## TABLE OF CONTENTS

### SECTION 1: INTRODUCTION TO THE SECURITY RULE 1
- Overview of the Security Rule 1
- Security Controls 2
- Security Rule Principles 2
- The Security Officer 4
- Definitions 5

### SECTION 2: UNDERSTANDING THE SECURITY RULE 6
- What does the rule do? 6
- Where do I start? 6
- Policies and Procedures 7
- Documentation Requirements 8
- Understand Your Information System 8
- Security Rule Safeguards 8
- Seven Steps to Security Compliance 11

### SECTION 3: HIPAA SECURITY PLAN INTRODUCTION 12

#### ADMINISTRATIVE SAFEGUARDS
- Standard #1: Assigned Security Responsibility 13
- Standard #2: Security Management Process 13
- Standard #3: Workforce Security 15
- Standard #4: Information Access Management 16
- Standard #5: Security Awareness Training 17
- Standard #6: Security Incident Procedures 19
- Standard #7: Contingency Plan 20
- Standard #8: Evaluation 22
- Standard #9: Business Associate Contracts 22

#### PHYSICAL SAFEGUARDS
- Standard #1: Facility Access Controls 24
- Standard #2: Workstation Use 25
- Standard #3: Workstation Security 26
- Standard #4: Device and Media Controls 26

#### TECHNICAL SAFEGUARDS
- Standard #1: Access Control 29
- Standard #2: Audit Controls 30
- Standard #3: Integrity 31
- Standard #4: Person or Entity authentication 31
- Standard #5: Transmission Security 32

#### ORGANIZATIONAL STANDARDS
- Standard #1: Policies and Procedures 33
- Standard #2: Documentation 33
DISTRICT HEALTH DEPARTMENT

HIPAA SECURITY

Section 1: Introduction to the Security Rule

OVERVIEW OF THE SECURITY RULE

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires physicians and other healthcare providers who conduct electronic transactions to adopt certain security measures to safeguard protected health information (PHI) in electronic form. The Security Rule compliments the HIPAA Privacy and Transaction Rules. Security affords safeguards for confidentiality; but security is more than confidentiality. Security also ensures that the data you transmit or receive are not altered in the process and that the data in your information systems are available to you when needed. Security is as much about integrity of information and backing up information as it is about making sure information is not inappropriately used or disclosed.

The HIPAA Security Rule is comprised of 3 levels of safeguards:

- **Administrative Safeguards**
  These safeguards address our operations. They include assigning responsibility to someone for security and having policies and procedures in place to direct our security efforts.

- **Physical Safeguards**
  These safeguards include locks and keys, where computers are located, how electronic media are disposed of and generally how to make the environment safe.

- **Technical Safeguards**
  These safeguards are controls directly applied to information systems. They identify who may have access to information systems, provide access to sets of data and specific functions in systems, audit persons who have used the systems and protect the systems from malicious software.

A key premise of HIPAA’s Security Rule is to determine what safeguards are appropriate for the size and type of office you have. HIPAA requires you to perform a risk analysis to use as a “blueprint” when making decisions about what is right for you. Then you document these decisions in policies and procedures and apply the controls that you have determined are right for your practice.

The Security Rule notes that security and privacy are linked. Protecting the privacy of information depends in large part on the existence of security measures. The security standards, however, are not limited to supporting only confidentiality; they support data integrity and availability as well. Keep in mind that data that has been subjected to a security attack may be rendered incorrect or incomplete or could possibly be lost forever.

SECURITY CONTROLS
Security Controls are designed to coordinate with the Security Rule Safeguards. They will ensure the protection of the ePHI in your office and information systems. Examples of security controls that you will implement are:

- **Administrative Controls**  
  Policies, procedures, plans and practices

- **Physical Controls**  
  Door locks, environmental and media controls

- **Technical Controls**  
  Access and audit controls, authentication, integrity and transmission controls

It is the combination of all the layers that provides full security coverage. In our training of the HIPAA Security Rule, we will describe and discuss how the layers work together and identify the “best practices” relative to applying security controls (“Best practice” does not mean the most expensive; it means the practice that is the most effective and efficient).

**SECURITY RULE PRINCIPLES**

The Security Rule is based on three principles: comprehensiveness, scalability and technology neutrality.

- **Comprehensiveness**  
  This refers to the fact that the Security Rule addresses all aspects of security. This means that security measures address confidentiality, data integrity and availability.

- **Scalability**  
  This assures that the Security Rule can be effectively implemented by covered entities of all types and sizes.

- **Technology neutrality**  
  This means the Security Rules does not define specific technology requirements, thereby allowing covered entities to make use of future technology advancements.

**Comprehensive**

The Privacy Rules is pervasive and impacts virtually every aspect of operations. The Security Rule is even more pervasive. It must be understood and practiced by every person in the office.

Privacy and Security are tightly linked. The following chart shows the similarities between the Privacy and Security standards.

