiving such a request. If the Company is unable to do so, the Company may have a one-time extension of no more than thirty (30) days, provided that within the initial sixty (60) day time period, the Company supplies the patient a written statement of the reasons for the delay and the date by which the Company will complete its action on the request.

Effective Date: April 14, 2003
Revised Date: November 20, 2015

Procedure for Timely Action for Accounting for Disclosures of PHI

Procedure:

1. An individual has a right to receive an accounting of disclosures of protected health information made by a covered entity in the six years prior to the date on which the accounting is requested, except for disclosures:

    - To carry out treatment, payment and health care operations.
    - To individuals of protected health information about them.
    - For the facility's directory or to persons involved in the individual's care or other notification purposes.
    - For national security or intelligence purposes.
    - To correctional institutions or law enforcement officials.
    - That occurred prior to the compliance date for the covered entity.

2. The Company will provide an accounting within sixty (60) days of receiving such a request. If the Company is unable to do so, the Company may have a one-time extension of no more than thirty (30) days, provided that within the initial sixty (60) day time period, the Company supplies the patient a written statement of the reasons for the delay and the date by which the Company will complete its action on the request.

    - The patient's request will be given to the Privacy Officer. The response time by the Privacy Officer will be made in writing within 60 days after receipt.
    - If we are unable to provide the requested information within the allowable time frame, we will be allowed a one-time 30 day extension.
    - We will provide the patient with a written statement explaining the reasons for the delay and the date by which action on the request will be completed during the initial 60 day time period.
    - Documentation will be scanned in the computer on the patient's account and the information will be scanned in the patient's demographics if it is an office patient and in the Correspondence File in Patient Accounts if the patient is from another place of service under the date of the comment.

Effective Date: April 14, 2002

Cost-based Fees for Multiple Accountings Within a 12-month Period

Policy:

Patients will be given one free accounting per twelve (12) month period. For each additional request by a patient within the twelve (12) month period, the Company may, with prior notice, charge a reasonable, cost-based fee.

Effective Date: April 14, 2002

Cost-based Fees for Multiple Accountings Within a 12-month Period

Procedure:

1. We may charge a reasonable amount based on our costs for subsequent accountings made in a 12-month period. However, we must inform the patient and allow him to withdraw the request.

2. We will provide a Request for an Accounting of Disclosures form for the patient to fill out and return has this option to accept the fee or decline if applicable.

The fee will be $20.00 and will be billed at the time we provide the accounting

Effective Date: April 14, 2003

Documentation for Requests and Restrictions of PHI

Policy:

1. For routine requests or disclosures of protected health information, the Company will establish policies and procedures to limit the amount of information requested or disclosed to the minimum amount necessary to accomplish the purpose of the request or disclosure.

2. The Company makes the following types of routine disclosures and has determined that the following information is the minimum necessary protected health information in such circumstances:

    - for disclosures to accreditation organizations - all relevant information requested consistent with the organization's protocols and methodologies, including the entire medical record;
    - for disclosures to attorneys - all relevant information requested by the attorneys;
    - for disclosures to risk managers at malpractice insurance companies - all relevant information requested by the risk managers;
    - for billing, coding, or practice management consultants - all relevant information consistent with their protocols or methodologies;
    - for disclosures to billing companies - all information required to file health care claims, but not the entire medical record, unless verification of billing and coding is to be provided by the billing company; and
    - for disclosures to transcriptionists - all information which needs transcribing, as well as any documents useful to ensuring the accuracy of those transcriptions.

3. The Company does not violate the Privacy Standards when it makes incidental uses and disclosures of PHI that cannot reasonably be prevented, that are limited in nature, and that occur as a by-product of an otherwise permitted uses or disclosures, so long as reasonable safeguards are taken to minimize the chance of incidental disclosure to others.

Effective Date: April 14, 2003
Revised Date: November 20, 2015

Procedure for Documentation for Requests and Restrictions of PHI

Procedure:

1. We will ask the individual to make requests for restrictions in writing. A Request for an Accounting of Disclosures form will be provided in order help expedite the request for accountings.

2. Each request for accounting and restriction of PHI will be documented in the computer on the account to include the date of the request, the date the information is provided, and who processed the information.

3. The request and response will be scanned in the patient's demographics if it is an office patient and in the Correspondence File in Patient accounts if the patient is from another place of service.

