Ralph Parker, MD
Information Security Policies and Procedures

INTRODUCTION

The purpose of this manual is to demonstrate a conscientious effort to meet the various elements of the HIPAA Security Rule and to require that all employees of this "covered entity" are aware of and participating in this endeavor.

The basis for this manual are found in the two following Standards of that Rule.

HIPAA §164.308 Administrative safeguards.

§164.316 Policies and procedures and documentation requirements.

Within this document, and in accordance with the HIPAA Security Rule, there are items shown as "Standard", "Required" and "Addressable". As the names imply, items that are **Standard** and **Required** are steps the covered entity is expected to take dedicatedly. Items shown as Addressable are steps left to the discretion of the covered entity but whatever steps there may or may not be should be noted.

It should be acknowledged that no two covered entities are the same and therefore each will have its own requirements and establish its own criteria and willingness to comply with the rules set out in both Federal and State governance.

The information contained in this manual is not intended to serve as legal advice nor should it substitute for legal counsel. The material is designed to provide a form of guidance regarding best practices. The guidance is not exhaustive, and readers are encouraged to seek additional detailed technical, and if necessary, legal guidance to supplement the information contained herein.

Ralph Parker, MD
Information Security Policies and Procedures

HIPAA §164.308 Administrative safeguards.

(a) A covered entity must, in accordance with §164.306:

(1) (i) Standard: Security management process. Implement policies and procedures to prevent, detect, contain, and correct security violations.

The preparation of this manual is evidence of our intention to meet this Standard.

(ii) Implementation specifications:

(A) Risk analysis (Required)
Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity.

On September 18, 2017, a Security Risk Analysis, as designed by the Office of the National Coordinator for Health Information Technology was performed and will be performed or reviewed annually.

(B) Risk management (Required)
Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with §164.306(a).

The practice maintains appropriate physical safeguards to include assuring that only authorized individuals have access to the facility and to where e-PHI may be used or maintained. Administratively, the practice is certain to see that all workforce members are aware of practice policies and procedures and trained on how to properly protect patient records. Technically, the practice has strict controls on access to our patient information and will make use of audit and access logs to monitor users and other activities. The practice also has in place technical safeguards to include scheduled, periodic reviews of audit logs, as well as using a firewall, virus protection and other systems to protect our patient data. We have Business Associate Agreements in place with third-party vendors who might create, maintain, transmit or receive patient data on our behalf and this manual has a separate section specifically dealing with our responsibilities in the event of a security incident or breach.

Ralph Parker, MD
Information Security Policies and Procedures

HIPAA §164.308 Administrative safeguards (cont'd.)

(C) Sanction policy (Required)
Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity.

The practice has a progressive disciplinary policy. Depending on the severity of the infraction, at a first offense, we would attempt to counsel with the employee and determine if additional training might be in order. At a second offense, and again, depending on the severity of the infraction, we would put a written report in the employee's personnel file with the possibility of additional disciplinary actions up to and including termination. A third offense would be automatic termination.

(D) Information system activity review (Required)
Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

The practice operates as a workgroup and, other than individual event logs on each computer, has no other systems to review. There is an access log in the EMR system that management will review to verify that users have not attempted to access areas that are not required based on their job responsibilities. A Security Incident Report form is a part of this manual and would be generated by an IT contractor in the event of a breach or other suspected unauthorized access to our system.

The practice has in place certain technical safeguards as well as firewall, virus protection and other systems used in connection with the EMR. Of particular note will be any discovered attempts at unauthorized access to the general IT infrastructure of the practice.

Ralph Parker, MD
Information Security Policies and Procedures

§164.316 Policies and procedures and documentation requirements.

A covered entity must, in accordance with §164.306:

(a) **Standard*: Policies and procedures.*** *Implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of this subpart, taking into account those factors specified in §164.306(b)(2)(i), (ii), (iii), and (iv). This standard is not to be construed to permit or excuse an action that violates any other standard, implementation specification, or other requirements of this subpart. A covered entity may change its policies and procedures at any time, provided that the changes are documented and are implemented in accordance with this subpart.*

Dr. Parker understands that policies and procedures must be kept on file, either written or in electronic form, for a period of six (6) years from the date this manual is prepared and that any and all changes must be kept for six (6) years from the date any changes are enacted.