<table>
<thead>
<tr>
<th>Privacy Standard</th>
<th>Complementary Security Standard</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimum Necessary</td>
<td>Information Access Management Access Controls</td>
</tr>
<tr>
<td>Verification of Identity and Authority</td>
<td>Person or Entity Authentication</td>
</tr>
<tr>
<td>Sanction Policy</td>
<td>Sanction Policy</td>
</tr>
<tr>
<td>Training</td>
<td>Training</td>
</tr>
<tr>
<td>----------</td>
<td>----------</td>
</tr>
<tr>
<td>Business Associate Contracts</td>
<td>Business Associate Contracts</td>
</tr>
<tr>
<td>Policies and Procedures</td>
<td>Policies and Procedures</td>
</tr>
<tr>
<td>Privacy Compliance Officer</td>
<td>Security Compliance Officer</td>
</tr>
<tr>
<td>Uses and Disclosures consistent with NPP</td>
<td>Information System Activity Review</td>
</tr>
<tr>
<td>Complaints to the Covered Entity</td>
<td>Evaluation</td>
</tr>
<tr>
<td></td>
<td>Incident Procedures</td>
</tr>
<tr>
<td>Safeguards</td>
<td>Facility Access Controls</td>
</tr>
<tr>
<td></td>
<td>Workstation Security</td>
</tr>
<tr>
<td></td>
<td>Device and Media Controls</td>
</tr>
</tbody>
</table>

The Security Rule is not just about technical controls; it is about people doing what they are supposed to do. It is focused on PHI when it is maintained in our computer system and as it is transmitted throughout an internal or external network or in any other “electronic media”. The Security rule standards safeguard ePHI from unauthorized access, alteration, deletion and transmission.

** Scalable**

You should be able to fit the Security Rule to your needs – whether you have a small office or a large clinic. The Security Rule emphasize being reasonable and appropriate.

**Reasonable and Appropriate**

The Security Rule specifically provides factors to be considered when determining which security measures to be used. These measures are:

- Size, complexity, and capabilities
- Technical infrastructure, hardware, and software security capabilities
- Costs of security measures
- Probability and criticality of potential risks to ePHI

The Security Rule cautions that the cost is not meant to free covered entities from the adequate security measures responsibility.

**Risk Analysis and Risk Management**

The Security Rule specifies that you must conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity and availability of ePHI our practice holds and implement security measures that are reasonable and appropriate to reduce risks and vulnerabilities to an acceptable level.

**Technology Neutral**
The concept of technology neutrality is based on the fact that information technology changes very rapidly. A technology neutral standard allows the Security Rule to be stable, yet flexible enough to take advantage of the newest technologies available.

**THE HIPAA SECURITY OFFICER**

The HIPAA Information Security Officer (or Data Management Coordinator) serves as the process director for all ongoing activities that serve to provide appropriate access to and protect the confidentiality of patient, provider, employee and business information in compliance with the practice policies and standards.

The position responsibilities include, but are not limited to:

- Ensures that our information systems comply with all applicable federal laws and regulations.
- Ensures that none of our information systems compromises the confidentiality, integrity, or availability of any other of our information systems.
- Develops documents and ensures proper dissemination of appropriate security policies, procedures, and standards for the users and administrators of our information systems and the data contained within them.
- Ensures that any of our newly acquired information systems have features that support required and/or addressable Security Rule implementation Specifications.
- Coordinates the selection, implementation, and administration of our security controls.
- Ensures that our workforce members receive regular security awareness training.
- Conducts periodic Risk Analysis of our information systems and security processes.
- Develops and implements an effective Risk Management program.
- Regularly monitors and evaluates threats and risks to our information systems that contain ePHI.
- Develops and monitors/audits records of our information systems’ activity to identify inappropriate activity.
- Maintains an inventory of all of our information systems that contain ePHI.
- Creates an effective security incident policy and related procedures.
- Ensures adequate physical security controls exist to protect our ePHI.
- Coordinates with our Privacy (Compliance) Officer to ensure that security policies, procedures and controls support compliance with the HIPAA Privacy Rule.
- Evaluates new security technologies that may be appropriate for protecting our information systems that contain ePHI.

**DEFINITIONS**

**Access** means the ability or the means necessary to read, write, modify, communicate data/information or otherwise use any system resource. (Not the same meaning of “access” in the Privacy Rule.
**Authentication** means the corroboration that a person is the one claimed.

**Availability** means that data or information is accessible and usable upon demand by an authorized person.

**Confidentiality** means that data or information is not made available or disclosed to unauthorized persons or processes.

**ePHI** means protected health information that is stored, maintained or transmitted in electronic form.

**Encryption** means the use of a process to transform data into a form in which there is a low probability of assigning meaning without the use of a confidential key.

**Information system** means an interconnected set of information resources under the same direct management control that shares common functionality.

**Integrity** means that data or information have not been altered or destroyed in an unauthorized manner.

**Malicious software** means software, for example, a virus, designed to damage or disrupt a system.

**Password** means confidential authentication information composed of a string of characters.

**Security incident** means the attempted or successful unauthorized use, disclosure, modification, or destruction of information or interference with system operations in an information system.

**User** means a person or entity with authorized access.

**Workstation** means an electronic computing device, for example, a laptop or desktop computer and electronic media stored in its immediate environment.
Section 2: Understanding the Security Rule

WHAT DOES THE RULE DO?

The stated purpose of the HIPAA Security Rule is to secure Protected Health Information (PHI) transmitted, stored, or maintained in electronic format only.

What the Rule does:

- Ensures the confidentiality, integrity, and availability of all ePHI that you create, receive, maintain, or transmit.
- Protects against any reasonable anticipated threats or hazards to the security or integrity of such information.
- Protects against any reasonable anticipated uses or disclosures of such information that are not permitted or required.
- Ensures compliance by your workforce.

In General:

- Focuses more on “what” needs to be done, rather than “how”.
- Cost, size, technical infrastructure and criticality of potential risks are factors, allowing for a flexible approach.
- Requires “incident response” to identify an intrusion and respond quickly.
- Results and documentation both are important.

The standards are grouped into 3 groups:

- Administrative Safeguards
- Physical Safeguards
- Technical Safeguards

The standards explain what must be done, implementation specifications explain how.

WHERE DO I START?