4. The information will be maintained for six years.

Effective Date: April 14, 2003
Revised Date: November 20, 2015

Processing Requests for an Accounting of Disclosures of PHI

Procedure:

Patients have the right to get written accounting of disclosures of their PHI made by our company during the past six years. We do not have to account for disclosures made for the purpose of treatment, payment and health care operations (TPO), disclosures to the patient, individuals involved in the patient's care, federal officials for national security or intelligence purposes, or to correctional institutes or law enforcement officials. If we have the patient's authorization to make the disclosure, the disclosure will not be included in the accounting. We only have to account for disclosures to business associates for non-TPO purposes.

1. The patient will be required to complete a Request for an Accounting of Disclosures form in order help expedite the request for accountings. The dates requested may only go back six years prior to the date of the request and we are not required to account for disclosures that occurred before April 14, 2003.

2. If our organization has accepted a request to restrict information, we will not give out the restricted PHI unless needed to provide emergency treatment.

3. The Privacy Officer will respond within 60 days with a one time 30 day extension if needed with the patient is informed in writing within the 60 days of the reason for the delay and the date the accounting will be provided.

4. Each request for accounting will be documented in the computer on the account to include the date of the request, the date the information is provided, who processed the information, and a brief statement explaining why the PHI was disclosed or that reasonably informs the patient of the purpose of the disclosure, or a copy of the patient's authorization or written request for disclosure.

5. We will not charge for the first accounting of PHI. We will charge $20.00 for additional accountings made in a 12 months period. This is address in the Request for an Accounting of Disclosures form the patient is required to fill out.

6. The request form and response will be scanned in the patient's demographics if it is an office patient and in the Correspondence File in Patient Accounts if the patient is from another place of service.

7. The information will be maintained for six years.

Section I: Privacy Standards

6. Breaches

PLEASE NOTE THAT THIS SAMPLE FORM MUST BE REVIEWED AND CUSTOMIZED TO FIT YOUR PARTICULAR NEEDS AND CIRCUMSTANCES

The only purpose of this **Sample Breach Notification Letter to Patient** is to serve as an informational example. It is not intended – and it should not be used – as a "one size fits all" form. It should be carefully reviewed and customized to fit your particular needs and circumstances. It is not legal advice, nor should it substitute for legal advice. You should always seek the advice of an attorney before using this Sample to develop a document that fits your particular situation and needs.

[Date]

[Patient Name]
[Address 1]
[Address 2]
[City, State, Zip]

Dear **[Patient Name]:**

I am writing to inform you of a breach, or potential breach, of your personal information from **[Clinic Name or Business Associate Name]** which we believe or understand occurred on or about **[Date of Breach]**. We became aware of this breach on **[Date of Discovery]**.

To the extent possible, the following information must be included in your letter:

- **A brief description of the breach**
- **A description of the types of information involved in the breach**
- **Steps patients should take to protect themselves from potential harm**
- **A brief description of what you have done to investigate the breach, mitigate the harm and prevent further breaches**
- **Contact information for patients if they have questions**

If the use or disclosure involved personally identifiable information or information that could be used for purposes of identity theft, below is sample language for steps patients can take for protection. This may not be appropriate if the use or disclosure only includes medical information.

While you are not required to take any action, we suggest that you monitor your credit and personal information for any suspicious activity. To help you with this process, [Clinic Name] will reimburse you for the cost of a credit check through Equifax, which is one of the three major credit reporting bureaus. You can obtain this credit check for approximately eleven to sixteen dollars by contacting Equifax at 1-866-493-9788. If

your Equifax credit check shows that an account has been fraudulently established using your identity since [Insert Date Breach], [Clinic Name] will provide Equifax credit monitoring to you as a courtesy and free of charge for 12 months.

In addition, you may consider taking the following steps to protect yourself:

- Call the toll-free numbers of any one of the three major credit bureaus (below) to place a fraud alert on your credit report. This can help prevent an identity thief from opening additional accounts in your name. As soon as the credit bureau confirms your fraud alert, the other two credit bureaus will automatically be notified to place alerts on your credit report, and all three reports will be sent to you free of charge.

    - **Equifax:** 1-800-525-6285; www.equifax.com; P.O. Box 740241, Atlanta, GA 30374-0241.
    - **Experian:** 1-888-EXPERIAN (397-3742); www.experian.com; P.O. Box 9532, Allen, TX 75013.
    - **TransUnion:** 1-800-680-7289; www.transunion.com; Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834-6790.