(b) (1) **Standard*: Documentation.***

(i) Maintain the policies and procedures implemented to comply with this subpart in written (which may be electronic) form; and

(ii) If an action, activity or assessment is required by this subpart to be documented, maintain a written (which may be electronic) record of the action, activity, or assessment.

See above.

(2) ***Implementation specifications:***

(i) ***Time limit (Required)*** *Retain the documentation required by paragraph (b)(1) of this section for 6 years from the date of its creation or the date when it last was in effect, whichever is later.*

See above.

Ralph Parker, MD
Information Security Policies and Procedures

§164.316 Policies and procedures and documentation requirements (cont'd.)

(ii) ***Availability*** ***(Required)*** *Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains.*

These policies and procedures will be shared with all workforce members so they will be aware of both, their responsibilities related to protecting patient confidentiality but also aware of the responsibilities of the practice relating to security and compliance regulations.

(iii) ***Updates*** ***(Required)*** *Review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the electronic protected health information.*

See above.

Ralph Parker, MD
Information Security Policies and Procedures

HIPAA §164.308(a)(2)

Standard*: Assigned security responsibility.* *Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the entity.*

The person(s) responsible for the development and implementation of the policies and procedures of this practice are as follows:

Name: Dr. Ralph Parker Date: 11/6/17

Position: Owner and Physician

Acknowledged by signature: _____

Name: Date:

Position:

Acknowledged by signature: _____

Name: Date:

Position:

Acknowledged by signature: _____

Name: Date:

Position:

Acknowledged by signature: _____

Ralph Parker, MD
Information Security Policies and Procedures

HIPAA §164.308(3)(i)

Standard*: Workforce security.* *Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information.*

Each workforce member who must, in the course of their job responsibilities, access patient information is assigned a unique login and password to our EMR. If an employee has no need for patient data to perform their daily functions, they would not be provided with a login or password to the EMR. Improperly sharing of logins and/or passwords is a terminable offense.

(ii) Implementation specifications:

(A) Authorization and/or supervision ***(Addressable****).*
Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.

Before a login and password are issued to a workforce member, their functions and responsibilities are reviewed. Then, when it is determined that access to the EMR is appropriate, they are assigned to the appropriate level of access and permissions in the EMR.

(B) Workforce clearance procedure ***(Addressable).***
Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.

Access and permissions are determined by the job functions to be fulfilled by the individual. Workforce members are not assigned to an access level that grants them more permissions than are necessary to perform their assigned duties.

Ralph Parker, MD
Information Security Policies and Procedures

HIPAA §164.308(3)(i) (cont'd.)

(C) Termination procedures (Addressable).
Implement procedures for terminating access to electronic protected health information when the employment of a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(B) of this section.

If an employee leaves the practice for any reason, we immediately deactivate their login and password to the EMR. Then, access to all other programs of the practice is removed and keys and any other company materials are also collected.

Ralph Parker, MD
Information Security Policies and Procedures

HIPAA §164.308(4)(i)

Standard*: Information access management.* *Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of subpart E of this part.*

Before granting access to patient data, management considers the functions to be performed by a workforce member and determines the level of access and amount of permissions to be granted to that workforce member. Access to the system will always be based on the "need to know" and the level of access will always be governed by the principal of "minimum necessary". Both of these criteria are a determination based on job responsibilities.

(ii) Implementation specifications:

(A) Isolating health care clearinghouse functions (Required)
If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization.

(If you use a healthcare clearinghouse that is part of a larger organization, have you confirmed that the clearinghouse has implemented policies and procedures to protect e-PHI from unauthorized access by the larger clearinghouse?)

The practice is not a clearinghouse but uses the services of a clearinghouse that is associated with MacPractice, the EMR. We have a Business Associates Agreement in place with the EMR vendor. A portion of the BA Agreement clearly specifies that the clearinghouse and the organizations with which they have a cooperative agreement, (if they should create, maintain, transmit or receive e-PHI on behalf of the practice or the clearinghouse), must abide by all regulations related to the protection of confidential patient information.

(B) Access authorization (Addressable).
Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism.

The practice operates as a workgroup and as such does not have other mechanisms for allowing access to the EMR. Management determines the appropriate access and levels of permissions for each workforce member and assigns them to that level in the EMR.