It is important to understand exactly what the specific requirements of the Security Rule are and how each provision needs to be addressed. The rule provides a number of “standards” and “implementation specifications”. These are divided into the three categories already discussed: administrative safeguards, physical safeguards, and technical safeguards. There are also two organizational requirements.

Standards

A “standard” is a general requirement that must be complied with by our practice. An example standard is “contingency planning”. It states that our practice must have contingency plans in case of emergencies or disasters. This is a general requirement.

Implementation Specifications

An “implementation specification” is a more detailed and specific description of the method or approach that your practice can use to meet a particular standard. For example, under contingency planning, there are five implementation specifications that provide specific direction on how to proceed. These include a data back up plan, emergency mode operations plan, testing
and revision procedure, and applications and data criticality analysis. Not all standards have implementation specifications.

**Required or Addressable**
The implementation specifications are either **Required (R)** or **Addressable (A)**. The specifications listed as **required** we **must do**. In the case of the addressable specifications, we **must address** and determine whether that specification applies to our practice and what action needs to be taken to implement that specification. All of these actions and determinations **must be documented**. In the case of addressable specifications, we may consider the cost of implementing a certain specification, but may not use cost alone as a reason not to implement it if it is necessary.

Security Implementation Specifications are either:

- **Required** – You must implement the specification as stated.
- **Addressable** – You may:
  - Implement the specifications as stated,
  - Implement an alternative that you believe suits your office better, or
  - Address the standard in another way because the implementation specification is not applicable to your situation.

Always remember, every standard is required. Just because a standard contains only addressable implementation specifications does not mean you can ignore it. **Addressable does not mean “not required” nor does it mean “optional”**. It means we must address the specification in some way or address the standard itself in some way. The purpose of this feature of the Security Rule is to ensure that it is, as already stated, comprehensive, scalable, and technology neutral.

**POLICIES AND PROCEDURES**

HIPAA Security **requires** our practice to develop a complete set of policies and procedures to document that we are meeting the requirements of the rule. The requirement to implement policies and procedures is flexible and scalable to reflect our needs. Keep in mind that all standards and all implementation specifications **must be considered**, even if we have determine not to move forward with a particular stand or specification.

**Policies** – HIPAA does not define the term “policy”, nor does it specify the content of policies. Rather, it relies on standard business practices for policy development.

The purpose of a policy is to:

- Guide members of the workforce in taking actions that is consistent with legal, ethical and organizational requirements.
- Conform to applicable laws and the requirements of licensing and accrediting agencies.
- Reflect the mission and culture of the organization.
- Establish measurable objectives and expectations for everyone within the organization.
- Assign responsibility for decision-making and a frame of reference for action.
- Define enforcement and consequences for violations.

**Procedures** – HIPAA does not define the term “procedure” either. Procedures are understood to be explicit, step-by-step instructions that implement the organization’s policies.
Procedures, with respect to an action, explain:

- What is to be done.
- When it is to be done.
- Where it is to be done.
- Who is to do it.
- Exactly how it is to be done.

The Van Buren/Cass District Health Department expects all employees to follow any and all policies written. Anyone found in violation will be reprimanded, up to and including, termination.

**DOCUMENTATION REQUIREMENTS**

Both the HIPAA Privacy and Security Rules require us to document policies and procedures to ensure compliance. These policies, procedures and processes must be documented and may be written or in electronic form. A healthcare practice may change its policies and procedures at any time, provided that the changes are documented and implemented in accordance with the Security Rule.

The Rules require that the documentation must be kept for a minimum of 6 years and be made available to those persons responsible for implementing the procedures to which the documentation pertains and to those persons who will be conducting compliance investigations. The Rules also require the documentation to be reviewed periodically, and updated as needed, in response to environmental or operational changes affecting the security of PHI. All documentation must be securely stored and maintained.

**UNDERSTAND YOUR INFORMATION SYSTEMS**

Our Security Compliance Officer will identify the information systems that are used to create, receive, maintain or transmit ePHI. An inventory has been compiled as part of our analyzing information flow to meet the necessary requirements for the HIPAA Privacy Rule. Our Security Compliance Officer formally explores and documents the systems’ security features. He/she may also decide to apply the security controls not only to ePHI systems but also to other information systems such as general ledger and payroll systems.

**SECURITY RULE SAFEGUARDS**

Security Rule Safeguards include the following:

**Administrative Safeguards** – are administrative actions, and policies and procedures for the management of security measures and to manage the conduct of our workforce both in relation to the protection of electronic protected health information (ePHI).

**Security Management Process** – are policies and procedures to prevent, detect, contain and correct security violations, done by conducting a Risk Analysis, Risk Management, apply Sanction Policies and conduct an Information System Activity Review.

**Assigned Security Responsibility** – identify and assign a security official who is responsible for the development and implementation of our policies and procedures impacted by the Security Rule.
**Workforce Security** – means to implement policies and procedures to ensure that all members of our workforce have appropriate access to ePHI through Authorization and/or Supervision; Workforce Clearance Procedures and Terminations Procedures.

**Information Access Management** – means the implementation of policies and procedures for authorizing access to ePHI through Access Authorization and Access Establishment and Modification.

**Security Awareness and Training** – means to implement a security and awareness program for all members of our workforce through Security Reminders, Protection from Malicious Software, Log-in Monitoring and Password Management.

**Security Incident Procedures** – means to implement policies and procedures to address security incidents through Response and Reporting.

**Contingency Plan** – means to establish and implement (as needed) procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure and natural disaster that damages systems that contain ePHI).

**Evaluation** – performs a periodic technical and non-technical evaluation in response to environmental or operational changes affecting the security of ePHI. This establishes the extent to which our security policies and procedures meet the requirements of the Security Rule.

**Business Associate Contracts and Other Arrangements** – means that we may permit a business associate to create, maintain, or transmit ePHI on our behalf only if we obtain satisfactory assurances that the business associate will appropriately safeguard the information through a written contract or other arrangement.

**PHYSICAL SAFEGUARDS**

**Physical Rule Safeguards:** are physical measures, policies and procedures created to protect our electronic information systems and related buildings and equipment from natural and environmental hazards and unauthorized intrusion.

**Physical Safeguards include:**

**Facility Access Controls** – means to implement policies and procedures to limit physical access to our electronic information systems and the facility in which they are housed, while ensuring that properly authorized access is allowed. This is done through Contingency Operations, Facility Security Plan, Access Control and Validation and Maintenance Records.

**Workstation Use** – means to implement policies and procedures that specify the proper physical attributes of the surrounding workstation that can access ePHI.

**Workstation Security** – means to implement physical safeguards for all workstations that access ePHI, to restrict access to authorized users.

**Device and Media Controls** – means to implement policies and procedures that govern the receipt and removal of the hardware and electronic data that contains ePHI into and out of a facility and the movement of these items within the facility by way of Disposal, Media Re-use, Accountability and Data Backup Storage.
TECHNICAL SAFEGUARDS

Technical safeguards mean the technology and the policy and procedures for its use that protect ePHI and control access to it.

Technical Safeguards include:

**Access Control** – means to implement technical policies and procedures for electronic information systems that maintain ePHI to allow access only to those persons or software programs that have been granted access rights. This is done through Unique User Identification, Emergency Access Procedures, Automatic Logoff and Encryption and Decryption.

**Audit Controls** – means to implement hardware, software and/or procedural mechanisms that record and examine activity to information systems that contain or use ePHI.

**Integrity** – means to implement policies and procedures to protect ePHI from improper alternation or destruction by the implementation of electronic mechanisms to authenticate ePHI.

**Person or Entity Authentication** – means to implement procedures to verify that a person or entity seeking access to ePHI is the one claimed.

**Transmission Security** – means to implement technical security measures to guard against unauthorized access to ePHI that is being transmitted over an electronic communications network through Integrity Controls and/or Encryption.
SEVEN STEPS TO SECURITY COMPLIANCE

1. **Understand the rules**
   Review the regulations and learn about security controls

2. **Assign responsibility**
   Appoint a Security Officer

3. **Make a list of your ePHI**
   Identify your information systems

4. **Conduct a Risk Analysis**
   Assess vulnerabilities and threats to ePHI
   Prioritize risks
   Identify security measures

5. **Implement Policies and Procedures**
   Documents all policies and procedures
   Document method to address security policies
   Select security controls to match the policies

6. **Deliver a security awareness training program**
   Train all employees and document training
   Conduct initial and ongoing training (at least annually)

7. **Monitor ongoing security progress**
   Audit, monitor and test security programs
   Integrate privacy complaints and security incidents
Section 3: HIPAA Security Plan Introduction

The HIPAA Security rule is comprised of 3 levels of safeguards:

- Administrative Safeguard
- Physical Safeguards
- Technical Safeguards

(Please review guidelines to get better understanding of what these entail)

Standards are a requirement of this agency and must be complied with. This is done through implementation specifications. Implementation Specifications can be either Required and/or Addressable. Below are our Administrative, Physical and Technical Safeguard policies and procedures. Anyone found in violation of these policies and procedures will be reprimanded, up to and including, termination.

As part of HIPAA Security training, employees are asked to review these guidelines and our HIPAA Security Plan. **After review of these documents, employees must download the acknowledgment page and return to the Administrative Assistant for filing.** These acknowledgment pages are used to determine who is in compliance with this requirement and are used for documentation of training.
ADMINISTRATIVE SAFEGUARDS

STANDARD #1: Assigned Security Responsibility (Required)

Policy
The purpose of our information Security Officer is to protect the confidentiality, integrity and availability of our information systems and ePHI. Our information Security Officer leads our office and is responsible for the development and implementation of all policies and procedures necessary to appropriately protect the confidentiality, integrity and availability of our information systems and ePHI.

Procedure
Our information Security Officer is the same individual as our Data Management Coordinator.

---

STANDARD #2: Security Management Process

Policy
We must ensure the confidentiality, integrity and availability of our information systems containing ePHI (received or created by us) by implementing appropriate and reasonable policies, procedures and controls to prevent, detect, contain and correction violations. All of our workforce members are responsible for appropriately protecting ePHI contained on our information systems from unauthorized access, modification, destruction and disclosure.

- IMPLEMENTATION SPECIFICATIONS

Risk Analysis (Required)

Policy
We must regularly identify, define and prioritize risks to the confidentiality, integrity and availability of our information systems containing ePHI.

Procedure
We have identified and examined each information system in our office for threats and vulnerabilities that could cause harm to our equipment and data. We have prioritized the possible threats and vulnerabilities (See our Environmental, Facility and Hardware and Software risk Analysis)

Risk Management (Required)

Policy
We must implement security measures that reduce the risks to our information system containing ePHI to reasonable and appropriate levels.

Procedures
We have selected and implemented security measures based on our risk analysis process in order to protect our information systems, equipment and data from any natural or other type of threat.

Sanction Policy (Required)
**Policy**
Our workforce members must comply with all of our applicable security policies and procedures or discipline action will be taken as shown below:

As an employee of our practice you must understand that the examples below are given as examples only and that there are other violations of HIPAA law that will be followed by disciplinary action. Disciplinary action is also dependent upon many variables, sanctions will be commensurate with the severity of non-compliance with our security policies and procedures on a case-by-case basis. The identification and definition of such sanctions will occur with the appropriate involvement of our Compliance and/or Security Officer, Immediate Supervisor and possibly legal counsel. All actions will be documented.