- Order your credit reports. By establishing a fraud alert, you will receive a follow-up letter that will explain how you can receive a free copy of your credit report. When you receive your credit report, examine it closely and look for signs of fraud, such as credit accounts that are not yours.

- Continue to monitor your credit reports. Even though a fraud alert has been placed on your account, you should continue to monitor your credit reports to ensure an imposter has not opened an account with your personal information.

Protecting our patients' privacy is very important to us. We apologize for any inconvenience or concern this may cause, but we believe it is important for you to be fully informed of any potential risk resulting from this incident.

If you have questions or concerns, please contact **[Clinic Privacy Office]** at **[Phone number, email, address, etc.]**

Sincerely,

[Physician or Privacy Officer/Administrator]

SAMPLE POLICY ON NOTIFICATION OF BREACHES OF UNSECURED PROTECTED HEALTH INFORMATION

I. Notification of Breach Policy

Radiology Consultants will notify a patient in writing by first class mail, by hand delivery, or by courier service such as FedEx or UPS, or by e-mail (if the patient has indicated a preference for being notified by e-mail) of any Breaches of the patient's Unsecured Protected Health Information of which we become aware as soon as possible, but in any event, not later than 60 days following our discovery of the Breach. In urgent cases, we may use an alternative form of notification, such as telephone, in conjunction with written notification.

II. Applicability of Policy on Notification of Breaches.

This policy only applies to "Breaches" of "Unsecured Protected Health Information."

A. **"Unsecured Protected Health Information"** is information that is not secured through the use of a technology or methodology identified by the Secretary of Health and Human Services to render the PHI unusable, unreadable and undecipherable to unauthorized users. "Unsecured Protected Health Information" may be in written, oral, or electronic format. Limited Data Sets (except those that have been stripped of zip code and date of birth) are subject to the Breach reporting requirements.

B. **Exceptions to Unsecured PHI.** The following information is not considered to be "Unsecured Protected Health Information" and is therefore not subject to this policy:

1. "De-Identified Health Information" which, by definition, is not PHI;

2. PHI that is encrypted according to an encryption algorithm and for which there is security of the decryption key or process. The encryption key must be kept on a separate device from the encrypted data to ensure that the key is not breached;

3. PHI that has been destroyed, *i.e.*, the media on which the PHI is stored or received have been destroyed so that:

a. paper, film, or other copies have been shredded and the PHI cannot be read or reconstructed, and

b. electronic media have been cleared, purged, or destroyed consistent with NIST Special Publication 800-88, Guidelines for Media Sanitation.

Redaction does not satisfy the requirement for destruction. But if all identifiers have been redacted, the information is not subject to this policy.

C. **"Breach"** is the unauthorized acquisition, access, use, or disclosure of PHI which compromises the security or privacy of the PHI.

1. An impermissible use or disclosure of PHI that is incidental to an otherwise permissible use or disclosure and that occurs despite reasonable safeguards and proper minimum necessary procedures is not considered a Breach.

2. Uses and disclosures of more than the "minimum necessary" information may constitute a Breach.

An unauthorized acquisition, access, use or disclosure of PHI is presumed to be a breach unless Radiology Consultants demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment of at least the following factors:

1. The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;

2. The unauthorized person who used the protected health information or to whom the disclosure was made;

3. Whether the protected health information was actually acquired or viewed; and

4. The extent to which the risk to the protected health information has been mitigated.

D. **"Discovery"** of a Breach is the first day on which the circumstances of a Breach are known to any employee, officer, or agent of Radiology Consultants, other than the person who committed the Breach.

III. "Red Flags" That Indicate a Potential Breach

Some "red flags" that might be warning signs of a Breach or a security problem are: virus infection or suspicious system activity (such as a mouse pointer moving

erratically, unknown programs launching, strange or unknown screen splashes); unknown system logon record or transaction processing; unusual number of logon failures, indicating potential hacker activity; unusual or suspicious request for information by an outsider or internal workforce member; suspicious system activity that cannot be readily explained; someone using other system IDs and passwords; stolen or missing media devices.

IV. Exceptions to Notification of Breach.

The following circumstances do not require us to give notice of a Breach:

A. Unintentional Access.

Unintentional acquisition, access, or use of PHI by a member of our workforce or an individual acting under our authority, provided that the unintentional activity was done in good faith, within the course of employment or other professional relationship, and does not result in further use or disclosure that is not permitted by the Privacy Rule.

B. Inadvertent Disclosure

Inadvertent disclosure of PHI by a person with authority to access the PHI at our business to another person who also has authority to access PHI, provided the recipient is part of Radiology Consultants, and provided the recipient does not further disclose the information in violation of the Privacy Rule.

C. Good Faith Unauthorized Disclosures

Unauthorized disclosures where, based on the good faith belief of the disclosing person, the recipient to whom the PHI is disclosed would not reasonably have been able to retain the information.

V. Contents of Notice of Breach.

The notices required under this policy shall include the following:

1. a brief description of the breach, including the date of the breach and the date of its discovery, if known;

2. a description of the types of Unsecured Protected Health Information involved in the breach;

3. steps the patient should take to protect himself/herself from potential harm resulting from the breach;

4. a brief description of the actions we are taking to investigate the breach, mitigate losses, and protect against further breaches;

5. contact information, including a toll-free telephone number, e-mail address, Web site or postal address to permit the patient to ask questions or obtain additional information;

6. any sanctions imposed on any workforce member involved in the breach.

VI. Breaches Affecting Ten or More Patients

A. Posting Notice of Breach When Ten or More Patients Are Involved

If a breach involves 10 or more patients whose contact information is out of date we will post a notice of the breach on the home page of our Website or in a major print or broadcast media outlet.

B. Media Posting When a Breach Involves More Than 500 Patients

If a breach involves more than 500 patients in a state or jurisdiction, we will send notices of the breach to prominent media outlets in those states or jurisdictions. We are not required to notify media outlets if no one state has more than 500 affected patients.

C. Notice to Secretary When a Breach Involves More Than 500 Patients

If a breach involves more than 500 patients, we will immediately notify the Secretary of the Department of Health and Human Services, no matter whether a state has more than 500 affected patients. In no case shall notification be made later than 60 days from discovery of the breach. We must submit the notice electronically on the appropriate form, which can be accessed at HHS.gov, OCR Home, Health Information Privacy, Breach Notification Rule. If, after we have submitted a breach notification form to the Secretary, we discover additional information to report, we will submit an additional form, checking the appropriate box to indicate that we are making an updated submission.

VII. Annual Report to Secretary and Maintenance of Log

We will maintain a written log of all breaches, regardless of how many patients are affected. We will submit an annual report to the Secretary of any breach that involves fewer than 500 patients during the year. We will submit that annual report within 60 days of the end of the calendar year in which the breaches occurred. This notice must be submitted electronically by accessing the appropriate form at HHS.gov, OCR Home, Health Information Privacy, Breach Notification Rule, and completing all information required on the breach notification form. A separate form must be completed for every breach that has occurred during the calendar year.

If, after we have submitted a breach notification form to the Secretary, we discover additional information to report, we will submit an additional form, checking the appropriate box to indicate that we are making an updated submission.

This Policy was last updated on November 20, 2015.

HIPAA Privacy and Security Standards

Policies and Procedures

Section II: Training and Education

Section II: Training and Education

Effective Date: April 14, 2002

Training Policy

Policy:

1. All members of the Company's workforce must undergo training on the Company's HIPAA and Corporate Compliance policies and procedures, as necessary and appropriate for the individuals to carry out their functions.

2. Initial training will occur before the compliance date, which is April 14, 2003.

3. For persons joining the workforce after the date of the initial training, training will be required within a reasonable period of time after the person joins the workforce. When the Company makes a material change in its privacy policies it will retrain those affected by the change within a reasonable period of time.

4. All members of the workforce will sign an acknowledgement when they have completed required training. This documentation will be maintained by the Privacy Officer for six (6) years from the date the acknowledgement is signed.

Effective Date: April 14, 2002
Revised Date: November 20, 2015

Procedure for HIPAA Training

Procedure:

1. All current employees, including physicians, supervisors and staff will undergo HIPAA training.

    - Physicians:

        - Administrator or other HIPAA consultant to explain HIPAA regulations, deadlines, risks & penalties.

    - Supervisors / Staff:
        - HIPAA - SVMIC website
        - Broad scope of regulations
        - Go over their job description for HIPAA regulations

2. Training of current employees will be done the month of December 2015.

3. New employees after December 2015 will be trained on their first day of work. (SVMIC website)

4. Annual training will be given to all employees. (SVMIC website)

5. All employees will sign that they have received training. This will be filled in the employee's personnel folder.

6. All employees will read and sign the Confidentiality Agreement.

Employee E-mail Usage Policy

E-mail is to be used for Radiology Consultants business and should not be overused or misused. Personal e-mail use is allowed before 8:00 a.m. and after 5:00 p.m. E-mail is an efficient way to send urgent messages or those designed to communicate with multiple people simultaneously. Use extreme caution to ensure that the correct e-mail address is used for the intended recipient(s).

Radiology Consultants may access and monitor e-mail at any time for any reason without notice. You should not expect or treat e-mail as confidential or private. E-mail users must provide the network administrator with passwords. Except for authorized Company personnel, no one is permitted to access another person's e-mail without consent.

System users should exercise extreme judgment and common sense when distributing messages. Confidential information should never be disseminated to unauthorized sources. This includes the transmission of documents containing financial information or Social Security numbers. Client-related messages should be carefully guarded and protected, like any other written materials. You must also abide by copyright laws, ethics rules and other applicable laws.

Sending harassing, abusive, intimidating, discriminatory, or other offensive e-mails is strictly prohibited. The use of the system to solicit for any purpose without the consent of the human resources director is strictly prohibited. If you receive a message containing defamatory, obscene, offensive or harassing information, or that discloses personal information without permission, you must delete it immediately and not forward it. Chain-type messages and executable graphics files should also be deleted and not forwarded because they cause overload on our system. Anyone engaging in the transmission of inappropriate emails, as determined by the Company, will be subject to discipline, up to and including termination.

I have read the Company's e-mail policy and agree to abide by it as consideration for my continued employment. I understand that violation of any of the above policies may result in my termination.

_____ _____

User Signature Date

Radiology Consultants
Workforce Confidentiality Agreement

As a member of the workforce at *Radiology Consultants* ("Practice"), I understand the following in regard to HIPAA and patient confidentiality:

- The Practice has an ethical and legal responsibility to ensure the confidentiality of patient information. As a member of their workforce, I also have this responsibility.
- As a condition of my employment, I agree to abide by all policies and procedures related to the privacy and security of all patients' protected health information (PHI).
- I will access, use and/or disclose **only** the PHI that is required for the performance of my job duties. If I have a question about whether or not I should access certain information, I will immediately check with my supervisor or the Privacy Officer.
- Any personal access codes, user IDs, and passwords that I am assigned will be kept confidential at all times and are not to be shared with other workforce members.
- I will not remove any PHI from the Practice, in paper or electronic form, without proper approval from my supervisor or the Privacy Officer.
- I will not disclose information pertaining to patients with anyone that is not authorized to receive such information. This includes but is not limited to, acquaintances, friends, and/or family members.
- I will not disclose PHI on any social media site, such as Facebook or Twitter, or any other internet outlet; including any discussion or description of patients (even if the patient is not specifically identified).
- I will not transmit PHI on any mobile device without using a secure messaging application approved by the Practice. This includes texting PHI to physicians, other workforce members and/or patients. I understand that texting PHI using the regular text messaging application on my phone can result in a HIPAA violation.
- I will not email PHI using a personal email account or any email account not approved by the Practice. If my job requires the use of email, I will follow the specific guidelines established for email by the Practice.
- I will not discuss information pertaining to patients with other workforce members, unless I have a valid work-related reason to do so.
- I will not make any unauthorized copies, modifications or deletion of PHI. This includes, but is not limited to, transferring PHI from the Practice's computer system to an unauthorized location, such as a personal computer, USB drive or personal email.
- Upon termination of my employment with the Practice, I will immediately return all property belonging to the Practice. This would include, but is not limited to, keys to the facility, ID badges, documents, electronic files, computer equipment and/or mobile devices.
- I agree that my obligation to maintain confidentiality of PHI will continue after the termination of my employment. I understand that knowingly using or disclosing PHI in violation of the HIPAA Privacy Rule is a criminal offense and I may personally face fines and/or time in jail.
- Any violation of this Agreement may result in disciplinary action, up to and including termination of my employment with the Practice.

I have read the above agreement and agree to comply with all of the terms as a condition of my employment with the Practice.

Signature of
Workforce Member: _____ Date: _____
(Employee/physician/student/volunteer)

Printed Name: _____

Privacy Officer Signature: _____ Date: _____