Ralph Parker, MD
Information Security Policies and Procedures

HIPAA §164.308(4)(i) (cont'd.)

(C) Access establishment and modification (Addressable).
Implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.

The practice plans to review our Policies and Procedures on an annual basis and this would include reviewing the access rights and privileges of our workforce members to patient data.

Should there be substantial changes in the environmental or operating aspects of the practice or, if a workforce member should have their responsibilities changed, we could find that it would be necessary to review our policies on a more frequent basis.

Ralph Parker, MD
Information Security Policies and Procedures

HIPAA §164.308(5)(i)

Standard*: Security awareness and training.* *Implement a security awareness and training program for all members of its workforce (including management).*

The practice has provided a new training program for the current employee and it meets the Federal HIPAA and Texas House Bill 300 requirements.

> *The following shows the original Texas training requirement for Texas House Bill 300 and then the actual changes to the legislation that came about via Texas Senate Bill 1609 one year later. When all is said and done, everyone in a Covered Entity must be trained in Texas on both the Federal HIPAA regulations as well as Texas rules.*

September 1, 2012 . . . Texas passed House Bill 300 which increased the training requirements for employees of covered entities. According to law, if a State rule is more stringent than the Federal law, the State law takes precedence. (The Texas House Bill WAS more stringent.)

Texas House Bill 300

SUBCHAPTER C. ACCESS TO AND USE OF PROTECTED HEALTH INFORMATION

Sec. 181.101. TRAINING REQUIRED.

(a) Each covered entity shall provide a training program to employees of the covered entity regarding the state and federal law concerning protected health information as it relates to:

(1) the covered entity's particular course of business; and

(2) each employee's scope of employment.

(b) An employee of a covered entity must complete training described by Subsection (a) not later than the 60th day after the date the employee is hired by the covered entity.

(c) An employee of a covered entity shall receive training described by Subsection (a) at least once every two years.

(d) A covered entity shall require an employee of the entity who attends a training program described by Subsection (a) to sign, electronically or in writing, a statement verifying the employee's attendance at the training program. The covered entity shall maintain the signed statement.

Ralph Parker, MD
Information Security Policies and Procedures

HIPAA §164.308(5)(i) . . . cont'd.

On September 1, 2013 . . . the Texas Legislature amended Texas House Bill 300 as it related to employee training

Section 181.101 TRAINING REQUIRED **(as amended by Senate Bill 1609 on Sept 1, 2013)**

AN ACT

relating to the training of employees of certain covered entities.
BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF TEXAS:
SECTION 1. Section 181.101, health and safety code is amended to read as follows:

Sec. 181.101 TRAINING REQUIRED. (a) Each covered entity shall provide ~~[a]~~ training ~~[program]~~ to employees of the covered entity regarding the state and federal law concerning protected health information as necessary and appropriate for the employees to carry out the employee's duties for the covered entity ~~[it relates to]~~:

~~[(1) the covered entity's particular course of business; and]~~
~~[(2) each employee's scope of employment].~~

(b) an employee of a covered entity must complete training described by subsection(a) not later than the 90th ~~[60th]~~ day after the date the employee is hired by the covered entity.

(c) if the duties of an ~~[An]~~ employee of a covered entity are affected by a material change in state or federal law concerning protected health information, the employee shall receive training described by subsection (a) within a reasonable period, but not later than the first anniversary of the date the material change in law takes effect ~~[at least once every two years]~~.

(d) a covered entity shall require an employee of the entity who receives ~~[attends a]~~ training ~~[program]~~ described by subsection (a) to sign, electronically or in writing, a statement verifying the employee's completion of ~~[attendance at the]~~ training ~~[program]~~. The covered entity shall maintain the signed statement until the sixth anniversary of the date the statement is signed.

Ralph Parker, MD
Information Security Policies and Procedures

HIPAA §164.308(5)(i) . . cont'd.

(ii) Implementation specifications. Implement:

(A) Security reminders ***(Addressable).***
Periodic security updates.

If the practice had multiple employees, we would hold periodic office meetings and information security would always be a topic of discussion such as making certain that patient records are not left unattended on computer screens and patient folders are not left in a position so that they could be seen by passersby.