All employees must report suspected or known workforce members who are non-compliant with our policies and procedures. Our office will not intimidate or retaliate against any individual who reports acts or practices that are unlawful, provided the individual in good faith believes that the practice is unlawful and reporting such a case is reasonable and does not disclose PHI in violation with HIPAA law. Also, sanctions will not be applied against whistleblowers or workforce member crime victims who are disclosing PHI to further their own case.

**Level #1: Accidental Breach**
Possible scenarios:
Employee does not log off the computer after use or at the end of the day. If employee is away from desk for short time and does not want to sign off, must have a password protected screen saver.
Employee faxes the wrong PHI to another practice.
Employee forgets to get a signed acknowledgment of receipt of the NPP (Notice of Privacy Practices). This does not include those NPPs that are mailed to clients but are not returned, these can be noted in the client’s chart.
Employee forgets to remove all PHI from desk at end of day (unless desk in room that locks).

Sanction:
Warning & Re-Education
Verbal warning documented in the employee’s file and mandatory re-education for the first offense. Continued offenses lead to progressive discipline up to and including termination.

**Level #2: Intentional Breach without Harmful or Dishonest Intentions**
Possible scenarios:
Employee emails PHI to the wrong email address and without the disclaimer. (This agency does not allow client information to be emailed at this time).
Viewing patient records out of curiosity.
Sharing PHI because the information is interesting (not for treatment purposes).
Employee shares computer password.
Discussing patient information in an unsecured area.

Sanction:
Written Warning & Re-Education, Possible Suspension
Written Warning documented in the employee’s file and mandatory re-education for the first offense. Continued offenses lead to progressive discipline up to and including suspension or termination.

**Level #3: Willful or Intentional Breach with Harmful or Dishonest Intentions.**
Possible scenarios:
Using PHI (personal health information) for personal gain (marketing without authorization).
Using PHI to cause harm (exposing information to unauthorized individuals because of dislike for the owner of the PHI).
Gives access to a restricted area to an unauthorized individual.
Gives access to PHI to an unauthorized individual

Sanction:
Termination
Termination and possible legal action.

Procedure
We have a sanction policy that applies to our entire workforce. The sanctions are commensurate with the severity of non-compliance with our security policies and procedures. We provide regular security training and awareness for our workforce members to help prevent any non-compliance of our security policies and procedures.

Information System Activity Review (Required)

Policy
We must regularly review records of activity on information systems containing ePHI. Appropriate hardware, software or procedural auditing mechanisms must be implemented on our information systems that contain or use ePHI. Records of activity created by audit mechanisms implemented on our information systems must be reviewed regularly.

Procedure
Our Security Officer audits the activity on our information systems. Workforce members will not have access to these audits. Systems containing ePHI are only accessible by logging in with user ID information. Our HIPAA Security Officer randomly audits the information systems activity.

---

STANDARD #3: Workforce Security

Policy
Access to our information systems containing ePHI must be authorized only for our properly training workforce members having a legitimate need for specific information in order to accomplish job responsibilities. Our workforce members must not attempt to gain access to our information systems containing ePHI for which they have not been given proper authorization

- IMPLEMENTATION SPECIFICATIONS

Authorization and/or Supervision (Addressable)

Policy
We must ensure that all workforce members who can access our information systems containing ePHI are appropriately authorized to access the system or supervised when they do so. We must ensure that the confidentiality, integrity, and availability of ePHI on our information systems are maintained when its information systems are accessed by third parties.

Procedure
Our Security Officer will ensure that all of our workforce members receive specific access to specific information systems and ePHI in order to accomplish their jobs. Third parties are not
permitted access to our ePHI unless access is granted by our Security Officer and their access is supervised.

**Workforce Clearance Procedure (Addressable)**

**Policy**
The background of all of our workforce members must be adequately reviewed during the hiring process. The type and number of verification checks conducted must be based on the employee’s probable access to our information systems containing ePHI and their expected ability to modify or change such ePHI.

**Procedure**
Our Supervisors will conduct background and verification checks, if necessary, depending on ePHI access privileges, of all prospective workforce members. We will verify previous employment and check references given. We will access the Office of the Inspector General (OIG) website to verify that the person has not previously been convicted of fraudulent billing practices. We will access the Michigan State Police (MSP) to verify that the person has not previously been convicted of a crime in Michigan. We will also access the state web site to verify licenses as needed.

**Termination Procedures (Addressable)**

**Policy**
When the employment of our workforce member ends, their information systems privileges, both internal and remote, must be disabled or removed by the time of departure. When workforce members leave our employment, they must return all equipment supplied by us by the time of the employee departure, including any records in their possession. If a workforce members is to be terminated immediately, their information system privileges must be removed or disabled just before they are notified of the termination.

**Procedure**
When the employment of our workforce member ends, their information system privileges, both internal and remote, will be promptly disabled or removed by our Security Officer. They will return all equipment supplied by us by the time of their departure. If a workforce member is to be terminated immediately, their information system privileges will be removed or disabled just before they are notified of the termination.

---

**STANDARD #4: Information Access Management**

**Policy**
Our workforce members must not be allowed access to information systems containing ePHI until properly authorized. Access to our information systems containing ePHI must be authorized only for our workforce members having a specific need for specific information in order to accomplish a legitimate task. Our workforce members must not attempt to gain access to our information systems containing ePHI for which they have not been given proper authorization.

- IMPLEMENTATION SPECIFICATIONS

Access Authorization (Addressable)
Policy
Our workforce members are not allowed access to information systems containing ePHI until properly authorized. Access to our information systems containing ePHI is authorized only for our workforce members having a specific need for specific information in order to accomplish a legitimate task. Our workforce members may not attempt to gain access to our information systems containing ePHI for which they have not been given proper authorization.

Procedure
Our Security Officer will assess each job in our office and then authorize proper access to our information systems containing ePHI for each of our workforce member. This access will be granted according to the specific need for the employee to accomplish a legitimate task.

Access Establishment and Modification (Addressable)

Policy
Only properly authorized and trained workforce members may access our information systems containing ePHI. Our Security Officer must review this access regularly. Access to our information systems containing ePHI is limited to our workforce members who have a need for specific ePHI in order to perform their job responsibilities. Our workforce members do not provide access to our information systems containing ePHI to unauthorized persons.

Procedure
Our Security Officer will review and establish workforce access to our information systems and ePHI. This access will be reviewed annually and modified if necessary. Our workforce members will not provide access to unauthorized persons.

---

STANDARD #5: Security Awareness and Training

Policy
All workforce members, both remote and onsite, must be provided with sufficient regular training and supporting reference materials to enable them to appropriately protect our information systems. After training has been conducted, each workforce member must verify that he or she has received the training by signing an acknowledgment form(s) stating they understand the material presented, and agrees to comply with it. All new employees must receive appropriate security training before being provide with access or accounts on our information systems.

• IMPLEMENTATION SPECIFICATIONS

Security reminders (Addressable)

Policy
We must make certain that all of our workforce members, including those who work in a remote location, are regularly reminded of information security risks and how to follow our security policies. In addition to providing regular information security awareness, we must provide security information and awareness to all our workforce members when a security incident occurs. Such information may be provided at our facility or through remote methods.
**Procedure**
On an ongoing basis, our HIPAA Security Officer will notify all of our workforce members, including those in remote locations, of information security risks and procedures and how to follow them. All workforce members will be provided with information on how to use our information systems in ways to minimize possible security risks.

**Protection From Malicious Software (Addressable)**

**Policy**
We must develop, implement, and regularly review a formal, documented process for guarding against, detecting and reporting malicious software that poses a risk to our information systems and data. All of our workforce members must be regularly trained and reminded about this process. Unless appropriately authorized, our workforce members must not bypass or disable anti-virus software.

**Procedure**
Our HIPAA Security Officer is responsible for obtaining appropriate software to detect malicious software, viruses, worms, and malicious codes that might affect our information systems containing ePHI. S/he will train our workforce members regarding this software’s use. Our workforce members will not bypass or disable it without proper authorization from our HIPAA Security Officer.

**Log-in Monitoring (Addressable)**

**Policy**
We must develop, implement, and regularly review a formal, documented process for monitoring log-in attempts and reporting discrepancies. All of our workforce members must be regularly trained and reminded about this process. Access to all of our information systems must be through a secure log-in process.

**Procedure**
Access to all of our information systems must be through a secure log-in process. All attempts to log-in to our information systems containing ePHI will be monitored for any discrepancies. This will show if unauthorized persons are attempting to access ePHI. Our HIPAA Security Officer will monitor and document any discrepancies.

**Password Management (Addressable)**

**Policy**
We must develop, implement and regularly review a formal documented process for appropriately creating, changing and safeguarding passwords used to validate a user’s identity and establish access to our information systems and data. All of our workforce members must be regularly trained and reminded about this process.

**Procedure**
Our HIPAA Security Officer trains and reminds our workforce members about our process for creating, changing and safeguarding passwords used to validate a user’s identity to access our information systems. Passwords will be changed from time to time and must not be shared with
anyone else or ever displayed in open view. No workforce member may request another employee to reveal their password.

---

**STANDARD #6: Security Incident Procedures**

**Policy**
All of our actions to respond to and recover from security incidents must be carefully and formally controlled. Our workforce members must report any observed or suspected security incidents as quickly as possible through our security incident procedure. Our Compliance Officer is authorized to investigate any and all alleged violations of our security policies, and to take appropriate action to mitigate the infraction and apply sanctions as warranted.

- **IMPLEMENTATION SPECIFICATION**

**Response and Reporting (Required)**

**Policy**
We must provide notification, damage control and problem correction services when a security incident occurs. We must create and document a formal security incident reporting procedure, which must be regularly reviewed and revised as necessary. We must provide our workforce members with an easy to use and effective process for reporting security incidents. All of our workforce members must be regularly made aware of this process. A workforce member must not prevent another member from reporting a security incident.

**Procedure**
Our HIPAA Security Officer is prepared to receive any and all reports of suspected or known security incidents and to respond accordingly. S(he) will notify all employees if a security incident occurs, and ensure that our information systems containing ePHI have not been compromised. S(he) will collect all pertinent evidence regarding each security incident. Our HIPAA Compliance Officer will provide appropriate retraining for all employees, if necessary.

Our security incident reporting procedures are as follows:

- Identify suspected or known security incidents
- Report security incidents to the HIPAA Security and/or Compliance Officer
  1) Response to a security incident includes:
     a) Preservation of evidence, if applicable,
     b) Correction of the situation that caused the incident,
     c) Mitigation of any harmful effects
- Document security incidents and their outcomes,
- Evaluate security incidents as part of ongoing risk management.

---

**STANDARD #7: Contingency Plan**

**Policy**
Our disaster and emergency response process must reduce the disruption to our information systems to an acceptable level through a combination of preventive and recovery controls and processes. Such controls and processes must identify and reduce risks to our information systems, limit damage caused by disaster and emergencies and ensure the timely resumption of
significant information systems and processes. Such controls and processes must be commensurate with the value of the information systems being protected or recovered.

- **IMPLEMENTATION SPECIFICATIONS**

**Data Backup Plan (Required)**

**Policy**
Backup copies of all ePHI on our electronic media and information systems must be made regularly. This include both ePHI received and created by us. We must have an adequate backup system that ensures that all ePHI can be recovered following a disaster or media failure. Backups of ePHI must be stored in a secure remote location at a sufficient distance from the facility to escape damage from a disaster at or near our facility. Restoration procedures must be regularly tested to ensure that they are effective and that they can be completed within the time allotted in our disaster recovery plan.

**Procedure**
Our HIPAA Security Officer is responsible for ensuring the weekly, monthly and annual backup of our data. These backup copies are stored at a secure remote location. Our HIPAA Security Officer regularly tests restoration procedures for our electronic media and information systems containing ePHI.

**Disaster Recovery Plan (Required)**

**Policy**
We must create and document a disaster recovery plan to recover our information systems if they are impacted by a disaster. The plan must be reviewed annually and revised as necessary. Our workforce must receive regular training on our disaster recovery plan. Our workforce members must be made aware of where our current copies of our plan are kept on site as well as off-site.

**Procedure**
Our Disaster Recovery Plan establishes procedures to restore any loss of ePHI. Two copies of this plan are readily accessible in our primary office (one in Administration and one in Data Management Coordinator’s office). Another copy is kept off-site at our Paw Paw facility.

Our security incident reporting procedures are as follows:
- Identify suspected or known security incidents
- Report security incidents to the HIPAA Security and/or Compliance Officer
  1. Response to a security incident includes:
     a) Preservation of evidence, if applicable,
     b) Correction of the situation that caused the incident,
     c) Mitigation of any harmful effects
- Document security incidents and their outcomes
- Evaluate security incidents as part of ongoing risk management.

**Emergency Mode Operation Plan (Required)**

**Policy**
We must have a formal, documented emergency mode operation plan for protecting our information systems containing ePHI during and immediately after a crisis situation. Our workforce members must receive regular training and awareness on our emergency mode operation plan.
Procedure
Our Emergency Mode Operation Plan establishes procedures that will enable us to continue critical business processes for the security of our ePHI while operating in emergency mode.

In an event of an emergency, we will implement this Plan. Following is a list of ways we can be prepared for an emergency incident.

1. We will have printed our appointment lists, encountered forms (with balance forward) and medical record chart “pull” lists for the next day.
2. We will print extra blank encounter forms and have them available for use.
3. We will hand-write in appointments that are added while our system is down.
4. We will use a manual payment log to record receipts of cash, checks, and credit cards including account numbers.
5. We will utilize laptops and/or notebook PCs with charged spare batteries, if necessary, for secondary versions of ePHI.
6. When our system is restored, we will enter the data records on hard copies into our information systems.

Testing and Revision Procedures (Addressable)

Policy
Under the direction of our HIPAA Security Officer, we must conduct regular testing of our contingency plan to ensure that it is current and operative. We must have a formal process defining how and when our plan will be tested. The contingency plan must be revised as necessary to address issues or gaps identified in the testing process. Our contingency plan must be kept current.

Procedure
Our HIPAA Security Officer will direct the testing of our contingency plan on an annual basis. Revisions to the plan will be made, as necessary, to address issues or gaps identified by the testing process. In cases where security incidents occur that warrant immediate changes in our plan, we will test our contingency plan and make the proper changes to remedy the security problem.

Application and Data Criticality Analysis (Addressable)

Policy
We must have a formal, documented process for defining and identifying the criticality of our information systems and the data contained within them. The prioritization of our information systems must be based on an analysis of the impact to our services, processes and business objectives if disaster or emergencies cause specific information systems to be unavailable for particular period of time. This criticality analysis must be conducted at least annually.

Procedure
This implementation specification is addressable. We have addressed its requirements and have determined that it is addressed elsewhere in this plan. (See Standard #2 “Risk Analysis” and “Risk Management”).
STANDARD #8: Evaluation (Required)

Policy
We must regularly conduct a technical and non-technical evaluation of our security controls and processes to document our compliance with our security policies and the HIPAA Security Rule. All appropriate areas and employees within our practice must be included in the evaluation. After the initial evaluation, we must conduct a thorough technical and non-technical evaluation of our security controls and processes when environmental or operational changes occur which significantly impact our ePHI. This evaluation must be conducted annually.

Procedure
Our HIPAA Security Officer will direct the testing of our contingency plans on an annual basis. Revision to the plan will be made, as necessary, to address issues or gaps identified by the testing process. Our HIPAA Security Officer will document the results of such tests. In cases where security incidents occur that warrant immediate changes in our plan, we will test our contingency plan and make the proper changes to remedy the security problem. Our HIPAA Security Officer will keep our plan current.

---

STANDARD #9: Business Associate Contracts (Required)

Policy
When another entity is acting as a business associate of our practice, the business associate must appropriately and reasonably protect the ePHI that it creates, receives, maintains or transmits on our behalf. We will permit a business associate to create, receive, maintain or transmit ePHI on our behalf only if there is a written agreement between the two parties which ensures that the business associate will appropriately and reasonably safeguard the information. We must make a good faith attempt to obtain satisfactory assurances that the business associate will safeguard our ePHI as required by the business associate contract and to document the attempt and the reasons if these assurances cannot be obtained.

Procedure
Our Compliance Office will obtain a signed business associate agreement with companies or persons we hire to handle ePHI on our behalf. This business associate agreement will have proper and appropriate language mandated by the HIPAA Privacy and Security Rules. These contracts will be securely maintained.
PHYSICAL SAFEGUARDS

STANDARD #1: Facility Access Controls

Policy
We must protect the confidentiality, integrity and availability of our information systems by preventing unauthorized physical access, tampering and theft to the systems and to the facility in which they are located, while ensuring that properly authorized access is allowed. Our information systems containing ePHI must be physically located in areas where unauthorized access is minimized. We must perform an annual inventory of all physical access controls used to protect the information systems at our office. The perimeter of the building or site containing our information systems containing ePHI must be physically sound and all external doors must have appropriate protections against unauthorized access. Doors and windows should be locked when unattended. External protection should be considered for windows, particularly at ground level.

• IMPLEMENTATION SPECIFICATIONS

Contingency Operations (Addressable)

Policy
We must ensure that, in the event of a disaster or emergency, appropriate persons can enter our office to take necessary actions defined in our Disaster Recovery and Emergency Mode Operations Plans. We must ensure that authorized employees can enter the office to enable continuation of processes and controls that protect ePHI while we are operating in emergency mode. These individuals will have keys made available to them so they can have access to any part of our facility at any given time.

Procedure
This implementation specification is addressable. We have addressed its requirements and have determined that is addressed elsewhere in our plan.

Facility Security Plan (Addressable)

Policy
We must protect our information systems by preventing physical access, tampering and theft. We must maintain and regularly review a formal, documented facility security plan that describes how our office and equipment will be appropriately protected. All appropriate workforce members must have a current copy of the plan. An appropriate number of current copies of the plan must be maintained off-site.

Procedure
This implementation specification is addressable. We have addressed its requirements and have determined that it is addressed elsewhere in our plan (See Standard #2 “Risk Analysis” and “Risk management”).

Access Control and Validation (Addressable)
**Policy**
Access rights to areas where ePHI is kept should be given only to workforce members who have a need for specific physical access in order to accomplish a legitimate task. Our workforce members must not attempt to gain physical access to sensitive areas containing information systems having ePHI or software programs that can access ePHI for which they have not been given proper authorization. All visitors to sensitive areas of our office must show proper identification, state reason for need to access and sign in prior to gaining access.

**Procedure**
This implementation specification is addressable. We have addressed its requirements and have determined that it is addressed elsewhere in our plan (See Standard #3 “Authorization and/or Supervision” and “Access Authorization”). Visitors that need access to building, (i.e. repairmen, salesperson and family members) will check in at the front desk of our facility. Front desk will check to see if individual needs access into building by contacting the employee the visitor wants to see. If determined that access is needed and/or required to accomplish a legitimate task, they will be asked to see proper ID and/or business card, sign visitor log stating time in and purpose of visit, and instructed to sign out when leaving the facility. Each visitor will receive a Visitor’s badge and/or have an employee escort. Family members and/or friends will not be allowed into a personal work area unless all PHI is either covered or removed.

**Maintenance Records (Addressable)**

**Policy**
We must document all repairs and modifications to the physical components of our office that are related to security of ePHI. We must conduct an annual inventory of all of the physical components of our office that are related to the protection of ePHI. Inventory results must be documented and stored in a secure manner (e.g. on a computer with appropriately filed access permissions or in a locked drawer). Repairs or modifications to any physical component listed in the above inventory must be documented.

**Procedures**
This implementation specification is addressable. We have addressed its requirements and have determined that it is addressed elsewhere in our plan. (See Standard #2 “Risk Analysis” and “Risk Management”).

---

**STANDARD #2: Workstation Use (Required)**

**Policy**
Workforce members must not use our workstations to engage in any activity that is either illegal under local, state, federal or international law or is in violation of our policies. Access to all of our workstations containing ePHI must be controlled with a username and password or an access device such as a token. All password-based access control systems on our workstations must mask, suppress, or otherwise obscure the passwords so the unauthorized persons are not able to observe them. Our workforce members must not share passwords with others. If a workforce member believes that someone else is inappropriately using a user-ID or password, they must immediately inform our HIPAA Compliance Officer. Our workstations containing ePHI must be physically located in such a manner as to minimize the risk that unauthorized individuals can gain access to them. The display screen of all of our workstations containing ePHI must be positioned such that information cannot be readily viewed through a window, by persons walking in a hallway, or by persons waiting in reception, public or other related areas. Security
screens must be purchased if necessary. Our workforce members must activate their workstation locking software whenever they leave their workstation unattended for 5 minutes or more. Our workforce members must log off from or lock their workstations(s) when their shifts are complete.

**Procedure**
Our workforce members will take all reasonable precautions to protect the ePHI on our information systems. Workforce members will not engage in ANY activity at their workstation that is not work-related. Passwords will be used for access and WILL NOT be shared with anyone else. Workforce members will log off or lock their workstation whenever they leave their workstation for 5 minutes or more and when their shifts are complete. Our HIPAA Compliance Officer will review and revise this plan on an annual basis or when necessary.

---

**STANDARD #3: Workstation Security (Required)**

**Policy**
Our workstations containing ePHI must be placed in locations that minimize the risk of unauthorized access to them. Our workforce members must take reasonable measures to prevent viewing ePHI on workstations by unauthorized persons. Unauthorized workforce members must not attempt to gain physical access to workstations that can access ePHI. Our workforce members must report loss or theft of any access device (such as keys) that allows them physical access to areas in our office having workstations that can access ePHI.

**Procedure**
Our HIPAA Compliance and Security Officer will coordinate with the Office Manager on the physical placement of our workstations in order to locate them where the risk of unauthorized access is minimal. Our workforce members will take reasonable steps to prevent the viewing of ePHI on their workstations. Unauthorized workforce members will not attempt to gain physical access to workstations that can access ePHI. