



INFORMATION SECURITY POLICY
Radiology Consultants of Little Rock, P.A.

Last Revision Date

May 1, 2016

Radiology Consultants of Little Rock, P.A.

HIPAA Information Security Policies

The following plans, policies and procedures have been reviewed by the appropriate personnel including, Security Officer, Privacy Officer, Confidentiality and Security Team, and Providers.

Title	Revision Date
Introduction	2016
Employee Responsibilities	2016
Identification and Authentication	2016
Network Connectivity	2016
Malicious Code	2016
Encryption	2016
Building Security	2016
Telecommuting	2016
Removable Media	2016
Mobile Devices and Phones	2016
Retention/Destruction of Practice Information	2016
Disposal and Reuse of Electronic Media	2016
Change Management	2016
Audit Controls	2016
Information System Activity Review	2016
Data Integrity	2016
Contingency Plan	2016
Security Awareness and Training	2016
Security Management Process	2016
Emergency Operations Procedures	2016
Emergency Access "Break the Glass"	2016
Sanction Policy	2016
Employee Background Checks	2016
Incident and Breach Notification Procedure	2016
Business Associate Policy	2016

Annual Policy review and approval

Date 4/22/16 Approved by: [Signature] Title: Security Officer

Date 7/22/16 Approved by: [Signature] Title: Privacy Officer

Date _____ Approved by: _____ Title: _____

Table of Contents

- Introduction 1
 - Purpose 1
 - Scope 1
 - Privacy Officer 2
 - Security Officer – Job Description 2
 - Confidentiality / Security Team (CST)..... 3
- Employee Responsibilities 4
 - Employee Requirements 4
 - Prohibited Activities 5
 - Electronic Communication, E-mail, Internet Usage 5
 - Internet Access 7
 - Reporting Software Malfunctions..... 7
 - Report Security Incidents 8
 - Transfer of Sensitive/Confidential Information 8
 - Transferring Software and Files between Home and Work..... 8
 - Internet Considerations 9
 - Use of Encryption for Files and E-mail 9
 - De-identification / Re-identification of Protected Health Information (PHI) 9
- Identification and Authentication 11
 - User Login IDs 11
 - Passwords 11
 - Confidentiality Agreement 12
 - Access Control 12
 - User Login Entitlement Reviews 13
 - Termination of User Login Account..... 13
- Network Connectivity 14
 - Dial-In Connections..... 14
 - Dial-Out Connections 14
 - Telecommunication Equipment 14
 - Permanent Connections 15
 - Emphasis on Security in Third Party Contracts 15
 - Firewalls 16
- Malicious Code: 17
 - Anti-virus Software Installation 17
 - New Software Distribution 17
 - Retention of Ownership 18
- Encryption 19
 - Policy 19
 - Equipment Encryption (data at rest): 19
 - Transmitted Data (data in motion): 20
 - Exceptions 20
- Building Security 21
- Telecommuting/Remote Access 23
 - General Requirements 23
 - Required Equipment 23
 - Hardware Security Protections 24
 - Data Security Protection 24
 - Disposal of Paper and/or External Media 25
- Removable Media 26
 - Definitions 26
 - Removable Media Usage Standards and Policy 26
- Mobile Devices and Phones 28
 - Definitions 28

Mobile Device Usage Standards and Policy	28
Retention / Destruction of Practice Information.....	31
Disposal and Reuse of Electronic Media.....	32
Change Management	34
Statement of Policy.....	34
Procedure.....	34
Audit Controls	35
Statement of Policy.....	35
Procedure.....	35
Information System Activity Review	36
Statement of Policy.....	36
Procedure.....	36
Data Integrity.....	38
Statement of Policy.....	38
Procedure.....	38
Contingency Plan	39
Statement of Policy.....	39
Procedure.....	39
Security Awareness and Training.....	42
Statement of Policy.....	42
Procedure.....	42
Security Management Process.....	45
Statement of Policy.....	45
Procedure.....	45
Emergency Operations Procedures.....	49
Notification:.....	49
Scheduling:.....	49
Patient Encounters:.....	49
System Restoration:.....	50
Emergency Access “Break the Glass”	51
Policy.....	52
Procedures	52
Sanction Policy.....	54
Violations	55
Recommended Disciplinary Actions	55
Employee Background Checks.....	57
Incident and Breach Notification Procedures	59
Procedure.....	60
Containing the Breach	60
Notification.....	61
Prevention.....	62
Business Associate Policy	63
Procedure.....	63
Appendix A – Network Access Request Form.....	66
Appendix B – Workforce Confidentiality Agreement.....	68
Appendix C – Approved Software	70
Appendix D – Approved Contractors	71
Appendix E – Device Inventory for Electronic Devices	72
Appendix F – Incident Response Tools for Privacy and Security	73
Appendix G – Background Check Authorization.....	74
Appendix H – Change Management Tracking Log.....	76
Appendix I – Employee Termination Checklist	77
Appendix J - Bring Your Own Device Agreement.....	78
Appendix K – Contractor Confidentiality Agreement.....	80

Radiology Consultants of Little Rock, P.A.	
Policy and Procedure	
Title: INTRODUCTION	P&P #: IS-1.0
Approval Date: 5/1/2016	Review: Annual
Effective Date: 5/1/2016	Information Technology

Introduction

Purpose

This policy defines the technical controls and security configurations users and Information Technology (IT) administrators are required to implement in order to ensure the confidentiality, integrity and availability of the data environment at Radiology Consultants of Little Rock, P.A., hereinafter, referred to as the **Practice**. It serves as a central policy document which all employees and contractors must be familiar and defines actions and prohibitions that all users must follow. The policy provides IT managers within the Practice policies and guidelines concerning the acceptable use of Practice technology equipment, e-mail, Internet connections, voice-mail, facsimile and future technology resources and information processing.

The policy requirements and restrictions defined in this document shall apply to network infrastructures, databases, external media, encryption, hardcopy reports, films, slides, models, wireless systems, telecommunication, conversations, and any other methods used to convey knowledge and ideas across all hardware, software, and data transmission mediums. This policy must be adhered to by all Practice employees and temporary workers at all locations including all contractors working with the Practice as subcontractors.

The Practice will make documentation available to those persons responsible for implementing the procedures to which the documentation pertains.

Scope

This policy document defines common security requirements for all Practice personnel and systems that create, maintain, store, access, process, receive, or transmit information. This policy also applies to information resources owned by others, such as contractors of the Practice, entities in the private sector, in cases where Practice has a legal, contractual or fiduciary duty to protect said resources while in Practice custody. In the event of a conflict, the more restrictive measures will apply. This policy covers the Practice network systems which consist of various hardware, software, communications equipment, mobile devices and other equipment designed to assist the Practice in the creation, receipt, storage, processing, and transmission of information. This definition includes equipment connected to any Practice domain or VLAN, either hardwired or wirelessly, and includes all stand-alone equipment that is deployed by the Practice at its office locations or remote locales.

Applicable Statutes / Regulations

The following is a list of the various agencies/organizations whose laws, mandates, and regulations were incorporated into the various policy statements included in this document.

CMS, DHHS, OCR-HIPAA, CLIA, DEA

Each of the policies defined in this document is applicable to the task being performed – not only to specific departments or job titles.

Privacy Officer

The Practice has established a Privacy Officer as required by the HIPAA Privacy Rule. The Privacy Officer will oversee all ongoing activities related to the development, implementation, maintenance, and oversight of the Practice’s privacy policies and procedures and privacy training program in accordance with applicable federal and state laws. The current Privacy Officer for the Practice is:

Lucille Whitlow

Alternate Privacy Officer (contact in the event Privacy Officer is unavailable.)

Annette Bowman

Security Officer – Job Description

The Practice has established a Security Officer as required by HIPAA. The job responsibilities of the Security Officer include the management and supervision of use of security measures to protect data, and conduct of personnel in relation to the protection of data.

The primary goals of the Security Officer are to protect the confidentiality and integrity of information, and maintain the technical mechanisms of legitimate access to it. To achieve these goals, the Security Officer’s responsibilities include:

- Oversight all ongoing activities related to the development, implementation, and maintenance of the Practice security policies
- Work closely with the Privacy Officer and Confidentiality / Security Team
- Direct/Indirect supervision of employees with access to patient information monitor, and when issues share according to organizational chart
- Arranging security training for all employees, providers, and others third parties
- Monitoring compliance with the organization’s information security policies and procedures among employees, providers, and other third parties
- Identifying problems and conducting breach investigation including resolution, notification, and documentation
- Monitoring internal control systems to ensure that appropriate information access levels and security clearances are maintained
- Arranging information security risk assessments and serving as the internal auditor for information security processes
- Preparing the organization’s disaster recovery and business continuity plans for information systems
- Monitoring changes in information security technologies and legislation that affect information security for applicability to Practice

The current Security Officer for the Practice is:

David Humphrey

Alternate Security Officer (contact in the event Security Officer is unavailable.)

Lance Ford

Confidentiality / Security Team (CST)

The Practice has established a Confidentiality / Security Team made up of key personnel whose responsibility it is to identify areas of concern within the Practice and act as the first line of defense in enhancing the appropriate security posture.

All members identified within this policy are assigned to their positions by the CEO. The term of each member assigned is at the discretion of the CEO, but generally it is expected that the term will be one year. Members for each year will be assigned at the first senior management meeting of the Practice in a new calendar year. This committee will consist of the positions within the Practice most responsible for the overall security policy planning of the organization - the CEO, PO, CMO, CSO, and the CIO (as applicable). The current members of the CST are:

- Security Officer
- Alternate Security Officer
- Privacy officer
- Alternate Privacy Officer

The CST will meet as necessary, but no less than annually, to discuss privacy and security issues and to review concerns that arose during previous meetings. The CST will identify areas that should be addressed during employee training sessions and review and update privacy and security policies as necessary.

The CST will address privacy and security issues as they arise and recommend and approve immediate actions to be undertaken. It is the responsibility of the CST to identify areas of concern within the Practice and act as the first line of defense in enhancing the security posture of the Practice. Privacy and security will use an integrated model to plan for and manage issues.

The CST is responsible for maintaining a log of privacy and security concerns or other confidentiality issues. This log must be maintained on a routine basis, and must include the dates of an event, actions taken to address the event, and recommendations for any personnel actions, if appropriate. This log will be reviewed during the quarterly meetings.

The CST will review these policies periodically and update as needed in response to changes, updates, and modifications based on Practice environmental or operational changes and when Regulation updates are published. CST will authorize any changes to the Information Security Policies and procedures; review and approve retention schedules and address audit findings. Policies and Procedures that require action, activity or assessment will be documented as changes are made and old versions maintained for the required HIPAA retention time frame addressed in the Retention and Destruction of Medical Information policy.

The CST will also keep employees aware of all policies in place at the Practice. Awareness can be achieved through periodic emails, staff meetings, posters, an electronic reminder, etc. Reminders must take place periodically throughout the year and should be documented.

The Security Officer (SO) is responsible for maintaining a log of security enhancements and features that have been implemented to further protect all sensitive information and assets held by the Practice. The Privacy Officer (PO) will keep a similar log concerning privacy matters. These logs will also be reviewed during CST meetings.

Radiology Consultants of Little Rock, P.A.	
Policy and Procedure	
Title: EMPLOYEE RESPONSIBILITIES	P&P #: IS-1.1
Approval Date: 5/1/2016	Review: Annual
Effective Date: 5/1/2016	Information Technology

Employee Responsibilities

Employee Requirements

The first line of defense in data security is the individual Practice user. Practice users are responsible for the security of all data which may come to them in whatever format. The Practice is responsible for maintaining ongoing training programs to inform all users of these requirements.

Identification Process – In order to help maintain building security, and due to the size of the clinic, employees are recognized by sight and are not required to wear name badges. Contractors and visitors who may be in practice facilities are checked in and out at the front desk and should be chaperoned throughout the facility.

Challenge Unrecognized Personnel – It is the responsibility of all Practice personnel to take positive action to provide physical security. If you see an unrecognized person in a restricted Practice office location, you should challenge them as to their right to be there. All visitors to Practice offices must sign in at the front desk. In addition, all visitors, excluding patients, must wear a visitor/contractor badge. All other personnel must be employees of the Practice. Any challenged person who does not respond appropriately should be immediately reported to a Practice manager or supervisor.

Secure Laptops – When out of the office all laptop computers must be secured with a cable lock and/or physically locked in a secure area (cabinet, desk, office, etc.).

Practice computers may contain sensitive data either of a medical, personnel, or financial nature, and the utmost care must be taken to ensure that this data is not compromised. Laptop computers are, unfortunately, easy to steal or misplace, particularly during the stressful period while traveling. Cable locks are not fool proof, but provide an additional level of security. Many laptop computers are stolen in ‘snatch and grab’ robberies, where the thief runs through an office or hotel room and grabs all of the equipment he or she can quickly remove. The use of a cable lock helps to thwart this type of event.

Unattended Computers – Unattended computers must be locked by the user when leaving the work area. This feature is discussed with all employees during regular security training. The Practice policy has been determined that all computers will have an automatic screen lock function set to automatically activate upon thirty (30) minutes of inactivity. Employees are not allowed to take any action which would override this setting.

Workstation – All computer monitors should be turned in such a manner in which patients and visitors cannot view PHI. It is the responsibility of the employee to ensure correct positioning of computer monitors and or use of security screens if applicable. Only the provider/technician and patient being seen should have a view of the equipment screens (i.e. Ultrasound, EKG, etc.). Employees must also clear any equipment screens of PHI before bringing the next patient into the room. Employees should keep their workstation free of excess clutter and food products that could harm the workstation functionality.

Home Use of Practice Corporate Assets – Only computer hardware and software owned by and installed by the Practice is permitted to be connected to or installed on Practice equipment. Only software that has been approved for corporate use by the Practice may be installed on Practice equipment. Personal computers supplied by the Practice are to be used

solely for business purposes. All employees and contractors must read and understand the list of prohibited activities that are outlined below. Modifications or configuration changes are not permitted on any computers supplied by the Practice.

Retention of Ownership – All software programs and documentation generated or provided by employees, consultants, or contractors for the benefit of the Practice are the property of the Practice unless otherwise covered by a contractual agreement. Nothing contained herein applies to software purchased by Practice employees at their own expense.

Training – Employees are required to undergo HIPAA (both privacy and security) training provided by the Privacy and Security Officer upon hire, annually, and periodically.

Organizational Chart – Follow organization chart chain of command.

Prohibited Activities

Personnel are prohibited from the following activities. The list is not inclusive. Other prohibited activities are referenced elsewhere in this document.

- Crashing an information system. Deliberately crashing an information system is strictly prohibited. Users may not realize that they caused a system crash, but if it is shown that the crash occurred as a result of user action, a repetition of the action by that user may be viewed as a deliberate act.
- Attempting to break into an information resource or to bypass a security feature. This includes running password-cracking programs or sniffer programs, and attempting to circumvent file or other resource permissions.
- Introducing, or attempting to introduce, computer viruses, Trojan horses, peer-to-peer (“P2P”) or other malicious software into an information system.
Exception: Authorized information system support personnel, or others authorized by the Practice, may test the resiliency of a system. Such personnel may test for susceptibility to hardware or software failure, security against hacker attacks, and system infection.
- Browsing. The willful, unauthorized access or inspection of confidential or sensitive information to which someone has not been approved on a "need to know" basis or exceeds the minimum amount of information accessed required to perform the required job action is prohibited. The Practice has access to patient level health information which is protected by HIPAA regulations which stipulate a "need to know" before approval is granted to view the information. The purposeful attempt to look at or access information to which you have not been granted access by the appropriate approval procedure is strictly prohibited.
- Personal or Unauthorized Software. Use of personal software is prohibited. All software installed on Practice computers must be approved by the Practice.
- Software/Hardware Use. Violating or attempting to violate the terms of use or license agreement of any software or hardware product used by the Practice is strictly prohibited.
- System Use. Engaging in any activity for any purpose that is illegal or contrary to the policies, procedures or business interests of the Practice is strictly prohibited.

Electronic Communication, E-mail, Internet Usage

As a productivity tool, the Practice encourages the business use of electronic communications. However, all electronic communication systems and all messages generated or handled by Practice owned equipment are considered the property of the Practice – not the property of individual users. Consequently, this policy applies to all Practice employees and contractors, and covers all electronic communications including, but not limited to, telephones, e-mail, voice mail, instant messaging, Internet, fax, workstations, laptops, mobile devices and servers.

Practice provided resources, such as individual computer workstations or laptops, computer systems, networks, e-mail, mobile devices and Internet software and services are intended for business purposes. However, incidental personal use is permissible as long as:

- 1) it does not consume more than a trivial amount of employee time or resources,
- 2) it does not interfere with staff productivity,
- 3) it does not preempt any business activity,
- 4) it does not violate any of the following:
 - a) Copyright violations – This includes the act of pirating software, music, books and/or videos or the use of pirated software, music, books and/or videos and the illegal duplication and/or distribution of information and other intellectual property that is under copyright.
 - b) Illegal activities – The use of Practice resources for, or in support of, illegal purposes as defined by federal, state or local law is strictly prohibited.
 - c) Commercial use – The use of Practice resources for personal or commercial profit is strictly prohibited.
 - d) Political Activities – All political activities are strictly prohibited on Practice premises. The Practice encourages all of its employees to vote and to participate in the election process, but these activities must not be performed using Practice assets or resources.
 - e) Harassment – The Practice strives to maintain a workplace free of harassment and that is sensitive to the diversity of its employees. Therefore, the Practice prohibits the use of computers, e-mail, voice mail, instant messaging, texting and the Internet in ways that are disruptive, offensive to others, or harmful to morale. For example, the display or transmission of sexually explicit images, messages, and cartoons is strictly prohibited. Other examples of misuse includes, but is not limited to, ethnic slurs, racial comments, off-color jokes, or anything that may be construed as harassing, discriminatory, derogatory, defamatory, threatening or showing disrespect for others.
 - f) Junk E-mail – All communications using IT resources shall be purposeful and appropriate. Distributing “junk” mail, such as chain letters, advertisements, or unauthorized solicitations is prohibited. A chain letter is defined as a letter sent to several persons with a request that each send copies of the letter to an equal number of persons. Advertisements offering services from someone else to you. Solicitations are when someone asks you for something. If you receive any of the above, delete the e-mail message immediately. Do not forward the e-mail message to anyone.