(B) Protection from malicious software ***(Addressable).***
Procedures for guarding against, detecting, and reporting malicious software.

Knowing that there are a variety of ways that malicious software can make its way into a practice, the office has established a review process to confirm that certain aspects of our in-house procedures have not been violated. This would include 1) verifying that no employees are utilizing company internet connectivity for any purpose not directly tied to the performance of their job, 2) verifying employees are not opening personal emails or visiting social websites on company computers, 3) verifying that employees have not installed any outside software or programs not previously approved by management and 4) reiterating that employees must not connect any external device to a company computer. This includes thumb-drives, i-phones or any other device used to download data, audio or video materials.

(C) Log-in monitoring ***(Addressable).***
Procedures for monitoring log-in attempts and reporting discrepancies.

Because the practice operates as a simple workgroup, there is no monitoring available other than the ability to review access logs in the EMR. There is only the doctor and his nurse so there are no other persons accessing the patient data.

(D) Password management ***(Addressable).***
Procedures for creating, changing, and safeguarding passwords.

The EMR requires that passwords conform to a certain criteria for length and complexity. Additionally, passwords are required to be changed periodically.

Ralph Parker, MD
Information Security Policies and Procedures

HIPAA §164.308(6)(i)

Standard*: Security incident procedures.* *Implement policies and procedures to address security incidents.*

Defined as: the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

In the event of a security incident, whether real or suspected, the person responsible for maintaining our infrastructure will perform whatever diagnostics and tests are necessary to determine if an incident did occur. While the primary concern will be whether or not patient records were accessed, the practice will investigate the cause of the incident and what can be done to prevent it from happening again.

If patient records have been accessed, the practice will follow the investigation and reporting protocol as prescribed by HHS.

(ii) Implementation specification: Response and Reporting (Required)

Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes.

See above.

Ralph Parker, MD
Information Security Policies and Procedures

HIPAA §164.308(7)(i)

***Standard*: Contingency plan.** *Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information.*

The degree of severity and type of occurrence would dictate steps to be taken. Of prime importance would be to secure any devices with the ability to create, maintain, transmit or receive e-PHI and also the ability to access patient records. Patient records are stored locally but there are multiple local backups of the data as well as a cloud-based backup. There are documented instructions on how to restore data in the event that the main data is lost or compromised. Also, determined by the degree of damage, the practice might have to consider its physical location needs, if nothing else, in order to decide how best to provide patient information to the patients or other providers as was necessary.

(ii) ***Implementation specifications:***

(A) ***Data backup plan*** ***(Required)***
Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.

There are multiple local backups of our practice data, an off-site backup of our data and an encrypted device that is also backed up to weekly and carried offsite.

(B) ***Disaster recovery plan*** ***(Required)***
Establish (and implement as needed) procedures to restore any loss of data.

Part of our documented contingency plan is a set of instructions of what must be done and in what order for the recovery of lost data. These instructions also include steps to be followed in the untimely loss of the owner and physician of the practice.

Ralph Parker, MD
Information Security Policies and Procedures

HIPAA §164.308(7)(i) (cont'd.)

(C) ***Emergency mode operation plan*** ***(Required)***
Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.

Noting that this requirement is specifically for the "protection of the security of electronic protected health information", a major consideration would be whether the practice will set up operations elsewhere or would the decision be made to wait until this facility was repaired and, what steps would be taken in order to be able to access patient data even if the practice wasn't currently seeing patients.

Because our EMR is in-house, if we were unable to work in our current facility, we would obtain the services of an IT contractor to take whatever precautions are necessary to see that whatever use of the EMR is available, would be in a secure environment. We would also take steps to see that if a device, capable of creating, maintaining, transmitting or receiving e-PHI, was not currently in use, it would be placed in a secure environment or taken off premises by an assigned individual.

(D) ***Testing and revision procedures*** ***(Addressable)***
Implement procedures for periodic testing and revision of contingency plans.

Our policies and procedures and all associated plans such as the contingency plan will be reviewed on an annual basis unless there is a substantial change in the environmental or operational conditions of the practice which could then require a more frequent review.

(E) ***Applications and data criticality analysis*** ***(Addressable)***
Assess the relative criticality of specific applications and data in support of other contingency plan components.

There are very few other programs that we must have other than our EMR. With a working computer, we can load the EMR program on one device, establish a secure internet connection and could then see patients in any other chosen location.

Ralph Parker, MD
Information Security Policies and Procedures

HIPAA §164.308(8)

***Standard*: Evaluation.** *Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, that establishes the extent to which an entity's security policies and procedures meet the requirements of this subpart.*

The practice will have a Security Risk Analysis performed each year and this would constitute our technical review.

On an annual basis, we will be reviewing our policies and procedures as well as any related plans. This could be performed more frequently if the practice should experience substantial environmental or operational changes. In either case, this would constitute our non-technical review.

Ralph Parker, MD
Information Security Policies and Procedures

HIPAA §164.308

Standard: *(b) (1)* ***Business associate contracts and other arrangements.*** *A covered entity, in accordance with §164.306, may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with §164.314(a) that the business associate will appropriately safeguard the information.*

(2) This standard does not apply with respect to—

(i) The transmission by a covered entity of electronic protected health information to a health care provider concerning the treatment of an individual.

(ii) The transmission of electronic protected health information by a group health plan or an HMO or health insurance issuer on behalf of a group health plan to a plan sponsor, to the extent that the requirements of §164.314(b) and §164.504(f) apply and are met; or

(iii) The transmission of electronic protected health information from or to other agencies providing the services at §164.502(e)(1)(ii)(C), when the covered entity is a health plan that is a government program providing public benefits, if the requirements of §164.502(e)(1)(ii)(C) are met.

(3) A covered entity that violates the satisfactory assurances it provided as a business associate of another covered entity will be in noncompliance with the standards, implementation specifications, and requirements of this paragraph and §164.314(a).

Our practice has Business Associate Agreements in place with all third-party entities that would create, maintain, transmit, or receive patient data on our behalf.

(4) ***Implementation specifications: Written contract or other arrangement (Required)***
Document the satisfactory assurances required by paragraph (b)(1) of this section through a written contract or other arrangement with the business associate that meets the applicable requirements of §164.314(a).

We utilize a combination of the BA Agreement and the Non-Disclosure Agreements to fulfill this requirement.

Ralph Parker, MD
Information Security Policies and Procedures

§164.310 Physical safeguards.

A covered entity must, in accordance with §164.306:

(a) (1) ***Standard:*** ***Facility access controls.***
Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.

Access is determined by the individual's job function. Employees may have keys to open the office for business but all keys may not necessarily open all areas of the practice. In the event that the facility suffers a physical occurrence that makes it necessary to shut down patient operations, all employee access would be curtailed with the exception of those who might be called in to assist in the cleanup operations and to secure equipment and documentation deemed important and/or recoverable.

(2) ***Implementation specifications:***

(i) ***Contingency operations*** ***(Addressable).***
Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.

There is only the doctor and his nurse so in the event of an emergency, they would be the only ones working to restore lost data.

(ii) ***Facility security plan*** ***(Addressable).***
Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.

When an employee would become a member of our practice, we would determine not only their access rights and permissions to patient data but also their access rights to the facilities. Some employees could be granted greater access than others. No employee is allowed to add to or take company property off premises unless it is checked out with management and must be returned and its return verified with management.

§164.310 Physical safeguards **(cont'd.)**

(iii) ***Access control and validation procedures*** ***(Addressable).***

Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.

At the time of employment and subsequently as needed, management determines the job responsibility and employment hours of each workforce member. The determination is also made regarding whether or not the workforce member will be involved in the opening and/or closing of the office which will determine whether or not this individual has keys and/or codes to the office.

Only management and those granted permissions by management (i.e. an IT contractor) have access to software programs for any reason.

(iv) ***Maintenance records*** ***(Addressable).***
Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks).

We would not limit our documentation to work done strictly for security purposes. We operate in a professional building and as such, should we desire modifications to our office, we would be required to coordinate this with the landlord and the work would take place at specified times and through specified contractors. Repairs to the physical facility would primarily be the responsibility of the landlord but not without our knowledge and cooperation.

Ralph Parker, MD
Information Security Policies and Procedures

§164.310 Physical safeguards (cont'd.)

(b) ***Standard: Workstation use.***
Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information.