The Practice is responsible for servicing and protecting the Practice’s electronic equipment, networks, data, and resource availability and therefore may be required to access and/or monitor electronic communications and data from time to time. Various methods may be employed to accomplish these goals. For example, an audit or cost analysis may require reports that monitor phone numbers dialed, length of calls, number of calls to or from a specific handset, the time of day, etc. Other examples where electronic communications or data may be monitored include, but are not limited to, research and testing to optimize IT resources, troubleshooting technical problems and detecting patterns of abuse or illegal activity.

The Practice reserves the right, at its discretion, to review any employee's files or electronic communications to the extent necessary to ensure all electronic media and services are used in compliance with all applicable laws and regulations as well as Practice policies.

Employees should structure all electronic communications with recognition of the fact that the content could be monitored, and that any electronic communications could be read, forwarded, intercepted, printed or stored by others.

Internet Access

Internet access is provided for Practice use and is considered a great resource for the organization. This resource is costly to operate and maintain, and must be allocated primarily to those with business, administrative or contract needs. The Internet access provided by the Practice should not be used for entertainment, listening to music, viewing sports highlights, games, movies, etc. Do not use the Internet as a radio or to constantly monitor the weather or stock market results. While seemingly trivial to a single user, the company wide use of these non-business sites consumes a huge amount of Internet bandwidth, which is therefore not available to responsible users.

Users must understand that individual Internet usage is monitored, and if an employee is found to be spending an excessive amount of time or consuming large amounts of bandwidth for personal use, disciplinary action will be taken.

Many Internet sites, such as games, peer-to-peer (P2P) file sharing applications, chat rooms, and on-line music sharing applications, may be blocked by Practice routers and firewalls. This list is constantly monitored and updated as necessary. Any employee visiting pornographic sites will be disciplined and may be terminated.

Reporting Software Malfunctions

Users should inform the appropriate Practice personnel when the user's software or computer system does not appear to be functioning correctly. The malfunction - whether accidental or deliberate - may pose an information security risk. If the user, or the user's manager or supervisor, suspects a computer virus infection, the Practice computer virus policy should be followed, and these steps should be taken immediately:

- Stop using the computer.
- Do not carry out any commands, including commands to <Save> data.
- Do not close any of the computer's windows or programs.
- Do not turn off the computer or peripheral devices.
- If possible, physically disconnect the computer from networks to which it is attached.
- Inform the Security Officer or other appropriate personnel as soon as possible.
- Write down any unusual behavior of the computer (screen messages, unexpected disk access, unusual responses to commands) and the time when they were first noticed.
- Write down any changes in hardware, software, or system use that preceded the malfunction.
- Do not attempt to remove a suspected virus yourself!

The Security Officer should monitor the resolution of the malfunction or incident, and report to the CST the result of the action with recommendations on action steps to avert future similar occurrences.

Report Security Incidents

It is the responsibility of each Practice employee or contractor to report perceived security incidents on a continuous basis to the appropriate Practice supervisor or security personnel. A user is any person authorized to access an information resource. Users are responsible for the day-to-day, hands-on security of that resource. Users are to formally report all suspected security incidents or violations of the security policy immediately to the Security Officer. Users should report any perceived security incident to either their immediate supervisor, their department head, or to any member of the Practice CST. Members of the CST are specified above in this document.

Reports of security incidents shall be escalated as quickly as possible. Each member of the Practice CST must inform the other members as soon as possible. Each incident will be analyzed to determine if changes to existing security controls are necessary. All reported incidents are logged and the remedial action indicated. It is the responsibility of the CST to provide training on any procedural changes that may be required as a result of the investigation of an incident.

Security breaches shall be promptly investigated. If criminal action is suspected, the Practice shall contact the appropriate law enforcement and investigative authorities immediately, which may include, but is not limited to, the police, FBI, state Attorney General, and/or U.S. Department of Health and Human Services.

Transfer of Sensitive/Confidential Information

When confidential or sensitive information from one individual is received by another individual while conducting official business, the receiving individual shall maintain the confidentiality of the information in accordance with the conditions imposed by the providing individual. All employees must recognize the confidential nature of data maintained by the Practice and hold all data in the strictest confidence. Any unauthorized release of data to which an employee may have access is a violation of Practice policy which will result in personnel action and may result in legal action.

Transferring Software and Files between Home and Work

Personal software shall not be used on Practice computers or networks. If a need for specific software exists, a request shall be submitted to a supervisor or department head. Users shall not use Practice purchased software on home or on non-Practice computers or equipment unless specifically authorized by Practice management.

Practice confidential information includes, but is not limited to, patient information, IT system and configuration information, financial information and human resource data. Confidential information shall not be placed on any computer that is not the property of the Practice without written consent of the respective supervisor or department head. It is crucial that all Practice information is protected; in order to do that effectively, systems storing, maintaining, receiving, or transmitting Practice information must be secured. In the event that a supervisor or department head receives a request to transfer Practice information to a non-Practice computer system, the supervisor or department head should notify the Security Officer or appropriate personnel of the intentions and need for such a transfer of information.

The Practice's network is maintained and secured using a wide range of security protections, including features such as virus protection, e-mail file restrictions, firewalls, anti-hacking hardware and software, intrusion prevention and detection, etc. Since the Practice does not control non-Practice personal computers, the Practice cannot be sure of the methods that may or may not be in place to protect Practice data, hence the need for this restriction.

Internet Considerations

Special precautions are required to block and track Internet (public) access to Practice information resources not intended for public access, and to protect confidential Practice information when transmitted over the Internet.

The following security and administration issues shall govern Internet usage.

Prior approval of the Security Officer or other appropriate personnel authorized by the Practice shall be obtained before:

- An Internet, or other external network connection, is established;
- Practice information (including notices, memoranda, documentation and software) is made available on any Internet-accessible computer (e.g., web or ftp server) or device;
- Users may not install or download any software (applications, screen savers, etc.). If users have a need for additional software, the user is to contact their supervisor;
- The use of Practice technology and information shall be consistent with the goals of the Practice.
- The use of Practice technology or information for personal profit or gain is strictly prohibited.
- Confidential or sensitive information - including credit card numbers, telephone calling card numbers, passwords, and other parameters that can be used to access goods or services - shall be encrypted before being transmitted through the Internet.
- PHI – Patient Protected Health Information must be encrypted before being transmitted through the Internet.
- The encryption software used, and the specific encryption keys (e.g., passwords, pass phrases), shall be escrowed with the Security Officer or appropriate personnel, to ensure they are safely maintained/stored. The use of encryption software and keys, which have not been escrowed as prescribed above, is prohibited, and may make the user subject to disciplinary action.

Use of Encryption for Files and E-mail

For specific procedures on the use of Encryption within the Practice, please see the Practice's Encryption policy (IS-5).

De-identification / Re-identification of Protected Health Information (PHI)

As directed by HIPAA, all personal identifying information must be removed from all data that falls within the definition of PHI before it is stored or exchanged, unless such PHI is encrypted using a Practice approved encryption solution.

De-identification is defined as the removal of any personally identifiable information (PII) using the Expert or Safe Harbor method specified by the U.S. Department of Health and Human Services (HHS) which may be used to uniquely identify an individual.

PII includes, but is not limited to:

- Names

- Addresses
- Geographic subdivisions smaller than a state
- All date elements dates directly related to the individual (birth, marriage, death, etc.)
- Telephone numbers
- Facsimile numbers
- Driver's license numbers
- Electronic mail addresses
- Social security numbers
- Medical record numbers
- Health plan beneficiary numbers
- Account numbers
- Certificate/License numbers
- Vehicle identifiers and serial numbers
- Device identifiers and serial numbers
- Web Universal Resource Locators (URLs)
- Internet Protocol (IP) address numbers
- Biometric identifiers
- Full face photographic images and any comparable images (identifying images of tattoos, injuries, etc.)

Re-identification of confidential information: A cross-reference code or other means of identification can be used to re-identify data as long as the code is not derived from or related to information about the individual and cannot be translated to identify the individual. In addition, the code is not disclosed for any other purpose nor is the mechanism for re-identification disclosed.

Radiology Consultants of Little Rock, P.A.	
Policy and Procedure	
Title: IDENTIFICATION and AUTHENTICATION	P&P #: IS-1.2
Approval Date: 5/1/2016	Review: Annual
Effective Date: 5/1/2016	Information Technology

Identification and Authentication

User Login IDs

Individual users shall have unique login IDs and passwords. An access control system shall identify each user and prevent unauthorized users from entering or using information resources. Security requirements for user identification include:

- Each user shall be assigned a unique identifier.
- Users shall be responsible for the use and misuse of their individual login ID.

All user login IDs shall be audited at least twice yearly and all inactive login IDs revoked. The Practice Human Resources Department shall notify the Security Officer or appropriate personnel upon the departure of all employees and contractors, at which time login IDs are revoked.

The login ID shall be locked or revoked after a maximum of three (3) unsuccessful login attempts which then require that the locked login ID's passwords to be reset by the appropriate system administrator.

Users who desire to obtain access to Practice systems, networks or workstations must have completed and signed a Network Access Request Form (Appendix A). This form must be signed by the supervisor or department head of each user requesting access.

Passwords

User Account Passwords

User IDs and passwords are required in order to gain access to all Practice networks, computer systems and workstations. All passwords are restricted by a corporate-wide password policy to be of a "strong" nature. This means that all passwords must conform to restrictions and limitations that are designed to make the password difficult to guess. Users are required to select a password in order to obtain access to any electronic information both at the server level and at the workstation level. When passwords are reset, the user will be automatically prompted to manually change that assigned password.

Password Length – Passwords are required to be a minimum of eight (8) characters.

Complexity Requirements – Passwords must contain a combination of upper and lower case alphabetic characters, numeric characters, and special characters.

Password Expiration – Passwords must be changed every ninety (90) days. Compromised passwords shall be changed immediately.

Password Reuse – The prior four (4) passwords cannot be reused.

Restrictions on Sharing Passwords – Passwords shall not be shared, written down on paper or stored within an unencrypted file or database on a workstation and must be kept confidential.

Restrictions on Recording Passwords – Passwords are masked or suppressed on all online screens, and are never printed or included in reports or logs. Any stored passwords must be stored in an encrypted format.

Unattended Computers – Unattended computers must be locked by the user when leaving the work area. This feature is discussed with all employees during regular security training. The Practice policy has been determined that all computers will have an automatic screen lock function set to automatically activate upon every thirty (30) minutes of inactivity. Employees are not allowed to take any action which would override this setting

Confidentiality Agreement

Users of Practice information resources shall sign, as a condition for employment, an appropriate workforce confidentiality agreement (Appendix B). This agreement shall include the following statement, or a paraphrase of it:

I understand that any unauthorized use or disclosure of information residing on any Practice information resource system may result in disciplinary action consistent with the policies and procedures of federal, state, and local agencies.

Temporary workers and third-party employees not already covered by a confidentiality agreement shall also sign such a document prior to accessing Practice information resources.

Confidentiality agreements shall be reviewed when there are changes to contracts or other terms of employment, particularly when contracts are ending or employees are leaving an organization.

Confidentiality shall be re-affirmed by users when necessitated by updates to applicable laws, regulations or Practice policies.

Access Control

Information resources are protected by the use of access control systems. Access control systems include both internal (i.e., passwords, encryption, access control lists, constrained user interfaces, etc.) and external (i.e., port protection devices, firewalls, host-based authentication, etc.).

Rules for access to resources (including internal and external telecommunications and networks) have been established by the information/application owner or manager responsible for the resources. Access is granted only by the completion of a Network Access Request Form (Appendix A). This form can only be initiated by the appropriate supervisor or department head, and must be signed by the user's supervision or department head and the Security Officer or appropriate personnel.

This guideline satisfies the "need to know" requirement of the HIPAA regulation, since the supervisor or department head is the person who most closely recognizes an employee's need to access data. Users may be added to the information system, network, EHR, PM or other systems **only** upon the signature of the Security Officer or appropriate personnel who is responsible for adding the employee to the network in a manner and fashion that ensures that the user is granted access to data only as specifically requested.

Online banner screens, if used, shall contain statements to the effect that unauthorized use of the system is prohibited and that violators will be subject to civil and/or criminal prosecution.

Identification and Authentication Requirements

The host security management program shall maintain current user application activity authorizations. Each initial request for a connection or a session is subject to the authorization process previously addressed.

User Login Entitlement Reviews

If a user (employee or contractor) changes positions within the Practice, the user's new supervisor or department head shall promptly notify the Information Technology (IT) Department of the change of roles by indicating on the Network Access Request Form (Appendix A) both the roles or access that need to be added and the roles or access that need to be removed so that the user has access to the minimum necessary data to effectively perform their new job functions. The effective date of the position change should also be noted on the form so that the IT Department can ensure that the user will have appropriate roles, access, and applications for their new responsibilities. For a limited training period, it may be necessary for the user who is changing positions to maintain their previous access as well as adding the roles and access necessary for their new responsibilities.

Periodically, the IT Manager shall facilitate entitlement reviews with supervisors and/or department heads to ensure that all users have the appropriate roles, access, and software necessary to perform their job functions effectively while being limited to the minimum amount of data necessary to perform their duties while adhering to HIPAA requirements and protecting patient data.

Termination of User Login Account

Upon termination of a user (employee or contractor), whether voluntary or involuntary, the user's supervisor or department head shall promptly notify the Security Officer by indicating "Remove Access" on the user's Network Access Request Form (Appendix A) and submitting the form to the Security Officer. If the user's termination is voluntary and user provides notice, the user's supervisor or department head shall promptly notify the Security Officer of the user's last scheduled work day so that their user account(s) can be configured to expire. The user's supervisor or department head shall be responsible for insuring that all keys, ID badges, and other access devices as well as all Practice equipment and property is returned to the Practice prior to the user leaving the Practice on their final day of employment or contract. Employee Termination Checklist (Appendix I)

Periodically, the Security Officer or his or her designee shall review a list of active user accounts for all Practice network and application access, including access to the clinical electronic health record (EHR) and the practice management (PM) system. If any of the users on the list are no longer employed by or under contract to the Practice, the Security Officer will remove access to all systems.

Radiology Consultants of Little Rock, P.A.	
Policy and Procedure	
Title: NETWORK CONNECTIVITY	P&P #: IS-1.3
Approval Date: 5/1/2016	Review: Annual
Effective Date: 5/1/2016	Information Technology

Network Connectivity

Dial-In Connections

Access to Practice information resources through modems or other dial-in devices or software, if available, shall be subject to authorization and authentication by an access control system. **Direct inward dialing without passing through the access control system is prohibited.**

Dial-up numbers shall be unlisted.

Systems that allow public access to host computers, including mission-critical servers, warrant additional security at the operating system and application levels. Such systems shall have the capability to monitor activity levels to ensure that public usage does not unacceptably degrade system responsiveness.

Dial-up access privileges are granted only upon the request of a supervisor or department head with the submission of the Network Access Form and the approval of the Security Officer or appropriate personnel.

Dial-Out Connections

The Practice provides a link to an Internet Service Provider (ISP). If a user has a specific need to link with an outside computer or network through a direct dial-up link, approval must be obtained from the Security Officer or appropriate personnel. The appropriate personnel will ensure adequate security measures are in place.

Telecommunication Equipment

Certain direct link connections may require a dedicated or leased phone line. These facilities are authorized only by the Security Officer or appropriate personnel and ordered by the appropriate personnel. Telecommunication equipment and services may include but are not limited to the following:

- phone lines
- fax lines
- calling cards
- phone head sets
- software (VOIP) phones installed on workstations
- conference calling contracts
- cell phones
- Blackberry type devices
- call routing software
- call reporting software
- phone system administration equipment
- Network lines
- long distance lines
- 800 lines

- local phone lines (POTS)
- T1/PRI circuits
- telephone equipment

Permanent Connections

The security of Practice systems can be jeopardized from third party locations if security practices and resources are inadequate. When there is a need to connect to a third party location, a risk analysis should be conducted. The risk analysis should consider the type of access required the value of the information, the security controls in use by the third party, and the implications for the security of Practice systems. The Security Officer or appropriate personnel should be involved in the request, design and approval process.

Emphasis on Security in Third Party Contracts

Access to Practice computer systems or networks should not be granted until a review of the following concerns have been made, and appropriate restrictions or covenants included in a statement of work (“SOW”) or contract with the party requesting such access.

- Applicable sections of the Practice Information Security Policy have been reviewed and considered.
- Policies and standards established in the Practice information security program are enforced.
- A risk assessment of the additional liabilities that will attach to each of the parties to the agreement.
- The right to audit contractual responsibilities should be included in the agreement or SOW.
- Arrangements for reporting and investigating security incidents must be included in the agreement in order to meet the covenants of the HIPAA Business Associate Agreement.
- A description of each service to be made available.
- Each service, access, account, and/or permission made available should only be the minimum necessary for the third party to perform their contractual obligations.
- A detailed list of users that have access to Practice computer and network systems must be maintained and auditable.
- If required under the contract, permission should be sought to screen authorized users.
- Dates and times when the service is available should be agreed upon in advance.
- Procedures regarding protection of information resources should be agreed upon in advance and a method of audit and enforcement implemented and approved by both parties.
- The right to monitor and revoke user activity should be included in each agreement.
- Language on restrictions on copying and disclosing information should be included in all agreements.
- Responsibilities regarding hardware and software installation and maintenance should be understood and agreement upon in advance.
- Measures to ensure the return or destruction of programs and information at the end of the contract should be written into the agreement.
- If physical protection measures are necessary because of contract stipulations, these should be included in the agreement.
- A formal method to grant and authorize users who will have access to the data collected under the agreement should be formally established before any users are granted access.
- Processes should be in place to ensure that security measures are followed by all parties to the agreement.
- Because regular security training is required under HIPAA regulations, a formal

procedure should be established to ensure that the training takes place, that there is a method to determine who must take the training, who will administer the training, and the process to determine the content of the training established.

- A detailed list of the security measures which will be undertaken by all parties to the agreement should be published in advance of the agreement.

Firewalls

Authority from the Security Officer or appropriate personnel must be received before any employee or contractor is granted access to a Practice router or firewall.

Radiology Consultants of Little Rock, P.A.	
Policy and Procedure	
Title: MALICIOUS CODE	P&P #: IS-1.4
Approval Date: 5/1/2016	Review: Annual
Effective Date: 5/1/2016	Information Technology

Malicious Code:

Anti-virus Software Installation

Anti-virus software is to be installed and configured on all Practice workstations, laptops and servers. Virus definitions are to be updated, at least, daily on Practice computer systems. The anti-virus solution must be configured to automatically scan any files downloaded from an external source (i.e., the Internet) as well as files accessed from other external sources (USB drives, cell phones, flash drives, etc.). Virus update engines and data files are to be monitored by appropriate administrative staff responsible for keeping all virus definitions up to date.

Configuration – The anti-virus software currently implemented by the Practice is Symantec Endpoint. Updates are received directly from Symantec which is scheduled daily.

Maintenance – Through an automated procedure, updates and virus patches may be pushed out to the individual workstations and servers on an as needed basis.

Monitoring/Reporting – A record of virus definitions for all workstations and servers on the Practice network may be maintained. Appropriate administrative staff is responsible for providing reports for auditing and emergency situations as requested by the Security Officer or appropriate personnel.

New Software Distribution

Only software approved by the Security Officer or appropriate personnel will be used on Practice computers and networks. A list of approved software is maintained in (Appendix C). All new software will be tested by appropriate personnel in order to ensure compatibility with currently installed software and network configurations. In addition, appropriate Practice personnel must scan all software for viruses before installation. This includes shrink-wrapped software procured directly from commercial sources as well as shareware and freeware obtained from electronic bulletin boards, the Internet, or on disks (magnetic disks or CD/DVD discs and custom-developed software).

Although shareware and freeware can often be useful sources of work-related programs, the use and/or acquisition of such software must be approved by the Security Officer or appropriate personnel. Because the software is often provided in an open distribution environment, special precautions must be taken before it is installed on Practice computers and networks. These precautions include determining that the software does not, because of faulty design, “misbehave” and interfere with or damage Practice hardware, software, or data, and that the software does not contain viruses, either originating within the software or acquired in the process of distribution.

All data and program files that have been electronically transmitted to a Practice computer or network from another location must be scanned for viruses immediately after being received. Contact the appropriate Practice personnel for instructions for scanning files for viruses.

Every diskette, CD-ROM, DVD, memory disk, thumb drive, USB device or any other removable external storage device or media is a potential source for a computer virus. Therefore, every removable external storage device, including electronic devices or media received from other practices as well as devices or media from patients, must be scanned for virus infection prior to using any such device or media with any Practice computer system.

Computers shall never be “booted” from a diskette, CD-ROM, DVD or USB device received from an outside source. Users shall always remove any diskette, CD-ROM, DVD or USB device from the computer when not in use. This is to ensure that the diskette, CD-ROM, DVD or USB device is not in the computer when the machine is powered on. A diskette, CD-ROM, DVD or USB device infected with a boot virus may infect a computer in that manner, even if the diskette, CD-ROM, DVD or USB device is not “bootable”.

Retention of Ownership

All software programs and documentation generated or provided by employees, consultants, or contractors for the benefit of the Practice are the property of the Practice unless covered by a contractual agreement. Employees developing programs or documentation must sign a statement acknowledging Practice ownership at the time of employment. Nothing contained herein applies to software purchased by Practice employees at their own expense.

Reporting suspicious activity and functionality

Suspicious software, software acting different than normal, instances where users are directed to different websites, and any unusual activities related to software and internet function should be reported to the Security Officer immediately.

Radiology Consultants of Little Rock, P.A.	
Policy and Procedure	
Title: ENCRYPTION	P&P #: IS-1.5
Approval Date: 5/1/2016	Review: Annual
Effective Date: 5/1/2016	Information Technology

Encryption

Definitions

- **Encryption:** The translation of data into a secret code, encryption is the most effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it. Unencrypted data is called plain text; encrypted data is referred to as cipher text.
- **Encryption Key:** An encryption key specifies the particular transformation of plain text into cipher text, or vice versa during decryption.
- **Confidential Data:** Confidential information may include, but is not limited to:
 - o any individuals' Protected Health Information (PHI);
 - o financial and operational information of the Practice; and
 - o any information regarding personnel of the Practice that is confidential in nature (e.g., compensation, benefits, disciplinary records, etc.).

Overview

Protected Health Information (PHI) and other confidential information is used, stored, maintained, received and transmitted on a number of electronic devices. It is the policy of this organization to use encryption solutions in order to maintain this data as securely as possible.

Purpose

To secure confidential information in the possession of this organization as required under applicable requirements, legal obligations and regulations, such as by PCI Data Security Standard Requirements 3 and 8.4, the HIPAA Security Rule §164.312(a)(2)(iv) and §164.312(e)(2)(ii) as well as any other applicable federal and state laws. Encrypted data cannot be viewed or otherwise discovered in the event of theft, loss or interception of data, thus protecting the confidential data from unauthorized access.

Scope

This policy covers all confidential data created, maintained, stored, received or transmitted on any electronic device or media of this organization.

Policy

All electronic devices or media that store, maintain, receive and/or transmit confidential data must use a Practice approved encryption method to secure the information stored, maintained, received or transmitted from that device or media.

Equipment Encryption (data at rest):

Full disk and/or boot disk encryption must be used for laptops and workstations that contain confidential data. Boot disk encryption will not allow access to the operating system thus rendering the device inoperable to an unauthorized user. Full disk encryption encrypts all data on

the device offering yet another layer of protection. Confidential data stored and/or maintained on servers must be saved using full disk encryption, an application (such as a database) that uses an approved encryption scheme, in an encrypted virtual drive or encrypted folder.

Transmitted Data (data in motion):

If, following a comprehensive risk analysis, it is determined that encryption is a reasonable and appropriate security control for electronically transmitting confidential data, such confidential data and files must be encrypted using a Practice approved encryption solution. When encrypted data is transferred between agencies, the agencies shall devise a mutually agreeable procedure for secure key management. In the case of conflict, the Practice shall establish the criteria in conjunction with the Security Officer or other appropriate personnel. Prior to transmitting any confidential data, the Security Officer must be contacted to ensure that the proper encryption technology is in place. Processes by which confidential data transmissions can be encrypted include the following methods:

- Encrypting files and folders using a variety of commercially available encryption products. Users sending and receiving these files would need to share private keys that are used to both encrypt and decrypt each transmission. These “keys” must be shared in a distinctly different communication from the encrypted data; preferably via phone.
- The transport layer can be encrypted, as implemented by the server (web browsing and file transfer are typically encrypted with SSL, TLS or secure FTP (sftp); network access typically with a VPN). All data sent over such connections would be encrypted.
- E-mail Encryption: Users desiring to exchange secure e-mail with an outside party may exchange public keys with the outside party. Once verified, a digital certificate can be installed on each end of the communication that will allow the transmission of secure e-mail.
- External Device Encryption (data at rest): Confidential data stored on portable devices such as USB drives, DVDs, CDs, external hard drives, and smart phones must be encrypted. Data on these devices will be considered secure as long as the encryption key is kept separate from the device.

Exceptions

- Point of care devices that record PHI in the process of use and that cannot use encryption because of technology limitations may be exempted from this policy. These devices must be covered under a risk assessment to ensure that risks are addressed via appropriate compensating controls to protect data.
- Additional information is available at:
 - HIPAA Security Rule:
<http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/securityrulepdf.pdf>
 - NIST Guide to Storage Encryption:
<http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/nist800111.pdf>

Radiology Consultants of Little Rock, P.A.	
Policy and Procedure	
Title: BUILDING SECURITY	P&P #: IS-1.6
Approval Date: 5/1/2016	Review: Annual
Effective Date: 5/1/2016	Information Technology

Building Security

It is the policy of the Practice to provide building access in a secure manner. Each site, as applicable, is somewhat unique in terms of building ownership, lease contracts, entranceway access, fire escape requirements, and server room control. However, the Practice strives to continuously upgrade and expand its security and to enhance protection of its assets and medical information that has been entrusted to it.

Physical and technical maintenance is documented (Appendix H) to track changes to the building and system that will affect access to patient information. Changes in access to patient information require a risk analysis and training to staff.

The following list identifies measures that are in effect at the Practice. All other facilities, as applicable, have similar security appropriate for that location.

Description of building: The Practice is housed in a multi-story brick building located at 9601 Baptist Health Drive, Suite 1100, in Little Rock, Arkansas. There is backup generator at both server locations.

- Entrance to the building during non-working hours is controlled by combination locks, swipe cards, and on-site security.
- Only specific Practice employees are given the keys for entrance. Sharing access to employee keys with non-employees is strictly prohibited.
- The keys are changed as needed and eligible employees are notified by company e-mail or voice mail. Keys are returned upon termination of employees that had access.
- The door leading from the reception area to office and exam areas is to be monitored or locked at all times and requires appropriate credentials or escort past the reception or waiting area door(s).
- Front desk personnel monitor the reception area and prevent unauthorized access to office and exam areas.
- Once a patient or visitor has checked in with the front desk personnel, and the front desk personnel have verified the appointment of the patient or visitor, the patient or visitor shall be escorted to the appropriate Practice exam or office area. Patients and visitors may be asked to show driver's license, business card, name tag or other form of identification prior to being given access to PHI.
- The reception area is to be staffed at all times during normal Practice business hours.
- Any unrecognized person in a restricted Practice location should be challenged as to their right to be there.
- All visitors must check in or sign in at the front desk, wear a visitor badge (if available, excluding patients), and be accompanied by a Practice staff member. In some situations, non-Practice personnel, who have signed the confidentiality agreement or that maintain a business associate agreement (BAA) with the Practice, may not need to be accompanied at all times.

Information Security Policy

- Fire Protection:
 1. Local building codes will be observed.
 2. Manufacturer's recommendations on the fire protection of individual hardware will be followed.
 3. Fire detection equipment is installed.
 4. Fire prevention equipment (sprinklers and/or fire extinguishers) are in use.

Radiology Consultants of Little Rock, P.A.	
Policy and Procedure	
Title: TELECOMMUTING	P&P #: IS-1.7
Approval Date: 5/1/2016	Review: Annual
Effective Date: 5/1/2016	Information Technology

Telecommuting/Remote Access

With the increased availability of broadband network access and secure VPNs, telecommuting has become more viable for many organizations. The Practice may consider telecommuting to be an acceptable work arrangement in certain circumstances. This policy is applicable to all employees and contractors who work either permanently or only occasionally outside of the Practice office environment. It applies to users who work from their home full time, to employees on temporary travel, to users who work from a remote office location, and to any user who connects to the Practice network and/or hosted EHR, if applicable, from a remote location.

While telecommuting can be an advantage for users and for the organization in general, it presents new risks in the areas of confidentiality and security of data. Workers linked to the Practice's network become an extension of the wide area network and present additional environments that must be protected against the danger of spreading Trojans, viruses, or other malware. This arrangement also exposes the corporate as well as patient data to risks not present in the traditional work environment.

General Requirements

Telecommuting workers are required to follow all Practice corporate, security, confidentiality, HR, and Code of Conduct policies that are applicable to all other employees and contractors.

- **Need to Know:** Telecommuting Users will have the access based on the same 'need to know' as they have when in the office.
- **Password Use:** The use of a strong, complex password, changed at least every 90 days, is even more critical in the telecommuting environment. Do not share your password or write it down where a family member or visitor can see it.
- **Training:** Personnel who telecommute must complete the same privacy and security training as all other employees.
- **Contract Specific:** There may be additional requirements specific to the individual contracts to which an employee or contractor may be assigned.

Required Equipment

Users approved for telecommuting must understand that the Practice will not provide all equipment necessary to ensure proper protection of information to which the user has access. The following lists define the equipment and environment required:

Practice Provided:

Computer that is exclusive to work use

Employee Provided:

Broadband connection and fees.

Paper shredder.

Secure office environment isolated from visitors and family.
A lockable file cabinet or safe to secure documents when away from the home office.

Hardware Security Protections

Virus Protection: Home users must never stop the update process for virus protection. Virus protection software is installed on all Practice computers and is set to update virus definitions on a, at least, daily basis. These updates are critical to the security of all data and must be allowed to complete.

VPN and Firewall Use: Established procedures must be rigidly followed when accessing Practice information of any type. The Practice requires the use of VPN software and a firewall device. Disabling a virus scanner or firewall is cause for termination.

Security Locks: Use security cable locks for laptops at all times, even if at home or at the office. Cable locks have been demonstrated as effective in thwarting robberies.

Lock Screens: No matter what location, always lock the screen before walking away from the workstation. The data on the screen may be protected by HIPAA or may contain confidential information. Workstations are programmed and set to automatically log off after thirty (30) minutes of inactivity.

Data Security Protection

Data Backup: Backup procedures have been established that encrypt the data being moved to an external media. Use only that procedure – do not create one on your own. If there is not a backup procedure established or if you have external media that is not encrypted, contact the Security Officer. Protect external media and devices by keeping it in your possession when traveling.

Transferring Data to the Practice: Transferring data to the Practice requires the use of an approved VPN connection to ensure the confidentiality and integrity of the data being transmitted. Do not circumvent established procedures, nor create your own method, when transferring data to the Practice.

External System Access: If you require access to an external system, contact your supervisor or department head. The Security Officer or appropriate personnel will assist in establishing a secure method of access to the external system.

E-mail: Do not send any protected health information (PHI) via e-mail unless it is encrypted. If you need assistance with this, contact the Security Officer or appropriate personnel to ensure an approved encryption solution is used for transmission.

Non-Practice Networks: Extreme care must be taken when connecting Practice equipment to a home or hotel network. Although the Practice actively monitors its security status and maintains organization wide protection policies to protect the data within all contracts, the Practice has no ability to monitor or control the security procedures on non-Practice networks.

Protect Data in Your Possession: View or access only the information that you have a need to see to complete your work assignment. Regularly review the data you have stored to ensure that the amount of patient level data is kept at a minimum and that old data is eliminated as soon as possible. Store electronic data only in encrypted work spaces. If your laptop has not been set up with an encrypted work space, contact the Security Officer or appropriate personnel for assistance. Protect external media by keeping it in your possession when traveling.

Hard Copy Reports or Work Papers: Never leave paper records around your work area. Lock all paper records in a file cabinet at night or when you leave your work area.

Data Entry When in a Public Location: Do not perform work tasks which require the use of sensitive corporate or patient level information when you are in a public area, i.e., airports, airplanes, hotel lobbies. Computer screens can easily be viewed from beside or behind you.

Sending Data Outside the Practice: All external transfer of data must be associated with an official contract, non-disclosure agreement, or appropriate Business Associate Agreement. Do not give or transfer any patient level information to anyone outside the Practice without the written approval of your supervisor or department head.

Disposal of Paper and/or External Media

Shredding: All paper which contains sensitive information that is no longer needed must be shredded by a cross-cut shredder before being disposed. Do not place in a trash container without first shredding. All employees working from home, or other non-Practice work environment, **MUST** have direct access to a cross-cut shredder.

Disposal of Electronic Media: All external media must be sanitized or destroyed in accordance with HIPAA compliant procedures.

- Do not throw any media containing confidential, sensitive, or protected information in the trash.
- Return all external media to your supervisor or department head.
- External media must be wiped clean of all data. The Security Officer or appropriate personnel have specific procedures for doing this – so all external media must be sent to them.
- The final step in this process is to forward the media for disposal by a certified destruction agency.

Radiology Consultants of Little Rock, P.A.	
Policy and Procedure	
Title: Removable Media	P&P #: IS-1.8A
Approval Date: 5/1/2016	Review: Annual
Effective Date: 5/1/2016	Information Technology

Removable Media

Definitions

Removable Media – Any portable electronic device or media used primarily to store information electronically. Examples of portable media may include, but are not limited to: CDs, DVDs, tapes, USB storage devices (thumb drives, removable hard drives, etc.), other removable storage/memory devices (Compact Flash cards, Secure Digital and MicroSD cards, Memory Sticks, etc.).

Confidential Information – Any individual’s Protected Health Information (PHI) as defined by HIPAA; financial, operating or other proprietary of the Practice; and other information of the Practice that is confidential in nature (i.e., employee compensation, benefit and disciplinary records).

Removable Media Usage Standards and Policy

The purpose of this policy is to guide employees/contractors of the Practice in the proper use of removable media when a legitimate business requirement exists to transfer data to and from Practice networks. Every workstation or server that has been used by either Practice employees or contractors is presumed to have confidential information stored on its hard drive. Therefore procedures must be carefully followed when copying data to or from removable media to protect confidential information. Because removable media, by its very design, is easily lost or stolen, care and protection of these devices must be addressed. Because it is likely that removable media will be provided to a Practice employee by an external source for the exchange of information, it is necessary that all employees receive guidance in the appropriate use and handling of removable media from external sources.

The use of removable media in various formats is common within the Practice. All users must be aware that confidential information could potentially be lost or compromised when moved outside of the Practice environment. Removable media received from an external source could potentially pose a threat to the Practice environment.

USB devices are convenient devices which allow the transfer of data in an easy to carry format. They provide a much improved format for data transfer when compared to other removable media formats, such as diskettes, CDs, or DVDs. The software drivers necessary to use a USB device are normally included on the USB device itself and install automatically when connected to computer equipment. They now come in a rugged titanium format which connects to any key ring. These factors make them easy to use and carry, but unfortunately also easy to be lost or stolen.

Rules governing the use of removable media within the Practice include:

- Confidential information is never to be stored on removable media unless the data is maintained in an approved encrypted format.
- All USB devices used to store Practice data or confidential information must use an encrypted USB device issued by the Security Officer or appropriate personnel.
- The use of personal USB or other removable media devices within the Practice is strictly prohibited.
- Non-Practice workstations and laptops may not have the same security protection standards required by the Practice, and accordingly malicious software could be transferred from a non-Practice device to the removable media and then back to a Practice workstation.

Example: Do not copy a work spreadsheet to your USB device and take it home to connect to your personal computer.

- Data may be exchanged between Practice workstations/networks and workstations used within the Practice. The very nature of data exchange requires that under certain situations data be exchanged in this manner.

Examples of necessary data exchange include:

Data provided to auditors via USB device for audit purposes.

- Only removable media issued by the Practice is permitted to be connected and used with Practice computers; except when said removable media is from an approved businesses or vendor listed on the Approved Contractors list (Appendix D).
- Before initial use and before any confidential information is transferred to removable media, the removable media must be sent to the Security Officer or other appropriate personnel to ensure appropriate and approved encryption is installed. Copy confidential information only to the encrypted location on the removable media. Non-confidential information may be transferred to unencrypted space on the removable media.
- All employees and contractors are required to report the loss of any removable media to their supervisor or department head immediately. It is important that the CST team is notified either directly from the employee or contractor or by the employee's or contractor's supervisor or department head immediately.
- When an employee or contractor leaves the Practice, all removable media in their possession must be returned to the Security Officer or other appropriate personnel for data sanitization conforming to HIPAA guidelines for the reuse or disposal of electronic media.

When no longer in productive use, all removable media must be wiped of data in a manner which conforms to HIPAA regulations. To ensure proper reuse and disposal procedures are followed, all removable media must be returned to the Security Officer or other appropriate personnel for data erasure when no longer in use. For more information on the proper disposal of electronic devices and media, please see the Practice's Disposal and Reuse of Electronic Media policy (IS-1.10).

Radiology Consultants of Little Rock, P.A.	
Policy and Procedure	
Title: Mobile Devices and Phones	P&P #: IS-1.8B
Approval Date: 5/1/2016	Review: Annual
Effective Date: 5/1/2016	Information Technology

Mobile Devices and Phones

Definitions

Mobile Devices – Any portable computer device capable of receiving, transmitting and/or storing or maintaining confidential information. Examples of mobile devices may include, but are not limited to: laptops, tablets, personal digital assistants (PDAs), etc.

Mobile Phones – Any portable phone device (smart or otherwise) that, in addition to having the capability to make and receive phone calls, is also capable of receiving, transmitting and/or storing and maintain confidential information. Examples of mobile phones may include, but are not limited to: cell phones, smartphones, tablets, etc.

Confidential Information – Any individual’s Protected Health Information (PHI) as defined by HIPAA; financial, operating or other proprietary of the Practice; and other information of the Practice that is confidential in nature (i.e., employee compensation, benefit and disciplinary records, etc.).

Mobile Device Usage Standards and Policy

This policy outlines the processes and procedures for acquiring wireless access privileges, using wireless networks, and ensuring the security of Practice mobile devices, Practice owned mobile phones and Practice wireless networks. If Practice offers general wireless access to patients and employees for their personal devices/phones, this must be separated from the Practice network. The use of personal mobile devices/phones for general purposes on the Practice network is strictly prohibited.

Generally, Practice owned mobile device/phones are the only devices permitted to connect to the Practice network. When Practice owned mobile devices/phones access public wireless services, care should be taken to limit functions to non-patient care while on the public wireless network. The use of personal mobile device/phones for conducting Practice business must be approved by the Security Officer.

Approval Procedure – If employees need access to Practice network and programs (Practice email, EHR etc.) on their personal devices/phones, they will be required to receive the approval of the Security Officer and sign the Personal Mobile Electronic Device Agreement (Appendix J). Once this form is completed the Practice can setup the personal mobile device.

General Requirements – All of the Practice’s standard computer equipment security requirements are in effect for mobile devices/phones as well. These requirements include, but are not limited to:

- Authentication using a unique user id and strong password
- Automatic screen lock
- Prohibition of installing unauthorized software

- Prohibition of modifying mobile device configuration settings

Other Requirements – The portable nature of mobile devices/phones requires procedures which may not be applicable for workstations or similar computer equipment. Your mobile device/phone training will include these mobile device/phone specific requirements. These requirements include, but are not limited to:

- Your duty to report a lost or stolen mobile device to the Practice Security Officer immediately.
- Receiving approval from your supervisor or department head prior to working on your mobile device/phone after hours or after the number of hours for an applicable work period has been reached.
- Receiving approval from your supervisor or department head prior to removing a Practice mobile device from the Practice.
 - If you have received approval to travel with a Practice mobile device, the device must be:
 - Powered off while not in use
 - Kept in a secure location while not in use
 - Never left unattended
- Unless specifically authorized by Practice management, recording any video, still pictures or audio with a mobile device is strictly prohibited.
- Your mobile phone must be kept in a secure location when not in use and never left unattended.

Software Requirements –

MOBILE DEVICES: The following is a list of the minimum software requirements for any Microsoft Windows based mobile device used within the Practice:

- Microsoft: Windows 7 Service Pack 1 with Internet Explorer 10.0
- Apple: MacOS X 10.7 (Lion)
- Practice approved anti-virus/anti-malware software
- Practice approved encryption solution
- Practice approved secure VPN client (if applicable)

MOBILE PHONES: The following is a list of minimum operating system versions for various mobile phones required for conducting Practice business on mobile phones:

- Android: Jelly Bean 4.1 or above
- iPhone: iOS 6.0.1 or above
- BlackBerry: BlackBerry OS 7.0 or above
- Microsoft: Windows Phone 7.8 or above

If employee's mobile device/phone does not have all of these software components, please notify the Security Officer so these components can be installed and configured.

Training Requirements – Once employees have approval for wireless access on personal mobile devices or the use of your personal mobile phone, they will be required to read and sign the Personal Mobile Electronic Device Agreement (Appendix J). This form provides training for employees and covers the basics of connecting to wireless networks, security standards and applications to install, securing mobile devices, transmission of confidential Practice information

This document has been customized for the HealthIT member for whom it has been provided. For security purposes and to ensure that each HealthIT member is receiving the appropriate documents, retransmitting, modifying, sharing or disseminating without express consent of HealthIT is strictly prohibited.

and other requirements. This training will be conducted within a reasonable period of time once wireless access has been approved, and in most cases will include several individuals at once.

End of Use – When no longer in productive use, all mobile devices/phones must be wiped of data in a manner which conforms to HIPAA regulations. To ensure proper reuse and disposal procedures are followed, all mobile devices/phones must be returned to the Security Officer or other appropriate personnel for data erasure when no longer in use.

Employee/Contractor Termination – When an employee or contractor leaves the Practice, any mobile devices/phones in their possession must be returned to the Security Officer or other appropriate personnel by the employee's or contractor's supervisor or department head for data sanitization conforming to HIPAA guidelines for the reuse or disposal of electronic equipment. Employee Termination Checklist (Appendix I).

Radiology Consultants of Little Rock, P.A.	
Policy and Procedure	
Title: RETENTION / DESTRUCTION of PRACTICE DOCUMENTS	P&P #: IS-1.9
Approval Date: 5/1/2016	Review: Annual
Effective Date: 5/1/2016	Information Technology

Retention / Destruction of Practice Information

Many state and federal laws regulate the retention and destruction of medical information. The Practice actively conforms to these laws and follows the strictest regulation if/when a conflict occurs. Guidelines for retention related to medical information can be found in the Rules and Regulations for Hospitals and Related Institutions in Arkansas

HIPAA Record Retention – Documents relating to uses and disclosures, authorization forms, business partner contracts, notices of information practice, responses to a patient who wants to amend or correct their information, the patient's statement of disagreement, a complaint record, Security policies and procedures and any other required HIPAA records and documentation shall be retained for a period of six (6) years.

Medical Record Retention – Patient medical records shall be retained pursuant to the state statute governing medical record retention requirements. Medical Records are retained for a period of ten (10) years. In the event that a HIPAA record becomes part of a patient’s medical record, those HIPAA records shall be retained pursuant to this Medical Record Retention policy.

Record Destruction – All hardcopy medical records that require destruction are shredded pursuant NIST SP 800-88 guidelines.

Radiology Consultants of Little Rock, P.A.		Policy and Procedure
Title: DISPOSAL AND REUSE OF ELECTRONIC MEDIA	P&P #: IS-1.10	
Approval Date: 5/1/2016	Review: Annual	
Effective Date: 5/1/2016	Information Technology	

Disposal and Reuse of Electronic Media

Overview

A tremendous amount of information is created, stored, maintained, received and transmitted using electronic devices and media in every type of business and organization. This information includes personal data, financial data and, in the case of a medical organization, Protected Health Information (PHI). It must be assumed that any electronic device or media of the Practice contains PHI or other confidential information. Therefore, before reusing, retiring or disposing of computers, disks, copier systems, flash drives, compact flash and similar memory card devices, external USB storage devices, backup tapes and cartridges, smart phones, point of care devices, or any other type of electronic media or device which may contain electronic media, it must be properly sanitized.

Purpose

To ensure that all data is protected from unauthorized access and to comply with the Health Insurance Portability and Accountability Act (HIPAA) and any other applicable federal and state laws that may be applicable as well as internal information security policies.

Scope

This policy covers all electronic media and all personnel who use or are responsible for equipment and systems that could contain PHI. This includes all vendors and/or contractors who have access to the equipment, electronic media and/or computer systems.

Policy

General

- 1) All media that stores or maintains PHI shall be accountable via control logs showing what it is, where it is located, what its intended use is and what individual is responsible for that media. Device Inventory for Electronic Devices (Appendix E).
- 2) All media that stores PHI shall have procedures in place for its proper use, storage and disposal.
- 3) Prior to working on equipment that is to be either reused or disposed of the device will be reviewed for PHI that may need to be backed up and create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment.
- 4) PHI that is no longer needed or that is on equipment that is to be either reused or disposed of shall be removed in a manner so as to permanently, completely, and irreversibly delete said PHI so as to prevent future access or use by unauthorized individuals.
- 5) It is the responsibility of each employee to identify electronic media for which he or she is responsible for and to follow this policy to ensure the secure disposal of said media.
- 6) When no longer needed, all media must be returned to the Security Officer or other appropriate personnel for proper disposal.

- 7) The Security Officer or other appropriate personnel will store media in a secure area until such time that the media can undergo proper disposal pursuant to NIST SP 800-88 guidelines.

Methods for media purge and destruction

- 1) Overwriting via approved sanitization software that uses at a minimum three passes of systematic overwriting.
- 2) Destruction of the media. Physically destroying the media so that it cannot be used or read in any manner. Disintegration, incineration, pulverizing and/or melting are some methods of physical destruction.
- 3) Other methods as defined within NIST SP 800-88 Media Sanitization guidelines.
- 4) Clearing the data. Reformatting or deleting information is *NOT* an acceptable means of sanitizing media.

Disposal

- 1) Prior to disposal all media should be sanitized. In the event that the media will not accept sanitization the media should be physically destroyed in a manner that renders it totally useless.
- 2) Media must *NEVER* be thrown into the trash as a method of sanitization/destruction for disposal.
- 3) Following proper sanitization and/or destruction, media can be disposed of in the manner consistent with local waste disposal requirements.
- 4) Records must be maintained that identify the destruction and disposal method, date of destruction and disposal, the party responsible for destruction and disposal, and identification (e.g., serial number) of the media.

Reuse

- 1) Upon proper purging of media by the Security Officer or other appropriate personnel, media or devices containing may be reused for various purposes which may include, but are not limited to:
 - a. spare parts,
 - b. emergency equipment replacements,
 - c. use in a testing environment,
 - d. as a backup for another system, or
 - e. as an additional temporary or permanent resource for personnel requiring more than one system or device.

Additional information is available at:

HIPAA Security Rule

<http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/securityrulepdf.pdf>

NIST Special Publication 800-88 Guidelines for Media Sanitization

http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_with-errata.pdf

US Department of Health and Human Services (HHS)

http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/guidance_breachnotice.html

Radiology Consultants of Little Rock, P.A.	
Policy and Procedure	
Title: CHANGE MANAGEMENT	P&P #: IS-1.11
Approval Date: 5/1/2016	Review: Annual
Effective Date: 5/1/2016	Information Technology

Change Management

Statement of Policy

To ensure that Practice is tracking changes to networks, systems, and workstations including software releases and software vulnerability patching in information systems that contains electronic protected health information (ePHI). Change tracking allows the Information Technology (IT) Department to efficiently troubleshoot issues that arise due to an update, new implementation, reconfiguration, or other change to the system.

Procedure

1. The IT staff or other designated Practice employee who is updating, implementing, reconfiguring, or otherwise changing the system shall carefully log all changes made to the system, except when such changes are already tracked within a system (i.e., Windows or EHR or other system updates performed and logged automatically or by a vendor). Change management tracking log (Appendix H) is available for tracking changes that effect the protection of patient information.
2. Physical and technical maintenance is documented to track changes to the building and system that will affect access to patient information. Changes in access to patient information require a risk analysis and training to staff.
3. The employee implementing the change will ensure that all necessary data backups are performed prior to the change.
4. The employee implementing the change shall also be familiar with the rollback process in the event that the change causes an adverse effect within the system and needs to be removed.

Radiology Consultants of Little Rock, P.A.	
Policy and Procedure	
Title: AUDIT CONTROLS	P&P #: IS-1.12
Approval Date: 5/1/2016	Review: Annual
Effective Date: 5/1/2016	Information Technology

Audit Controls

Statement of Policy

To ensure that the Practice implements hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain electronic protected health information (ePHI). Audit Controls are technical mechanisms that track and record computer activities. An audit trail determines if a security violation occurred by providing a chronological series of logged computer events that relate to an operating system, an application, or user activities.

The Practice is committed to routinely auditing users' activities in order to continually assess potential risks and vulnerabilities to ePHI in its possession. As such, the Practice will continually assess potential risks and vulnerabilities to ePHI in its possession and develop, implement, and maintain appropriate administrative, physical, and technical security measures in accordance with the HIPAA Security Rule.

Procedure

1. See policy entitled Information System Activity Review (IS 1.13) for the administrative safeguards for auditing information system activities.
2. The Security Officer shall ensure that auditing is enabled on all software that process, transmit, receive, maintain and/or store ePHI for purposes of generating audit logs. Each audit log shall include, at a minimum: user ID, login time and date, and scope of patient data being accessed for each attempted access. Audit trails shall be stored in a secure area to minimize access to audit trails.
3. The Practice shall utilize appropriate network-based and host-based intrusion detection systems. The Information Technology manager shall be responsible for installing, maintaining, and updating such systems.

Radiology Consultants of Little Rock, P.A.	
Policy and Procedure	
Title: INFORMATION SYSTEM ACTIVITY REVIEW	P&P #: IS-1.13
Approval Date: 5/1/2016	Review: Annual
Effective Date: 5/1/2016	Information Technology

Information System Activity Review

Statement of Policy

To establish the process for conducting, on a regular basis, an operational review of system activity including, but not limited to, user accounts, system access, file access, security incidents, audit logs, and access reports. The Practice shall conduct on a regular basis an internal review of records of system activity to minimize security violations.

Procedure

1. Information Technology personnel or Practice Security Officer shall be responsible for conducting reviews of the Practice’s information systems’ activities. Such person(s) shall have the appropriate technical skills with respect to the operating system and applications to access, review, and interpret audit logs and related information appropriately.
2. The Security Officer shall develop a report format to capture the review findings. Such report shall include the reviewer’s name, date and time of performance, and significant findings describing events requiring additional action (e.g., additional investigation, employee training and/or discipline, program adjustments, modifications to safeguards, etc.).
3. Such reviews shall be conducted in a timely manner or immediately if the Practice has reason to suspect wrongdoing. In conducting these reviews, Information Technology personnel shall examine audit logs for security-significant events including, but not limited to, the following:
 - a. Logins – Review successful and unsuccessful login attempts. Identify multiple failed login attempts, account lockouts, and unauthorized access.
 - b. File accesses – Scan successful and unsuccessful file access attempts. Identify multiple failed access attempts, unauthorized access, and unauthorized file creation, modification, or deletion.
 - c. Security incidents – Examine records from security devices or system audit logs for events that constitute system compromises, unsuccessful compromise attempts, malicious program code (e.g., viruses, worms, etc.), denial of service, or scanning/probing incidents.
 - d. User Accounts – Review of user accounts within all systems to ensure users that no longer have a business need for information systems no longer have such access to the information and/or system.

All significant findings shall be recorded using the report format referred to in Section 2 of this policy.

4. Information Technology personnel shall forward all completed reports, as well as recommended actions to be taken in response to findings, to the Security Officer for review. The Security Officer shall be responsible for maintaining such reports and share with the Confidentiality and Security Team. The Security Officer shall consider such reports and recommendations in determining whether to modify the Practice's administrative, physical, and/or technical safeguards. In the event a security incident is detected through such auditing, such matter shall be addressed pursuant to the policy included in the Reporting and Managing a Breach Procedure (IS-6.0) policy.