Only functions and programs necessary for the running of the practice are installed on company computers. Employees are not allowed to load or download programs. Any program or software that is needed will be handled by management. Computers are located strategically throughout the practice and in areas where only authorized personnel can access them and all computers require authentication before access is granted.

It is the policy of this practice that employees are not allowed to add to or delete programs on practice devices. Only persons who require specific programs in the performance of their duties are given permission to use those programs.

Work stations are used for practice business only and no personal use of company computers is allowed. There are no computers in unsecured areas where anyone other than a clinic employee can get to them. Those computers are not placed in a position or location where they can be easily viewed by patients or other non-employees.

(c) ***Standard: Workstation security.***
Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users.

No computers exist in unprotected areas of the practice. Only personnel who have been granted specific permission or assigned unique logins and passwords such as would be required to access patient data, are allowed to utilize practice programs. Computers are not placed in a position or location where they can be viewed by patients or other non-employees unattended.

Ralph Parker, MD
Information Security Policies and Procedures

§164.310 Physical safeguards (cont'd.)

(d) (1) Standard: Device and media controls.
Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility.

No devices would be moved around the facility other than laptops or tablets etc. If anyone other than management should need to carry a device out of the office, they would be required to log the device out with management and back in again when it returns.

At present, the only device that is carried out of the office is an encrypted thumbdrive that is used as a backup device. It is usually updated and carried offsite by the doctor over the weekends.

(2) ***Implementation specifications:***

(i) ***Disposal (Required)***
Implement policies and procedures to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored.

We are aware that there are multiple devices in our practice that have the ability to store patient information, even if only on a temporary basis, such as a scanner or copier. If any device that has the ability to create, maintain, transmit or receive patient data should cease to function and need to be taken out of commission, we will require that the memory unit (ex: hard drive), be removed from the device and given to management before the parent device is allowed to be taken from our facilities. We will then have the memory units appropriately destroyed and where possible, obtain documentation verifying its destruction.

(ii) ***Media re-use (Required)***
Implement procedures for removal of electronic protected health information from electronic media before the media are made available for re-use.

If the practice determines to re-purpose a piece of equipment that had previously been used to access e-PHI, but in its new function will not be required to access the EMR, before the device would be moved to that new function, the EMR software would be removed from the device and/or the hard drive would be re-formatted.

Ralph Parker, MD
Information Security Policies and Procedures

§164.310 Physical safeguards (cont'd.)

(iii) ***Accountability*** ***(Addressable).***
Maintain a record of the movements of hardware and electronic media and any person responsible therefore.

Equipment is not moved within the facility other than normal mobile devices such as laptops. Each year, we have a Security Risk Analysis which includes a location specific inventory.

(iv) ***Data backup and storage*** ***(Addressable).***
Create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment.

Equipment is not moved within the facility other than normal mobile devices such as laptops. There are multiple backups in multiple formats performed weekly. There will always be copies of e-PHI available.

Ralph Parker, MD
Information Security Policies and Procedures

HIPAA §164.312 Technical safeguards.

A covered entity must, in accordance with §164.306:

(a) (1) ***Standard: Access control.***
Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in §164.308(a)(4)

Only individuals that have been assigned unique logins and passwords would have access to patient data regardless of where it was placed.

(2) ***Implementation specifications:***

(i) ***Unique user identification*** ***(Required)***
Assign a unique name and/or number for identifying and tracking user identity.

All workforce members who must access patient data are assigned a unique login and password.

(ii) ***Emergency access procedure*** ***(Required)***
Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.

The process would be dependent on the cause and resulting effects of the occurrence.

The access procedures would be dependent on the condition of the office and the equipment used to access the EMR. The only two requirements for obtaining necessary e-PHI would be device(s) with the EMR software loaded and a device with the EMR “server” software loaded (it could be the same device accessing the patient data). If the device with the EMR “server” software loaded was other than a secondary device (PC, tablet, etc), the “server” would need to be in a secure location.

Ralph Parker, MD
Information Security Policies and Procedures

HIPAA §164.312 Technical safeguards (cont'd.)

(iii) ***Automatic logoff*** ***(Addressable).***
Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.

Our EMR has an automatic setting that will terminate access in five minutes after inactivity.

(iv) ***Encryption and decryption*** ***(Addressable).***
Implement a mechanism to encrypt and decrypt electronic protected health information.

The EMR selected by the practice is certified to meet the requirements of the Office of the National Coordinator for Health Information Technology and the HIPAA regulations as follows:

§170.210 Standards for health information technology to protect electronic health information created, maintained, and exchanged.
The Secretary adopts the following standards to protect electronic health information created, maintained, and exchanged:

(a) **Encryption and decryption of electronic health information**.

(1) **General**. A symmetric 128 bit fixed-block cipher algorithm capable of using a 128, 192, or 256 bit encryption key must be used.

(b) ***Standard*****: Audit controls.** *Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.*

The practice is a workgroup and as such does not have the functionality of a network. Management has the ability to review all activity within the EMR through various reports that can be viewed or run.

Ralph Parker, MD
Information Security Policies and Procedures

HIPAA §164.312 Technical safeguards (cont'd.)

(c) (1) ***Standard:*** ***Integrity.***
Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.

Based on levels of access, employees are not capable of modifying patient records in the EMR. Any changes or amendments made to a patient record will have a date, time and name of the person making the changes. The physician is the only user that has unlimited access to all portions of the patient records.

The EMR selected by the practice is certified to meet the requirements of the Office of the National Coordinator for Health Information Technology and the HIPAA regulations as follows:

§170.302 General certification criteria for Complete EHRs or EHR Modules.
The Secretary adopts the following general certification criteria for Complete EHRs or EHR Modules. Complete EHRs or EHR Modules must include the capability to perform the following functions electronically and in accordance with all applicable standards and implementation specifications adopted in this part:

(s) **Integrity**.

(2) **Detection**. Detect the alteration and deletion of electronic health information and audit logs, in accordance with the standard specified in §170.210(c).

Ralph Parker, MD
Information Security Policies and Procedures

HIPAA §164.312 Technical safeguards (cont'd.)

(2) ***Implementation specification:***

Mechanism to authenticate electronic protected health information (Addressable).

Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.

The EMR selected by the practice is certified to meet the requirements of the Office of the National Coordinator for Health Information Technology and the HIPAA regulations as follows:

§ 170.210 Standards for health information technology to protect electronic health information created, maintained, and exchanged.

The Secretary adopts the following standards to protect electronic health information created, maintained, and exchanged:

> **(b)** ***Record actions related to electronic health information.*** The date, time, patient identification, and user identification must be recorded when electronic health information is created, modified, accessed, or deleted; and an indication of which action(s) occurred and by whom must also be recorded.

(d) ***Standard: Person or entity authentication.***

Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.

The practice operates as a simple workgroup and as such there are no systems to verify the authentication of persons accessing the EMR. Management is exclusively responsible for assigning logins and passwords to all workforce members that must access patient records as a part of their job responsibilities. Sharing of this information is a terminable offense.

Ralph Parker, MD
Information Security Policies and Procedures

HIPAA §164.312 Technical safeguards (cont'd.)

(e) (1) ***Standard****: **Transmission security.***
Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.

The EMR selected by the practice is certified to meet the requirements of the Office of the National Coordinator for Health Information Technology and the HIPAA regulations as follows:

§170.302 General certification criteria for Complete EHRs or EHR Modules.
The Secretary adopts the following general certification criteria for Complete EHRs or EHR Modules. Complete EHRs or EHR Modules must include the capability to perform the following functions electronically and in accordance with all applicable standards and implementation specifications adopted in this part:

(s) **Integrity**.

(1) **In transit**. Verify that electronic health information has not been altered in transit in accordance with the standard specified in §170.210(c).

(2) ***Implementation specifications:***

(i) ***Integrity controls*** ***(Addressable).***
Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.

See above.

Ralph Parker, MD
Information Security Policies and Procedures

HIPAA §164.312 Technical safeguards (cont'd.)

(ii) ***Encryption*** ***(Addressable).***
Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.

Although we do not use a conventional EMR, we do have our patient data encrypted locally and also for our remote backups.

§170.210 Standards for health information technology to protect electronic health information created, maintained, and exchanged.
The Secretary adopts the following standards to protect electronic health information created, maintained, and exchanged:

(a) **Encryption and decryption of electronic health information**.

(1) **General**. A symmetric 128 bit fixed-block cipher algorithm capable of using a 128, 192, or 256 bit encryption key must be used.