Radiology Consultants of Little Rock, P.A.	
Policy and Procedure	
Title: DATA INTEGRITY	P&P #: IS-1.14
Approval Date: 5/1/2016	Review: Annual
Effective Date: 5/1/2016	Information Technology

Data Integrity

Statement of Policy

The Practice shall implement and maintain appropriate mechanisms to corroborate that ePHI has not been altered or destroyed in an unauthorized manner.

The purpose of this policy is to protect Practice’s ePHI from improper alteration or destruction.

Procedure

1. To the fullest extent possible, the Practice shall utilize applications with built-in intelligence that automatically checks for human errors.
2. The Practice shall acquire network-based and/or host-based intrusion detection systems appropriate to the size, complexity and capabilities of the Practice. The Security Officer shall be responsible for installing, maintaining, and updating such systems.
3. To prevent transmission errors as data passes from one device to another, the Practice will use encryption, as determined to be appropriate, to preserve the integrity of data.
4. The Practice will check for possible duplication of data in its network to prevent poor data integration between different computer systems.
5. To prevent programming or software bugs, the Practice will test its information systems for accuracy and functionality before it starts to use them. The Practice will update its systems when IT vendors release fixes to address known bugs or problems.
6. The Practice will install and regularly update anti-virus software on all equipment to detect and prevent malicious code from altering or destroying data.
7. To prevent exposing magnetic media to a strong magnetic field, workforce members shall keep magnetic media away from strong magnetic fields and heat. For example, mobile devices should not be left in automobiles during the summer months.

Radiology Consultants of Little Rock, P.A.	
Policy and Procedure	
Title: CONTINGENCY PLAN	P&P #: IS-1.15
Approval Date: 5/1/2016	Review: Annual
Effective Date: 5/1/2016	Information Technology

Contingency Plan

Statement of Policy

To establish and implement policies and procedures for responding to an emergency or other occurrence (e.g., fire, vandalism, system failure, natural disaster) that damages systems that contain ePHI.

The Practice is committed to maintaining formal practices for responding to an emergency or other occurrence that damages systems containing ePHI. The Practice shall continually assess potential risks and vulnerabilities to protect health information in its possession, and develop, implement, and maintain appropriate administrative, physical, and technical security measures in accordance with the HIPAA Security Rule.

Procedure

1. Data Backup Plan

- a. The Practice, under the direction of the Security Officer, shall implement a data backup plan to create and maintain retrievable exact copies of ePHI.
- b. Tape back up
The Practice Security Officer or delegate backs up data from the practice management lab, pharmacy, and electronic health record systems on a daily basis and stores the data in secure off-site and on-site locations. The Practice also maintains secure off-site daily, weekly, monthly, and quarterly backups of electronic protected health information on its patients. Tapes are encrypted and taken off site each night by Practice Security Officer or delegate. During transit, tapes are protected at all times and are stored in a secure container at destination.
- c. Remote backup
The Practice Security Officer or delegate coordinates back up of data from the practice management lab, pharmacy, and electronic health record systems on a daily basis with the remote host.
- d. Backup media that is no longer in service will be disposed of in accordance with the Disposal and Reuse of Electronic Media policy (IS 1.10).
- e. The Security Officer shall monitor storage and removal of backups and ensure all applicable access controls are enforced.

- f. The Practice continuously monitors backup system performance and tests its backup systems on an annual basis to determine that the integrity of the stored electronic protected health information is safeguarded and exact copies of ePHI can be retrieved and made available. Such testing shall be documented by the Security Officer. To the extent such testing indicates need for improvement in backup procedures; the Security Officer shall identify and implement such improvements in a timely manner.

2. Disaster Recovery and Emergency Operations Plan

- a. The Security Officer shall be responsible for developing and regularly updating the written disaster recovery and emergency mode operations plan for the purpose of:
 - i. Restoring or recovering any loss of ePHI and/or systems necessary to make ePHI available in a timely manner caused by fire, vandalism, terrorism, system failure, or other emergency; and
 - ii. Continuing operations during such time information systems are unavailable. Such written plan shall have a sufficient level of detail and explanation that a person unfamiliar with the system can implement the plan in the event of an emergency or disaster situation. Copies of the plan shall be maintained on-site and at the off-site locations at which backups are stored or other secure off-site locations as needed.
- b. The disaster recovery and emergency operations plans shall include the following:
 - i. Current copies of the Practice's information systems inventory and network configuration documentation. Appendix E Device Inventory
 - ii. Current copies of the written backup and restore procedures developed and updated pursuant to this policy and will identify the order in which data is to be restored based on the Practice's criticality analysis. Appendix C Approved Software
 - iii. An inventory of hard copy forms and documents needed to record clinical, registration, and financial interactions with patients.
 - iv. Identification of an emergency response team. A list of all staff their title, phone and physical home address will be maintained by the Office Manager. Members of such team shall be responsible for the following:
 - 1. Contacting appropriate emergency personnel.
 - 2. Determining the impact of a disaster and/or system unavailability on the Practice's operations.

3. In the event of a disaster, securing the site and providing ongoing physical security.
 4. Retrieving lost data.
 5. Identifying and implementing appropriate workarounds during such time information systems are unavailable.
 6. Taking such steps as necessary to restore Practice operations including contact vendors to assist with restoring network functions. Appendix D Approved Contractors.
- v. Procedures for responding to a loss of electronic data including, but not limited to, retrieval and loading of backup data or methods for recreating data should backup data be unavailable.
- vi. Telephone numbers and/or e-mail addresses for all persons to be contacted in the event of a disaster or emergency situation, including the following:
1. Members of the immediate response team,
 2. Facilities at which backup data is stored,
 3. Information systems vendors and contractors, and (Appendix D)
 4. All current workforce members.
- c. The disaster recovery team shall meet on an at least an annual basis to:
- i. Review the effectiveness of the plan in responding to any disaster or emergency situation experienced by the Practice;
 - ii. In the absence of any such disaster or emergency, plan drills to test the effectiveness of the plan and document and evaluate the results of such drills; and
 - iii. Review the disaster recovery and emergency operations plans and make appropriate changes to the plans. The Security Officer shall be responsible for convening and maintaining minutes of such meetings. The Security Officer shall also be responsible for revising the plans based on the recommendations of the disaster recovery team.

Radiology Consultants of Little Rock, P.A.	
Policy and Procedure	
Title: SECURITY AWARENESS AND TRAINING	P&P #: IS-1.16
Approval Date: 5/1/2016	Review: Annual
Effective Date: 5/1/2016	Information Technology

Security Awareness and Training

Statement of Policy

To establish a security awareness and training program for all members of the Practice’s workforce, including management.

All workforce members shall receive appropriate training concerning the Practice’s privacy and security policies and procedures. Such training shall be provided to all new employees as part of the new employee orientation process and repeated annually for all employees.

Procedure

- a. Security Training Program
 - i. The Security Officer shall have responsibility for the development and delivery of initial security training. All workforce members shall receive such training addressing the requirements of the HIPAA Security Rule including the updates to HIPAA regulations found in the Health Information Technology for Economic and Clinical Health (HITECH) Act, Omnibus Rule and any subsequent updates to the HIPAA Security Rule. Security training shall be provided to all new workforce members as part of the orientation process. Attendance and/or participation in such training shall be mandatory for all workforce members. The Security Officer shall be responsible for maintaining appropriate documentation of all training activities.
 - ii. The Security Officer shall have responsibility for the development and delivery of ongoing security training provided to workforce members in response to environmental and operational changes impacting the security of ePHI, e.g., the addition of new hardware or software, new and increased threats, etc.
- b. Security Reminders
 - i. The Security Officer shall generate and distribute to all workforce members routine security reminders on a regular basis. Periodic reminders shall address password security, malicious software, incident identification and response, and access control. The Security Officer may provide such reminders through formal training, e-mail messages, and discussions during staff meetings, screen savers, log-in banners, newsletter/intranet articles, posters, and other effective means. The Security Officer shall be responsible for maintaining appropriate documentation of all periodic security reminders.

- ii. The Security Officer shall generate and distribute special notices to all workforce members providing urgent updates, such as new threats, hazards, vulnerabilities, and/or countermeasures.
- c. Protection from Malicious Software
- i. As part of the aforementioned Security Training Program and Security Reminders, the Security Officer shall provide training concerning the prevention, detection, containment, and eradication of malicious software. Such training shall include the following:
 - a) Guidance on opening suspicious e-mail attachments, e-mail from unfamiliar senders, and hoax e-mail,
 - b) The importance of updating anti-virus software and how to check a workstation or other device to determine if virus protection is current,
 - c) Instructions to never download files from unknown or suspicious sources,
 - d) Recognizing signs of a potential virus that could sneak past anti-virus software or could arrive prior to an update to anti-virus software,
 - e) The importance of backing up critical data on a regular basis and storing the data in a safe place,
 - f) Damage caused by viruses and worms, and
 - g) What to do if a virus or worm is detected.
- d. Password Management
- i. As part of the aforementioned Security Training Program and Security Reminders, the Security Officer shall provide training concerning password management. Such training shall address the importance of confidential passwords in maintaining computer security, as well as the following requirements relating to passwords:
 - a) Practice requirements for passwords including change frequency, reuse, length, etc.
 - b) Commonly used words, names, initials, birthdays, or phone numbers should not be used as passwords.
 - c) A password must be promptly changed if it is suspected of being disclosed, or known to have been disclosed.
 - d) Passwords must not be disclosed to other workforce members (including anyone claiming to need a password to “fix” a computer or handle an emergency situation) or individuals, including family members.

Information Security Policy

- e) Passwords must not be written down, posted, or exposed in an unsecure manner such as on a notepad or posted on a workstation.
- f) Employees should refuse all offers by software and/or Internet sites to automatically login the next time that they access those resources.
- g) Any employee who is directed by the Security Officer to change his/her password to conform to the aforementioned standards shall do so immediately.

Radiology Consultants of Little Rock, P.A.	
Policy and Procedure	
Title: SECURITY MANAGEMENT PROCESS	P&P #: IS-1.17
Approval Date: 5/1/2016	Review: Annual
Effective Date: 5/1/2016	Information Technology

Security Management Process

Statement of Policy

To ensure Practice conducts an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI held by the Practice.

The Practice shall conduct an accurate and thorough risk analysis and risk management process to serve as the basis for the Practice’s HIPAA Security Rule compliance efforts. The Practice shall re-assess the security risks to its ePHI and evaluate the effectiveness of its security measures and safeguards as necessary in light of changes to its environment, operations, business practices and technological advancements. Risk analysis and risk management is separate from the annual Security Risk Analysis conducted for Meaningful Use attestation.

Procedure

- a. The Security Officer shall be responsible for coordinating the Practice’s risk analysis. The Security Officer shall identify appropriate persons within the organization to assist with the risk analysis.
- b. The risk analysis shall proceed in the following manner:
 - i. Document the Practice’s current information systems.
 - a) Update/develop information systems inventory. List the following information for all hardware (i.e., network devices, workstations, printers, scanners, mobile devices) and software (i.e., operating system, various applications, interfaces): date acquired, location, vendors, licenses, owner, maintenance schedule, and function. Device Inventory (Appendix E)
 - b) Update/develop facility security requirements including, physical security, fire and burglary alarm equipment, and storage for hazardous materials. See Building Security policy IS-1.6.
 - c) For each application identified, identify each licensee (i.e., authorized user) by job title and describe the manner in which authorization is granted. Network Access Request Form (Appendix A)
 - d) For each of these applications: Approved Software (Appendix C)
 - i) Describe the data associated with that application.

- ii) Determine whether the data is created by the organization or received from a third party. If data is received from a third party, identify that party and the purpose and manner of receipt.
 - iii) Determine whether the data is maintained within the organization only or transmitted to third parties. If data is transmitted to a third party, identify that party and the purpose and manner of transmission.
 - iv) Define the criticality of the application and related data as high, medium, or low. Criticality is the degree of impact on the organization if the application and/or related data were unavailable for a period of time.
 - v) Define the sensitivity of the data as high, medium, or low. Sensitivity is the nature of the data and the harm that could result from a breach of confidentiality or security incident.
 - vi) For each application identified, identify the various security controls currently in place and locate any written policies and procedures relating to such controls.
- e) Identify and document threats to the confidentiality, integrity, and availability (referred to as “threat agents”) of ePHI created, received, maintained, or transmitted by Practice. Consider the following:
- i) Natural threats, e.g., earthquakes, floods, storm damage.
 - ii) Environmental threats, e.g., fire and smoke damage, power outage, utility problems.
 - iii) Human threats
 - a. Accidental acts, e.g., input errors and omissions, faulty application programming or processing procedures, failure to update/upgrade software/security devices, lack of adequate financial and human resources to support necessary security controls
 - b. Inappropriate activities, e.g., inappropriate conduct, abuse of privileges or rights, workplace violence, waste of corporate assets, harassment
 - c. Illegal operations and intentional attacks, e.g., eavesdropping, snooping, fraud, theft, vandalism, sabotage, blackmail
 - d. External attacks, e.g., malicious cracking, scanning, demon dialing, virus and malware introduction
 - iv) Identify and document vulnerabilities in the Practice’s information systems. A vulnerability is a flaw or weakness in security policies and procedures, design, implementation, or controls that could be accidentally triggered or intentionally exploited, resulting in

unauthorized access to ePHI, modification of ePHI, denial of service, or repudiation (i.e., the inability to identify the source and hold someone accountable for an action). To accomplish this task, conduct a self-analysis utilizing the standards and implementation specifications to identify vulnerabilities.

- f) Determine and document the probability and criticality of identified risks.
 - i) Assign probability level, i.e., the likelihood of a security incident involving an identified risk.
 - a. "Very Likely" (3) is defined as having a probable chance of occurrence.
 - b. "Likely" (2) is defined as having a significant chance of occurrence.
 - c. "Not Likely" (1) is defined as a modest or insignificant chance of occurrence.
 - ii) Assign criticality level. Potential impact or severity.
 - a. "High" (3) is defined as having a catastrophic impact on the Practice including a significant number of medical records which may have been lost or compromised.
 - b. "Medium" (2) is defined as having a significant impact including a moderate number of medical records within the practice which may have been lost or compromised.
 - c. "Low" (1) is defined as a modest or insignificant impact including the loss or compromise of some medical records.
 - iii) Determine risk score for each identified risk. Multiply the probability score and criticality score. Those risks with a higher risk score require more immediate attention.
- g) Identify and document appropriate security measures and safeguards to address key vulnerabilities. To accomplish this task, review the vulnerabilities you have identified in relation to the standards and implementation specifications. Focus on those vulnerabilities with high risk scores, as well as specific security measures and safeguards required by the Security Rule.
- h) Develop and document an implementation strategy for critical security measures and safeguards.
 - i) Determine a timeline for implementation.
 - ii) Determine the costs of such measures and safeguards and secure funding.

- iii) Assign responsibility for implementing specific measures and safeguards to appropriate person(s).
 - iv) Make necessary adjustments based on implementation experiences.
 - v) Document actual completion dates.
 - i. Evaluate the effectiveness of measures and safeguards following the implementation and make appropriate adjustments.
- c. The Security Officer shall be responsible for identifying appropriate times to reassess risk analysis. The Security Officer shall identify appropriate persons within the organization to assist with such evaluations. Evaluations shall be conducted upon the occurrence of one or more of the following events: changes in the HIPAA Security Rule regulations; new federal, state, or local laws or regulations affecting the security of ePHI; changes in technology, environmental processes, or business processes that may affect HIPAA Security policies or procedures; or the occurrence of a serious security incident. Follow-up evaluations could include the following:
 - i. Inspections, reviews, interviews, and analysis to assess adequacy of administrative and physical safeguards. Such evaluation shall include interviews to assess employee compliance; after-hours walk-through inspections to assess physical security, password protection (i.e., passwords not posted), and workstation sessions terminated (i.e., employees logged out); review of the latest security policies and procedures for correctness and completeness; and inspection and analysis of training, incident, and other relevant logs for compliance.
 - ii. Analysis to assess the adequacy of controls within the network, operating systems and applications. As necessary, the Practice shall engage outside resources to assist in the evaluation of existing administrative, physical and technical controls and make recommendations for improvements.

Radiology Consultants of Little Rock, P.A.	
Policy and Procedure	
Title: Emergency Operations Procedures (EHR outage)	P&P #: IS-2.0
Approval Date: 5/1/2016	Review: Annual
Effective Date: 5/1/2016	Information Technology

Emergency Operations Procedures

Purpose

To provide procedures for managing and documenting patient encounters when Electronic Health Record (EHR) and Practice Management (PM) systems are unavailable due to planned or unexpected outages.

Definitions

Electronic Health Record (EHR) – Electronic records of patient encounters in a healthcare delivery setting. An electronic health record typically consists of information including: patient demographics, progress notes, medication history, vital signs and laboratory results.

Practice Management (PM) – A practice Management System is usually a computer based system used to manage the day-to-day operations of a healthcare practice. Tasks typically performed by a PM system include: scheduling appointments, maintaining patient and insurance information, billing functions and generating various reports.

Procedures

Notification:

The Information Systems or Technology Manager shall notify Practice management as soon as practicable in the event of:

- planned downtime of practice IT resources,
- unexpected IT system disruptions or outages, and
- resumption of IT services following a disruption or outage such that normal operations may resume.

Scheduling:

If the EHR or other critical system is not operational or is otherwise unavailable, the schedule printed the previous day is retrieved. The Practice manager is tasked with maintaining a copy of this schedule or assigning this duty as appropriate. If phones are not operational, patient appointments may not be made. The operator should ask for pertinent contact information and record a message using the paper telephone encounter form.

Patient Encounters:

- Telephone encounters should be entered onto the paper telephone encounter form and transferred to a nurse for triage.
- Utilize system for use of temporary charts.

- Paper encounter forms should be used to record patient encounter for billing/tracking purposes.
- Check-in staff should verify patient's name, date of birth, telephone number, home address, and insurance information as available on the paper; schedule and record all changes on the encounter form.
- If the patient is a walk-in or new patient and demographic information is not available, paper registration forms should be filled out by check-in staff and placed in a temporary chart.
- If co-pay information was available on the schedule, or if the patient has a co-pay amount listed on their insurance card, the check-in person should collect as appropriate.
- Notify nursing staff when a patient is ready to be taken back.
- Paper progress note templates should be used to record usual nurse intake.
- Notify provider that the patient is ready.
- Provider records notes on paper progress notes.
- Provider orders are recorded on paper progress notes, while recording the appropriate charges for orders on the paper encounter form.
- When the provider/nurse is finished with the patient, the provider will complete the encounter form (diagnosis, charges, and desired return appointment date/time) and have the patient go to check-out.
- Encounter forms and progress notes should be kept for loading into the EHR for when the EHR system is operational and normal operations resume.

System Restoration:

Patient encounters occurring during system downtime should be entered into the system via the following procedures:

- The chief complaint should be appended with “- downtime progress note attached.”
- Paper progress notes should be attached to electronic progress notes by scanning and or data entry directly onto the progress note.
- Billing/insurance information should be updated as necessary as the diagnosis and charges from the encounter form are entered.
- Immunizations should be entered into the electronic progress notes.
- Scheduling and telephone encounters for all other issues should be entered into the system and routed as appropriate.

Additional Functions:

- The Practice manager is responsible for maintaining an adequate stock of paper forms in anticipation of system downtime.
- Faxes will be evaluated by a nurse for urgency of review by provider.
- Items requiring review by a provider will be directed to their attention.
- All other phone/fax information will be scanned into the patient's record when the EHR system is operational and normal operations have resumed.

Radiology Consultants of Little Rock, P.A.	
Policy and Procedure	
Title: Emergency Access “Break the Glass”	P&P #: IS-3.0
Approval Date: 5/1/2016	Review: Annual
Effective Date: 5/1/2016	Information Technology

Emergency Access “Break the Glass”

Policy Summary

The Practice has an emergency access procedure enabling authorized workforce members to obtain required ePHI during a medical emergency. The Practice has an emergency access procedure enabling Practice workforce members to access the minimum ePHI necessary to effectively and efficiently treat patients in the event of a major medical emergency.

Purpose

This policy reflects the Practice’s commitment to have emergency access procedures enabling authorized workforce members to obtain required ePHI during an emergency situation.

Definitions

Medical emergency means medically necessary care which is immediately needed to preserve life, prevent serious impairment to bodily functions, organs, or parts, or prevent placing the physical or mental health of the patient in serious jeopardy.

Electronic protected health information (ePHI) means individually identifiable health information that is:

- Transmitted by electronic media
- Maintained in electronic media

Electronic media means:

1. Electronic storage media including memory devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card; or
2. Transmission media used to exchange information already in electronic storage media. Transmission media include, for example, the Internet, extranet (using Internet technology to link a business with information accessible only to collaborating parties), leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media. Certain transmissions, including of paper, via facsimile, and of voice, via telephone, are not considered to be transmissions via electronic media, because the information being exchanged did not exist in electronic form prior to the transmission.

Information system means an interconnected set of information resources under the same direct management control that shares common functionality. Such a system would normally include hardware, software, information, data, applications, communications, and people.

Workforce member means employees, volunteers, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity. This includes full and part time employees, affiliates,

associates, volunteers, and staff from third party entities who provide service to the covered entity.

Policy

1. The Practice has emergency access procedures enabling authorized workforce members to obtain required ePHI during a medical emergency. The procedure includes:
 - Identifying and defining which Practice workforce members are authorized to access ePHI during an emergency.
 - Identifying and defining manual and automated methods to be used by authorized Practice workforce members to access ePHI during a medical emergency.
 - Identifying and defining appropriate logging and auditing that must occur when authorized Practice workforce member's access ePHI during an emergency.
2. The Practice has emergency access procedures enabling Practice workforce members to access the minimum ePHI necessary to treat patients in the event of a medical emergency. Such access must be authorized by appropriate Practice management or designated personnel.
3. Regular training and awareness on the emergency access procedure is provided to all Practice workforce members.
4. All appropriate Practice workforce members have access to a current copy of this procedure and an appropriate number of copies of this procedure should be kept off-site.

Scope/Applicability

This policy is applicable to all divisions and workforce members that use or disclose electronic protected health information for any purpose. This policy's scope includes all electronic protected health information, as described in definitions below.

HIPAA Security

Regulatory Category: Technical Safeguards

Regulatory Type: REQUIRED Implementation Specification for Access Control Standard

Regulatory Reference: 45 CFR 164.312(a)(2)(ii)

Rule Language:

"Establish (and implement as needed) procedures for obtaining necessary electronic protected health information (ePHI) during a medical emergency."

Scenario

"Break the Glass" refers to the practice of enabling a licensed practitioner to view a patient's medical record, or a portion thereof, under emergency circumstances, when that practitioner does not have the necessary system access privileges.

Policy Authority/Enforcement

The Practice Security Officer is responsible for monitoring and enforcing this policy.

Procedures

Mechanism to Provide Emergency Access to ePHI

1. This process will bypass formal access procedures and is limited to medical emergencies.
2. The Security Officer may make requests for emergency access.
3. The request should contain:
 - a. The individual being granted the emergency access,
 - b. Job title
 - c. Reason for emergency access

- d. Date and time granted access
- e. The name of the individual granting access.
4. The Security Officer, or designated person, records information about emergency users and the emergency access rights assigned to them.
5. The system administrator and Security Officer will create an emergency access account upon above request and approval.
6. The emergency access will be tracked and documented based on capabilities of the EHR system. The tracking documentation will be reviewed by the Security Officer to determine that emergency access was appropriate.
7. At the conclusion of the event that precipitated the granting of emergency access, the Security Officer ensures the break-glass accounts are disabled, and new ones created in anticipation of the next emergency.
8. Any inappropriate use of emergency access will be treated as a security incident, and may subject an employee to disciplinary action, up to and including termination.
9. Documentation concerning emergency access will be retained and maintained for at least six years from the date of creation.

Note:

When using a specific user account that provides full access to all ePHI (an administrator account) consider the following:

- Creating an extremely complicated password (but one an employee will be able to enter while under the stress of an emergency situation).
- Securing the password.
- Periodically changing the password.

Enforcement

Please refer to *IS-4.0 Sanction Policy* for details regarding disciplinary action against employees, contractors, or any individuals who violate this policy.

Radiology Consultants of Little Rock, P.A.	
Policy and Procedure	
Title: Sanction Policy Security Violations and Disciplinary Action	P&P #: IS-4.0
Approval Date: 5/1/2016	Review: Annual
Effective Date: 5/1/2016	Human Resources

Sanction Policy

Policy

It is the policy of the Practice that all workforce members must protect the confidentiality, integrity, and availability of sensitive information at all times. The Practice will impose sanctions, as described below, on any individual who accesses, uses, or discloses sensitive information without proper authorization.

The Practice will take appropriate disciplinary action against employees, contractors, or any individuals who violate the Practice’s information security and privacy policies or state, or federal confidentiality laws or regulations, including the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

Purpose

To ensure that there are appropriate sanctions that will be applied to workforce members who violate the requirements of HIPAA, Practice’s security policies, Directives, and/or any other state or federal regulatory requirements.

Definitions

Workforce member means employees, volunteers, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity. This includes full and part time employees, affiliates, associates, volunteers, and staff from third party entities who provide service to the covered entity.

Sensitive information, includes, but not limited to, the following:

- Protected Health Information (PHI) – Individually identifiable health information that is in any form or media, whether electronic, paper, or oral.
- Electronic Protected Health Information (ePHI) – PHI that is in electronic format.
- Personnel files – Any information related to the hiring, termination, discipline and/or employment of any individual who is or was employed by the Practice.
- Payroll data – Any information related to the compensation of an individual during that individuals’ employment with the Practice.
- Financial/accounting records – Any records related to the accounting practices or financial statements of the Practice.
- Other information that is confidential – Any other information that is sensitive in nature or considered to be confidential including social security numbers, demographic information, payment methods and numbers, passwords etc.

Availability refers to data or information which is accessible and useable upon demand by an authorized person.

Confidentiality refers to data or information which is not made available or disclosed to unauthorized persons, systems or processes.

Integrity refers to data or information that has not been altered or destroyed in an unauthorized manner.

Violations

Listed below are the types of violations that require sanctions to be applied. They are stated at levels 1, 2, and 3 depending on the seriousness of the violation.

Level	Description of Violation
1	<ul style="list-style-type: none"> • Accessing information that you do not need to know to do your job. • Sharing computer access codes (user name & password). • Leaving computers unattended while being able to access sensitive information. • Disclosing sensitive information with unauthorized persons. • Copying sensitive information without authorization. • Changing sensitive information without authorization. • Discussing sensitive information in a public area or in an area where the public could overhear the conversation. • Failing/refusing to cooperate with the Information Security Officer, Privacy Officer, Security Officer, Chief Information Officer, and/or authorized designee.
2	<ul style="list-style-type: none"> • Second occurrence of any Level 1 offense (does not have to be the same offense). • Unauthorized use or disclosure of sensitive information. • Using another person's computer access code (user name & password). • Failing/refusing to comply with a remediation resolution or recommendation.
3	<ul style="list-style-type: none"> • Third occurrence of any Level 1 offense (does not have to be the same offense). • Second occurrence of any Level 2 offense (does not have to be the same offense). • Obtaining sensitive information under false pretenses. • Using and/or disclosing sensitive information for commercial advantage, personal gain, or malicious harm.

Recommended Disciplinary Actions

In the event that a workforce member violates the Practice’s privacy or security policies and/or violates the Health Insurance Portability and Accountability Act of 1996 (HIPAA) or related federal or state laws governing the protection of sensitive, PHI or personally identifiable information, the following recommended disciplinary actions will apply.

Violation Level	Recommended Disciplinary Action
1	<ul style="list-style-type: none"> • Verbal or written reprimand • Retraining on privacy/security awareness • Retraining on the Practice’s privacy and security policies • Retraining on the proper use of internal or required forms
2	<ul style="list-style-type: none"> • Letter of Reprimand*; or suspension • Retraining on privacy/security awareness • Retraining on the Practice’s privacy and security policies • Retraining on the proper use of internal or required forms
3	<ul style="list-style-type: none"> • Termination of employment or contract

	<ul style="list-style-type: none">• Civil penalties as provided under HIPAA and other applicable federal, state and local law• Criminal penalties as provided under HIPAA and other applicable federal/, state, and local law
--	--

Important Note: The recommended disciplinary actions are identified in order to provide guidance in policy enforcement and are not meant to be all-inclusive. If formal discipline is deemed necessary, the Practice shall consult with Human Resources prior to taking action. When appropriate, progressive disciplinary action steps shall be followed allowing the employee to correct the behavior which caused the disciplinary action.

*A Letter of Reprimand should be reviewed by Human Resources or Legal Council before given to the employee.

Exceptions

Depending on the severity of the violation, any single act may result in disciplinary action up to and including termination of employment or contract with the Practice.

Radiology Consultants of Little Rock, P.A.	
Policy and Procedure	
Title: EMPLOYEE BACKGROUND CHECKS	P&P #: IS-4.1
Approval Date: 5/1/2016	Review: Annual
Effective Date: 5/1/2016	Human Resources

Employee Background Checks

The Practice may conduct employment reference checks, investigative consumer reports, and background investigations on applicable candidates for employment prior to making a final offer of employment, and may use a third party to conduct these background checks. The Practice will obtain written consent (Appendix G) from applicants and employees prior to ordering reports from third-party providers, and will provide a description of applicant and employee rights and all other documentation as required by law to each applicant or candidate in accordance with FCRA and applicable state and federal statutes. All background checks are subject to these notice and consent requirements.

The type of information that could be collected by the Practice in background checks, investigative consumer reports and background investigations may include, but is not limited to, some or all of the following:

- Private and government agency reports related to any history of criminal, dishonest, or violent behavior, and other reports that relate to suitability for employment
- Education verification checks (including degrees awarded and GPA)
- Employment history verification, abilities, and reasons for termination of employment
- Professional licensing board verification
- HHS Office of the Inspector General List of Excluded Individuals
- Address history
- Social networking site reviews
- Credit reports
- Social security number verification
- Civil court filings, criminal record check
- Motor vehicle and driving records
- Professional and/or personal references through friends, relatives, neighbors and associates

This information may also be verified at other times during employment, such as during reassignment, promotional periods, following safety infractions, as part of a regularly scheduled review or for any other reason or for no reason at all.

The Practice will conduct background checks in compliance with the federal Fair Credit Reporting Act (FCRA), the Americans with Disabilities Act (ADA), and all other applicable local, state, and federal laws and regulations.

A reported offense will not necessarily disqualify a candidate from consideration for employment, unless the nature of the offense and job role being considered for the potential employee would preclude an offer of employment (i.e., an offense for fraud for a financial position or inclusion in OIG's list of excluded individuals where the position would involve providing services for a federally funded health program). The nature and seriousness of the offense, the date of the offense, the surrounding circumstances, rehabilitation, the relevance of the offense to the specific position(s), and whether hiring, transferring or promoting the applicant would pose an unreasonable risk to the business may be considered before a final decision is reached. The Practice will follow FCRA requirements, other applicable statutes, and Practice procedures for providing information and reports, making decisions, and responding to applicants and employees regarding potentially adverse actions to an investigative report.

The Practice reserves the right to withdraw any offer of employment or consideration for employment, or discharge an employee, upon finding falsification, misrepresentation, or omission of fact on an employment application, resume, or other attachments, as well as in verbal statements, regardless of when it is discovered.

Background check reports shall be maintained in separate, confidential files and retained in accordance with the Practice's document retention procedures.

Radiology Consultants of Little Rock, P.A.	
Policy and Procedure	
Title: Incident and Breach Notification Procedure	P&P #: IS-5.0
Approval Date: 5/1/2016	Review: Annual
Effective Date: 5/1/2016	Information Technology

Incident and Breach Notification Procedures

Purpose

To outline the process for notifying affected individuals of a breach of protected information under the Privacy Act, unsecured protected health information (PHI) for the purposes of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Health Information Technology for Economic and Clinical Health Act (HITECH), and/or state breach notification purposes.

Scope

This applies to all employees, volunteers, and other individuals working under contractual agreements with the Practice. Breach can apply to either privacy or security incidents and can be investigated by either and both the Privacy Officer and the Security Officer.

Definitions

State Breach – Unauthorized acquisition or reasonable belief of unauthorized acquisition of Personal Information that compromises the security, confidentiality or integrity of the Personal Information.

Personal Information – Personal Information has many definitions including definitions by statute which may vary from state to state. Generally, Personal Information is a combination of data elements which could uniquely identify an individual. Please review applicable state data breach statutes to determine what definition of Personal Information is applicable for purposes of the document.

HIPAA Breach – Unauthorized acquisition, access, use, or disclosure of unsecured PHI.

Personally Identifiable Information (PII) – Information in any form that consists of a combination of an individual’s name and one or more of the following: Social Security Number, driver’s license or state ID, account numbers, credit card numbers, debit card numbers, personal code, security code, password, personal ID number, photograph, fingerprint, or other information which could be used to identify an individual.

Individually Identifiable Health Information (IIHI) – PII which includes information related to the past, present or future condition, treatment, payment or provision of health care to the identified individual.

Privacy Act Breach – Unauthorized acquisition or reasonable belief of unauthorized acquisition of personal information protected by the Privacy Act. This information includes, but is not limited to Social Security Numbers, government issued ID numbers, financial account numbers or other information posing a risk of identity theft.

Private Information – Information protected by the Privacy Act, Personally Identifiable Information, Personal Information and Protected Health Information collectively.

Protected Health Information (PHI) – Individually identifiable health information except for education records covered by FERPA and employment records.

Procedure

Reporting a Possible Breach

1. Any employee who becomes aware of a possible breach of privacy or security involving Private Information in the custody or control of the Practice will immediately inform their supervisor/manager, and the Privacy or Security Officer.
2. Notification should occur immediately upon discovery of a possible breach or before the end of your shift if other duties interfere, however, in no case should notification occur later than twenty-four (24) hours after discovery.
 - a. The supervisor/manager will verify the circumstances of the possible breach and inform the Privacy or Security Officer and the division Administrator/Director within twenty-four (24) hours of the initial report.
3. You may call the Privacy Officer directly at **(501) 978-5407**.
 - a. Provide the Privacy Officer with as much detail as possible.
 - b. Be responsive to requests for additional information from the Privacy Officer.
 - c. Be aware that the Privacy Officer has an obligation to follow up on any reasonable belief that Private Information has been compromised.
4. The Privacy Officer, in conjunction with the Practice's Legal Counsel, will decide whether or not to notify the President/CEO as appropriate by taking into consideration the seriousness and scope of the breach.

Containing the Breach

1. The Privacy Officer will take the following steps to limit the scope and effect of the breach.
 - a. Work with department(s) to immediately contain the breach. Examples include, but are not limited to:
 - i. Stopping the unauthorized practice
 - ii. Recovering the records, if possible
 - iii. Shutting down the system that was breached
 - iv. Mitigating the breach, if possible
 - v. Correcting weaknesses in privacy or security practices
 - vi. Notifying the appropriate authorities including the local Police Department if the breach involves, or may involve, criminal activity

Investigating and Evaluating the Risks Associated with the Breach

1. To determine what other steps are immediately necessary, the Privacy Officer in collaboration with the Practice's Legal Counsel and affected department(s) and administration, will investigate the circumstances of the breach.
 - a. A team will review the results of the investigation to determine root cause(s), evaluate risks, and develop a resolution plan.
 - i. The Privacy Breach Assessment tool will help aid the investigation.
 - b. The Privacy Officer, in collaboration with the Practice's Legal Counsel, will consider, at a minimum, four factors in determining whether to notify individuals affected by the breach including. If, after consideration of the four factors listed

below, it can be determined that there is a low probability of compromise of the individuals' PHI, then a decision can be made to not report the incident as a breach and to not notify affected individuals. If, however, it cannot be determined that there is a low probability of compromise of the individuals' PHI, then the breach must be reported to the affected individuals and the Secretary of HHS. The analysis of these four factors in determining whether or not to report a breach must be documented and such documentation retained by the Practice.

These four factors are:

- i. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
 - ii. The unauthorized person who used the PHI or to whom the disclosure was made;
 - iii. Whether the PHI was actually acquired or viewed; and
 - iv. The extent to which the risk to the PHI has been mitigated.
- c. In addition to the required four factors indicated above, additional factors may be considered which could include:
- i. Risk of physical harm if the loss puts an individual at risk of stalking or harassment
 - ii. Risk of hurt, humiliation, or damage to reputation when the information includes medical or disciplinary records

Notification

1. The Privacy Officer will work with the department(s) involved, the Practice's Legal Counsel and appropriate leadership to decide the best approach for notification and to determine what may be required by law.
2. If required by law, notification of individuals affected by the breach will occur as soon as possible following the breach. (sample letter in Appendix E)
 - a. Affected individuals must be notified without reasonable delay, but in no case later than sixty (60) calendar days after discovery, unless instructed otherwise by law enforcement or other applicable state or local laws.
 - i. Notices must be in plain language and include basic information, including:
 1. What happened
 2. Types of PHI involved
 3. Steps individuals should take
 4. Steps covered entity is taking
 5. Contact Information
 - ii. Notices should be sent by first-class mail or, if the individual agrees, electronic mail. If insufficient or out-of-date contact information is available, then a substitute notice is required as specified below.
 - b. If law enforcement authorities have been contacted, those authorities will assist in determining whether notification may be delayed in order not to impede a criminal investigation.
3. The required elements of notification vary depending on the type of breach and which law is implicated. As a result, the Practice's Privacy Officer and Legal Counsel should work closely to draft any notification that is distributed.
4. Indirect notification such as website information, posted notices, media will generally occur only where direct notification could cause further harm, or contact information is lacking. (sample letter in Appendix F)

- a. If a breach affects five-hundred (500) or more individuals, or contact information is insufficient, the Practice will notify a prominent media outlet that is appropriate for the size of the location with affected individuals, and notice will be provided in the form of a press release.
5. In certain cases, multiple methods of notification may be the most effective approach.

Business associates must notify the Practice if they incur or discover a breach of unsecured PHI.

1. Notices must be provided in accordance with the business associate's business associate agreement with the Practice, or, if such a provision is not included within the business associate agreement, without reasonable delay and in no case later than sixty (60) days after discovery of the breach.
2. Business associates must cooperate with the Practice to investigate and mitigate breaches.

Notice to Health and Human Services (HHS) as required by HIPAA – If the Practice's Legal Counsel determines that HIPAA notification is not required; this notice is also not required.

1. Information regarding breaches involving five-hundred (500) or more individuals, regardless of location, must be submitted to HHS at the same time that notices to individuals are issued.
2. If a breach involves fewer than five-hundred (500) individuals, the Practice will be required to keep track of all breaches and to notify HHS within sixty (60) days after the end of the calendar year.

Prevention

1. Once immediate steps are taken to mitigate the risks associated with the breach, the Privacy Officer will investigate the cause of the breach.
 - a. If necessary, this will include a security audit of physical, organizational, and technological measures.
 - b. This may also include a review of any mitigating steps taken.
2. The Privacy Officer will assist the responsible department to put into effect adequate safeguards against further breaches.
3. Procedures will be reviewed and updated to reflect the lessons learned from the investigation and regularly thereafter.
4. The resulting plan will also include audit recommendations, if appropriate.

Compliance and Enforcement

All managers and supervisors are responsible for enforcing these procedures. Employees who violate these procedures are subject to discipline up to and including termination in accordance with the Practice's Sanction Policy.

Attachments

Appendix F: Incident Response Tools for Privacy and Security

Radiology Consultants of Little Rock, P.A.	
Policy and Procedure	
Title: Business Associate Policy	P&P #: IS-6.0
Approval Date: 5/1/2016	Review: Annual
Effective Date: 5/1/2016	Information Technology

Business Associate Policy

POLICY:

In accordance with the Health Insurance Portability and Accountability Act of 1996 and its accompanying regulations (HIPAA), Covered Entities must establish agreements and procedures with certain persons or entities which provide services to or on behalf of Covered Entities to ensure compliance with HIPAA regulations related to Business Associates. The Covered Entity must determine who is a Business Associate and have written Business Associate Agreements in place before disclosing protected health information (PHI) to Business Associates.

DEFINITIONS:

Business Associate. “Business Associate” is a person or entity, other than a member of the workforce of a Covered Entity, who performs functions or activities on behalf of, or provides certain services to, a Covered Entity that involve access by the Business Associate to protected health information. A “Business Associate” can also be a subcontractor that creates, receives, maintains, or transmits protected health information on behalf of a Business Associate.

Covered Entity. “Covered Entity” means a Practice or individual that is: 1) a health care provider that conducts certain transactions in electronic form, 2) a health care clearinghouse, or 3) a health plan.

Subcontractor. “Subcontractor” means a person that creates, receives, maintains, or transmits protected health information on behalf of a Business Associate.

Procedure

Contract review: The Privacy/Security Officer of the Practice will be involved in the contract process so that determination can be made if contractors are Business Associates and if an agreement is needed. Each contract arrangement can have different elements and functions and the Privacy/Security Officer can determine which contracts need agreements. The identification of Business Associates should be made at the time contracts are negotiated or arrangements for services with contractors are made and prior to releasing PHI to the contractor. Approved Contractors (Appendix D) serves as a log of all Business Associates.

Identify Business Associates:

It is important to understand who is and who is not a Business Associate. A Business Associate is an entity that on behalf of a Covered Entity performs or assists in the performance of any of the following, if it involves use or disclosure of PHI or any other function regulated by HIPAA:

- Claims processing or administration;
- Data analysis;
- Processing or administration;
- Utilization review;
- Quality assurance;

This document has been customized for the HealthIT member for whom it has been provided. For security purposes and to ensure that each HealthIT member is receiving the appropriate documents, retransmitting, modifying, sharing or disseminating without express consent of HealthIT is strictly prohibited.

- Billing;
- Benefit management;
- Practice management;
- Repricing;
- Legal guidance;
- Consulting.

Identify exceptions to the rule:

There are important exceptions. First, a member of the Practice workforce is not a Business Associate. Workforce means employees, volunteers, trainees, and others whose work performance is under the Covered Entity's direct control, regardless of whether they are paid.

Additionally, if the Practice healthcare providers participate in an organized healthcare arrangement which means:

- a) a clinically integrated care setting in which individuals typically receive health care from more than one health care provider; or
- b) an organized system of health care in which more than one Covered Entity participates, and in which the participating Covered Entities hold themselves out to the public as participating in a joint arrangement and participate in joint activities.

If another member of the arrangement performs a function or activity on behalf of the arrangement that by itself does not make that other member a Business Associate.

Also the following are NOT considered Business Associates:

- a) Provider to Provider. The disclosure is to a provider concerning treatment of the individual about whom the information pertains,
- b) Health Plan. The other party is a plan sponsor, provided that the requirements of the regulations for plan-sponsor documents are satisfied and are a group health plan, health insurer or HMO,
- c) Eligibility. Government program providing public benefits and either
 - a. eligibility or enrollment is determined by the Business Associate, or
 - b. determination for eligibility or enrollment is made by the provider but information to make those decisions is collected by the Business Associate.
- d) Service or Maintenance Contractors Without Exposure to PHI. Relationships with persons or organizations, such as janitorial services, electricians, or copier repair companies, whose functions or services are not intended to involve the use or disclosure of PHI, and where any disclosure of PHI during the performance of their duties would be limited and incidental, such as disclosures that may occur while walking through or working in file rooms.
- e) Couriers. Disclosures of PHI to a person or organization that acts merely as a conduit for protected health information, such as the U.S. Postal Service, UPS, FedEx, other private couriers, and their electronic equivalents.
- f) Financial Transaction Institutions. When a Covered Entity initiates transactions as requested by the patient for payment of health care or health plan premiums.

- g) No PHI Disclosed. If the information disclosed is not PHI, or if the PHI is de-identified in accordance with the HIPAA de-identification standards, then the person or entity receiving the information would not be a Business Associate.

Business Associate Agreement: Once contractors have been identified as a Business Associate, a Business Associate Agreement must be signed. The Agreement approved for use by this Practice is on file at Practice. It is the policy of this Practice that the contractor signs the Business Associate Agreement of the Covered Entity that is the healthcare provider. If a contractor insists on their Business Associate Agreement be signed the Agreement must be reviewed for all relevant content as required by HIPAA, Breach Notification and HITECH regulations.

Content of the Business Associate Agreement shall require that Business Associates Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the covered entity. The Agreement will also ensure that any agent, including a subcontractor, to whom it provides such information agrees to implement reasonable and appropriate safeguards to protect it. The Agreement will require the Business Associate to report to the covered entity any security incident of which it becomes aware and authorize termination of the contract by the covered entity, if the covered entity determines that the business associate has violated a material term of the contract.

Practice maintains the right to request any contractor to sign a Business Associate Agreement.

Once signed, the Business Associate Agreement shall be maintained with the contract and both parties will have copies of the agreement. The Business Associate Agreement will be kept with the contract and retained for the life of the contract with that contractor or 6 years, whichever is greater.

Contractor Confidentiality Agreement: Contractors who do not create, receive, maintain, or transmit protected health information on behalf of a Covered Entity but still have limited or incidental exposure to a Practice PHI may be required to sign a Contractor Confidentiality Agreement (Appendix K).

Updates:

Updates to this Business Associate Agreement will be executed as required by HIPAA, Breach Notification and HITECH regulations. Timeframes for implementing new agreements will follow the guidelines set forth in these federal regulations.

Notifications:

Business Associate is required to report to the Covered Entity any breach of Business Associate or subcontractor. All notifications are to be addressed to Practice representative outlined in Business Associate Agreement.

VIOLATIONS:

Violations of the Business Associate policy or the Business Associate Agreement should be reported immediately to the Privacy/Security Officer. Violations may constitute a breach of contract and may be subject to contract termination.

Appendix A – Network Access Request Form

Employee or Contractor Request for Network Access

EMPLOYEE/CONTRACTOR INFORMATION	
<input type="checkbox"/> New Employee <input type="checkbox"/> New Contractor <input type="checkbox"/> Existing User <input type="checkbox"/> Temporary	Today's Date:
First Name:	Last Name: *MI:
Position:	Department: Supervisor:
<input type="checkbox"/> Full-time <input type="checkbox"/> Part-time	Start date or Requested due date: Temporary or Contractor end date, if known:
SECURITY & EMAIL	
New Account: <input type="checkbox"/> Network Account <input type="checkbox"/> Email <input type="checkbox"/> Security/Email similar to what existing user:	
<input type="checkbox"/> Include in which E-mail Group(s): <input type="checkbox"/> Remove from which E-mail Group(s): <input type="checkbox"/> Include in which Security Group(s): <input type="checkbox"/> Remove from which Security Group(s):	
<input type="checkbox"/> Permit access to the following network location(s):	
Drive	Path Access: <input type="checkbox"/> Read-only <input type="checkbox"/> Read/write <input type="checkbox"/> Full Access <input type="checkbox"/> Remove Access
Drive	Path Access: <input type="checkbox"/> Read-only <input type="checkbox"/> Read/write <input type="checkbox"/> Full Access <input type="checkbox"/> Remove Access
Drive	Path Access: <input type="checkbox"/> Read-only <input type="checkbox"/> Read/write <input type="checkbox"/> Full Access <input type="checkbox"/> Remove Access
<input type="checkbox"/> Miscellaneous Needs (<i>Enter any other requests</i>):	
EHR ACCESS	
<input type="checkbox"/> EHR Account	
Roles & Access:	
<input type="checkbox"/> Front Office	Access: <input type="checkbox"/> Read-only <input type="checkbox"/> Read/write <input type="checkbox"/> Full Access <input type="checkbox"/> Remove Access
<input type="checkbox"/> Clinician	Access: <input type="checkbox"/> Read-only <input type="checkbox"/> Read/write <input type="checkbox"/> Full Access <input type="checkbox"/> Remove Access
<input type="checkbox"/> Physician	Access: <input type="checkbox"/> Read-only <input type="checkbox"/> Read/write <input type="checkbox"/> Full Access <input type="checkbox"/> Remove Access
<input type="checkbox"/> Accounting	Access: <input type="checkbox"/> Read-only <input type="checkbox"/> Read/write <input type="checkbox"/> Full Access <input type="checkbox"/> Remove Access
<input type="checkbox"/> Records Management	Access: <input type="checkbox"/> Read-only <input type="checkbox"/> Read/write <input type="checkbox"/> Full Access <input type="checkbox"/> Remove Access
<input type="checkbox"/> Reporting	Access: <input type="checkbox"/> Read-only <input type="checkbox"/> Read/write <input type="checkbox"/> Full Access <input type="checkbox"/> Remove Access
<input type="checkbox"/> Administrator	Access: <input type="checkbox"/> Read-only <input type="checkbox"/> Read/write <input type="checkbox"/> Full Access <input type="checkbox"/> Remove Access
<input type="checkbox"/> Other: Specify	Access: <input type="checkbox"/> Read-only <input type="checkbox"/> Read/write <input type="checkbox"/> Full Access <input type="checkbox"/> Remove Access
<input type="checkbox"/> Miscellaneous Needs (<i>Enter any other requests</i>):	
HARDWARE & SOFTWARE	
Hardware:	
<input type="checkbox"/> Laptop <input type="checkbox"/> Desktop <input type="checkbox"/> Either Laptop or Desktop	
<input type="checkbox"/> Screen protector	<input type="checkbox"/> Laptop bag <input type="checkbox"/> Cable lock
<input type="checkbox"/> Multifunction printer	<input type="checkbox"/> Netgear Router <input type="checkbox"/> Numeric keypad
<input type="checkbox"/> Standard inkjet printer	<input type="checkbox"/> Dual monitors <input type="checkbox"/> Docking station
<input type="checkbox"/> iPhone <input type="checkbox"/> iPad <input type="checkbox"/> Windows Mobile Device	

Software:

- Adobe Acrobat (full version) Email Encryption
 Microsoft Office Professional 2003 Microsoft Office Professional 2007
 MS Project 2007 MS Visio 2007 MS OneNote 2007
 Fax Server - *Specify level of access:*

Miscellaneous Needs (*Enter any other requests*):

TELEPHONY

Telephone:

- Desk Phone Softphone (IP Communicator)
 Desk phone currently exist at location. Current extension is:

Accessories:

- Wireless headset Wired headset

CELL PHONE / AIR CARD

- Cell phone Air Card

Accessories:

- Cell Phone Case/Holder Car Charger
 Miscellaneous Needs (*Enter any other requests*):

BUILDING ACCESS

Access Requested for the following location(s):

- Medical Records Room Server Room
 Lobby Other, *Specify:*

Additional Access Restriction:

- After-Hours Access, *Specify Hours:*

Other Restrictions (be specific):

SPECIAL INSTRUCTIONS

Manager Checklist/Reminder:

- Signature below can be of the Department Head or the Data Owner if new network access is requested.
- Ensure employee badge is requested
- Schedule new employee orientation, if applicable
- Ensure name appears on any appropriate sign-in/out sheets
- Remember to have all new employees/contractors read and sign appropriate forms, i.e. Confidentiality Form (Appendix B)
- Request appropriate training/background:
 - o HR Background Investigation
 - o Security Training
 - o Any additional training and/or background check

NAME (Print Name)	SIGNATURE	DATE OF INITIAL REQUEST	DATE OF REVIEW
Department Head			
Privacy/Security Officer or Appropriate Authority			

Appendix B – Workforce Confidentiality Agreement

I understand that Practice has a legal and ethical responsibility to maintain patient privacy, including obligations to protect the confidentiality of patient information and to safeguard the privacy of patient information.

I understand that Practice has a legal and ethical responsibility to maintain the confidentiality, integrity, and accessibility of protected health information maintained in hard copy or electronic format.

In addition, I understand that during the course of my employment/assignment/ affiliation at Practice, I may see or hear other confidential information, such as financial data and operational information pertaining to the Practice, that Practice is obligated to maintain as confidential.

As a condition of my employment/assignment/affiliation with Practice, I will be subject to pre-employment reference checks or criminal checks and that I understand that I must sign and comply with this agreement.

By signing this document I understand and agree that:

- I will disclose Patient Information and/or confidential information only if such disclosure complies with Practice policies and is required for the performance of my job.
- My personal access code(s), user ID(s), access key(s), and password(s) used to access computer systems or other equipment are to be kept confidential at all times.
- I will not access or view any information other than what is required to do my job. If I have any question about whether access to certain information is required for me to do my job, I will immediately ask my supervisor for clarification.
- I will not access my own records or records of my family members without first notifying the Privacy or Security Officer and having appropriate documentation (i.e. complete Authorization to Release Medical Information).
- I will not discuss any information pertaining to the Practice or its patients in an area where unauthorized individuals may obtain such information (for example, in hallways, on elevators, in the cafeteria, on public transportation, at restaurants, social media, blogging or other similar websites and at social events). I understand that it is not acceptable to discuss any Practice information in public areas even if specifics such as a patient's name are not used.
- I will not make inquiries about any Practice information for any individual or party who does not have proper authorization to access such information.
- I will not make any unauthorized transmissions, copies, disclosures, inquiries, modifications, or purging of patient information or confidential information. Such unauthorized transmissions include, but are not limited to; removing and/or transferring patient information or confidential information from Practice's computer system to unauthorized locations (for instance, home).
- Patient social security numbers are used for patient identification, billing, and collection purposes only. I understand that misuse of social security numbers will result in disciplinary action up to and including termination.
- Upon termination of my employment/assignment/affiliation with Practice, I will immediately return all property (e.g. keys, documents, ID badges, etc.) to Practice.

Information Security Policy

- I understand that I am required to immediately report criminal or administrative charges and/or convictions which may impact my ability to perform the essential functions of my job to the Practice. I will notify the HIPAA Privacy or Security Officer if I suspect that any confidential information has been misused, improperly disclosed, lost or stolen.
- I agree that the education, degree, certifications, and/or licensure I present at employment and for continued employment are true and accurate. In the event that the status of the above mentioned education, degree, certifications, and/or licensure change or is revoked I will immediately report this to the Practice.
- I agree that my obligations under this agreement regarding patient information will continue after the termination of my employment/assignment/affiliation with Practice.
- I understand that violation of this Agreement may result in disciplinary action, up to and including termination of my employment/assignment/affiliation with Practice and/or suspension, restriction, or loss of privileges, in accordance with Practice' policies, as well as potential personal civil and criminal legal penalties.
- I understand that any confidential information or patient information that I access or view at Practice does not belong to me.
- I have read and understand the Sanction Policy.
- I understand that any unauthorized use or disclosure of information residing on the PRACTICE information resource systems may result in disciplinary action consistent with the policies and procedures of federal, state, and local agencies.

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

Signature of Employee/Physician/Student/Volunteer

Date

Print Name

Appendix C – Approved Software

The following list has been approved for use by the Practice. All software must be installed and maintained by the appropriate Practice personnel.

Inventory of Software								
Name of Software	Version	Type of Data	Software supported by: (Company Name)	Data created by Practice or third-party	Data maintained by Practice or off-site	Impact if unavailable 3-High; 2-Medium; 1-Low	Harm if data breach 3-High; 2-Medium; 1-Low	Comments
EX: EHR vendor	11.0	PHI and clinical documentation	Amazing Charts	Practice	OffsiteServer	3	3	
EX: Lab interface	5.6	lab results	Quest	third-party	OffsiteServer	2	3	
EX: cleaning service	AL	none				no	offices	

See full document for detail

Appendix D – Approved Contractors

Inventory of Contractors - Business Associates and Contractors											
Contractor Company Name	Primary Contact (name)	Office Number	Mobile Number	Product/Service	Does Vendor access/use PHI?	How do they access PHI?	Business Associate Agreement (BAA) or Confidentiality Agreement (CA) in place?	Date of Agreement (BAA or CA)	Does Contractor need User ID and Password?	What PHI do they have access to in EHR?	Vendor Termination Date
EK: outside IT support	Nathan	501-555-1254	501-555-1236	Offsite IT support	yes	view into EHR at clinic	BAA	10/1/2013	yes to 2 employee	open to all functions of EHR	
EK: Lab company	MaryAnn	870-555-6987	870-555-7896	Process lab and return results to clinic	yes	pick up samples at clinic and take to lab. Results are sent electronically to EHR	BAA	6/6/2012	yes to 5 employees	limited to lab results section	
EK: cleaning service	Al	none	870-555-1234	cleans clinic after hours	no	see PHI when in offices	CA	8/23/2013	none		
EK: ShredIt	Jeff	501-555-4569	501-555-4789	offsite shredding	yes	remove shredding to shred off site	BAA	1/1/2014	none	none	
EK: HFArkansas	Mollie	501-212-8616	501-555-1598	REC assist with MU	yes	view PHI in EHR	BAA	4/3/2013	none	none	






See full document for detail

Appendix E – Device Inventory for Electronic Devices

Device Type	Make/Model	Date Acquired	Serial #	Location	User	Moved?	Date Moved, if applicable	Maintenance Performed?	Date of Maintenance	Description of Maintenance	Maintenance Performed By	Date Discarded	Hard Drive/Data Destroyed?	Method Used for Destruction	Name of Individual Who Completed Destruction	Name of Official Who Verified Destruction
Example 1 - Desktop	HP / Desktop 4520s	6/5/2011	123987654	Billing Office	Jane Doe	N	N/A	Y	9/26/2011	DVD replaced	ABC Computers	N/A	N/A	N/A		N/A
Example 2 - Laptop	Dell / XPS 250	1/3/2010	23456789	Nurses Station	John Doe	Y	7/9/2011	N	N/A	N/A	N/A					
Example 2 - Cont - Laptop	Dell / XPS 250	1/3/2010	23456789	Administrator's Off	Suzie Q	N	N/A	N	N/A	N/A	N/A	1/26/2012	Y	Data Erase 123	Joe Smith	

See full document for details

Appendix F – Incident Response Tools for Privacy and Security

Tool	Attached Form/Worksheet	Description
Incident Report	 Security_Incident-Report-Confidential.doc	Incident report utilized by the reporting employee or witness to an incident or potential incident.
Incident Investigation	 Security_Incident-Investigation-Confident	Incident investigation report that allows for further investigation of a potential incident upon receipt of the initial incident report.
Incident Log	 Security_Incident-Log-Confidential.xls	Incident log to ensure incidents are tracked for further analysis and follow-up.
Breach Assessment Tool	 Security_Incident-Breach Assessment-Cor	Breach assessment tool which can assist in determining the severity of a breach.
Breach Notification	 Security Incident Breach Notification dc	Notification letter to patient and notification statement to media when breach is found.

Appendix G – Background Check Authorization

AUTHORIZATION AND RELEASE TO OBTAIN INFORMATION

Under the provisions of the Fair Credit Reporting Act (15 U.S.C. §1681 et seq.), the Americans with Disabilities Act, and all applicable federal, state, and local laws, I hereby authorize and permit to obtain a consumer report and/or an investigative consumer report which may include the following:

1. My employment records;
2. Records concerning any driving, criminal history, credit history, civil record, workers' compensation (post-offer only), and drug testing;
3. Verification of my academic and/or professional credentials; and
4. Information and/or copies of documents from any military service records.

I understand that an "investigative consumer report" may include information as to my character, general reputation, personal characteristics, and mode of living, which may be obtained by interviews with individuals with whom I am acquainted or who may have knowledge concerning any such items of information.

I agree that a copy of this authorization has the same effect as an original.

I understand that information obtained in this authorized investigative consumer report and background investigation may result in not being offered a position of employment. I hereby release and hold harmless any person, firm, or entity that discloses information in accordance with this authorization, as well as from liability that might otherwise result from the request for use of and/or disclosure of any or all of the foregoing information except with respect to a violation of the Act. I authorize Practice and its designated agent and all associated entities to receive any criminal history information or credit report pertaining to me in the files of any state or local criminal justice agency. I authorize all corporations; companies; former employers; supervisors; credit agencies; educational institutions; law enforcement/ criminal justice agencies; city, state, county and federal courts; state motor vehicle bureaus; and other persons and entities to release information they may have about me to the Practice or their designated agent.

I hereby authorize the Practice to obtain and prepare an investigative consumer report and background investigation as set forth above, as part of its investigation of my employment application. This authorization shall remain in effect over the course of my employment. Reports may be ordered periodically during the course of my employment such as during reassignment or promotional periods and following safety infractions or other incidents. (NOTE: Except for those states where an annual release is required, i.e. California – Continuing consent concept is inapplicable and a separate authorization must be requested each time a report is ordered. - CA Civ. Code 1786.22)

I understand and acknowledge that under provision of the Fair Credit Reporting Act, I may request a copy of any consumer report from the consumer reporting agency that compiled the report, after I have provided proper identification.

My signature below also indicates that I have received a [Summary of Rights](#) in accordance with the Fair Credit Reporting Act.

Date _____

Applicant's Signature _____

Information Security Policy

Applicant's Printed Name _____

Other Names Used _____

Social Security Number ____/____/____ Date of Birth _____

Driver's License # _____ State _____

Current Address _____

City/Town _____ State _____ Zip Code _____

Previous address _____

City/Town _____ State _____ Zip Code _____

Adapted from <http://www.softechinternational.com/SampleReleaseForm.pdf> and
<http://www.national-employment-screening.com/background-check-release.htm>.

Appendix H – Change Management Tracking Log

Appendix G - Change Management Log - Physical and Technical Maintenance Log							5/2015
Clinic Name:			Year:				
#	Date	Change Description (update, new application, reconfiguration or work being done)	Change Implemented by: (vendor, employee etc.)	Type= physical or technical	Location	Duration of project	Issue Description and Actions Taken to resolve issues
	4/10/2013	Removed wall between two patient rooms and relocate lab services	Davis Contracting	physical	patient rooms 3 and 4	2 weeks	Due to physical changes in building, risk analysis performed to determine if PHI at risk.
	8/12/2013	upgrade EHR software	EHR vendor and local IT support	technical	server and each workstation	3 days	Training provided to staff on changes in upgrade
1							
2							
3							
4							

See full document for detail

Appendix I – Employee Termination Checklist

EMPLOYEE TERMINATION CHECKLIST		
Employee Name		
Date of Termination		
Title		
Department/Clinic		
Termination	<input type="checkbox"/> Voluntary <input type="checkbox"/> Involuntary	Rehire <input type="checkbox"/> Yes <input type="checkbox"/> No
Task	Returned	Responsible Individual
<input type="checkbox"/> Collect Employee’s Identification Badge/Access Card	<input type="checkbox"/> Yes _____ <input type="checkbox"/> No _____ <input type="checkbox"/> N/A _____	Supervisor
<input type="checkbox"/> Collect Employee’s Keys (e.g., building, department, desk, file cabinets, etc.)	<input type="checkbox"/> Yes _____ <input type="checkbox"/> No _____ <input type="checkbox"/> N/A _____	Supervisor
<input type="checkbox"/> Collect Employee’s Pager/Cell Phone, Laptop, Tablet, etc.	<input type="checkbox"/> Yes _____ <input type="checkbox"/> No _____ <input type="checkbox"/> N/A _____	Supervisor
<input type="checkbox"/> Collect Any Other Equipment/Items Issued to Employee <ul style="list-style-type: none"> ▪ Uniforms/Work Clothes ▪ Parking Pass ▪ Credit Card ▪ Other: _____ 		Supervisor
<input type="checkbox"/> Terminate Employee’s Network Access		Supervisor to Contact IS to Terminate Access
<input type="checkbox"/> Terminate Employee’s E-Mail Account		Supervisor to Contact IS to Terminate Access
<input type="checkbox"/> Terminate Employee’s Voice Mail		Supervisor to Contact IS to Terminate Access
<input type="checkbox"/> Terminate Employee’s Access to Security Alarms or Building Access		
<u>Terminate Employee’s Access to Other Software Programs:</u> <ul style="list-style-type: none"> <input type="checkbox"/> _____ <input type="checkbox"/> _____ <input type="checkbox"/> _____ <input type="checkbox"/> _____ <input type="checkbox"/> _____ 		Supervisor to Contact IS to Terminate Access
<input type="checkbox"/> Transfer Employee’s Electronic Files		Supervisor to Contact IS to Facilitate Transfer
Completed By <i>(Name/Title)</i>		
Date		

Appendix J - Bring Your Own Device Agreement

Practice Personal Mobile Electronic Device Agreement

I understand and acknowledge that as an employee of Practice, I may have access to, use or disclose Confidential Information made available to me on electronic devices. Such Confidential Information may include, but is not limited to:

1. any individuals' Protected Health Information (PHI);
2. financial and operational information of the Practice; and
3. information regarding personnel of the Practice that is confidential in nature (e.g., compensation, benefits, and disciplinary records).

Whereas, I wish to have access to or use Confidential Information on my personal mobile electronic device to conduct business of the Practice,

I hereby agree that my personal mobile electronic device ('mobile device') will be subject to restrictions and conditions to protect Confidential Information and further agree to the following:

1. The use of my mobile device is not permitted without prior approval and inspection by the Practice's Security Officer or other appropriate personnel.
2. Approval for the use of my mobile device will not be considered until I have successfully completed the mobile device training session.
3. That certain security standards and, possibly, applications may be required to be installed, configured and controlled by the Practice on my mobile device. Such standards and applications may include, but are not limited to:
 - a. Encryption for data at rest (stored) and data in motion (transmitted/received)
 - b. Device management software to remotely manage my mobile device by the Practice
 - c. Remote wipe capabilities to delete data from my mobile device
 - d. Device authentication by PIN, password, biometric or other secure method
 - e. Automatic lock screen requiring authentication to access my mobile device after a defined period of inactivity
4. That any Confidential Information or any other Practice data which may be stored on or transmitted to or from my mobile device is owned by the Practice.
5. The Practice reserves the right to access, view or otherwise inspect my mobile device at any time, in person or by remote means, to ensure that Confidential Information is kept secure.
6. I will notify the Practice immediately if I believe my mobile device has been lost or stolen.
7. I will notify the Practice when I decide to upgrade, change or stop using my mobile device.
8. If I am no longer using my previously approved mobile device for conducting Practice business, I will present my mobile device to the Practice and allow the Practice Security Officer or other appropriate personnel to ensure that any Confidential or other Practice information is securely deleted from my mobile device.
9. I will not share my mobile device with other people and will keep my PIN, password and/or other authentication information private and known only to myself.
10. I authorize the Practice, if it has a reasonable belief that my mobile device has been lost, stolen or in any way compromised, to remotely wipe any and all data (including my own personal data) from my mobile device.
11. That, whenever possible, my mobile device should only be used to access secure applications and computer equipment of the Practice to access Confidential Information and should not have any Confidential Information stored or downloaded to my mobile device.
12. In the event that Confidential Information must be downloaded or stored to my mobile device, the storage of such Confidential Information must be kept in an encrypted form using an encryption solution approved by the Practice.

13. If Confidential Information is stored on my mobile device, I will take steps to securely delete Confidential Information from my mobile device once it is longer required according to Practice approved secure deletion procedures.
14. Any electronic transmissions made between my mobile device and any other electronic device in which Confidential Information is transmitted must be encrypted using an encryption solution approved by the Practice.
15. Although the Practice will make reasonable efforts to assist me with the secure use of my mobile device to conduct Practice business, I understand that this device is not a Practice asset and that the support the Practice provides to me for the use of my mobile device may be limited or none at all.
16. I will not disable or modify any of the configuration settings applied and/or applications installed by the Practice on my mobile device.
17. I will maintain my mobile device and apply application and operating system updates to keep my mobile device current with any security fixes.
18. I will not 'jailbreak' my mobile device or otherwise bypass my mobile device manufacture's or the Practice's security measures.
19. I understand that in no event shall the Practice be held liable for any damages (direct, indirect, punitive, special, consequential or any other type of damages) for any of the actions and activities taken by the Practice in order to secure, maintain and control my mobile device. Such actions and activities may include but are not limited to surveillance of any and all activities conducted on my mobile device, the deactivation of my mobile device and the secure and irreversible removal of any and all data, including my personal data, from my mobile device.
20. I also understand that the use of my mobile device for business purposes may increase costs associated with the service plan for my mobile device and that any reimbursement for the increase in costs associated with the business use of my mobile device will not be reimbursed by the Practice.

Employee Signature

Date

Employee Name (Printed)

Appendix K – Contractor Confidentiality Agreement

CONTRACTOR CONFIDENTIALITY AGREEMENT

I understand that Practice has a legal and ethical responsibility to maintain patient privacy, including obligations to protect the confidentiality of patient information and to safeguard the privacy of patient information.

I understand that Practice has a legal and ethical responsibility to maintain the confidentiality, integrity, and accessibility of protected health information maintained in hard copy or electronic format.

In addition, I understand that during the course of my contract with Practice, I may see or hear other confidential information such as financial data and operational information pertaining to the Practice that Practice is obligated to maintain as confidential.

As a condition of my contract with Practice, I understand that I must sign and comply with this agreement.

By signing this document I understand and agree that:

- I will disclose Patient Information and/or confidential information only if such disclosure complies with Practice policies and is required for the performance of my contract.
- I will not access or view any information other than what is required to fulfill my contract. If I have any question about whether access to certain information is required, I will immediately ask the Privacy or Security Officer at the Practice for clarification.
- I will not discuss any information pertaining to the Practice or its patients in an area where unauthorized individuals may obtain such information (for example, in hallways, on elevators, in the cafeteria, on public transportation, at restaurants, social media, blogging or other similar websites, and at social events). I understand that it is not acceptable to discuss any Practice information in public areas even if specifics such as a patient's name are not used.
- I will not make inquiries about any Practice information for any individual or party who does not have proper authorization to access such information.
- I will not make any unauthorized transmissions, copies, disclosures, inquiries, modifications, or purging of patient information or confidential information. Such unauthorized transmissions include, but are not limited to; removing and/or transferring patient information or confidential information from Practice to unauthorized locations (for instance, home).
- Patient social security numbers are used for patient identification, billing, and collection purposes only. I understand that misuse of social security numbers will result in disciplinary action up to and including termination of my contract.
- Upon termination of my contract with Practice, I will immediately return all property (e.g. keys, documents, ID badges, etc.) to Practice.
- I understand that I am required to immediately report to the Practice when patient information has been accessed, disclosed or used by myself or others associated with the Contractor.
- I understand that I am required to immediately report criminal or administrative charges and/or convictions which may impact my ability to perform the essential functions of my contract to the HIPAA Privacy or Security Officer.

- I agree that my obligations under this agreement regarding patient information will continue after the termination of my contract with Practice.
- I understand that violation of this Agreement may result in disciplinary action, up to and including termination of my contract with Practice and/or suspension, restriction, or loss of privileges, in accordance with Practice' policies, as well as potential personal civil and criminal legal penalties.
- I understand that any confidential information or patient information that I access or view at Practice does not belong to me.

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

Signature of Contractor

Date

Print Name

Contractor Company Name (print)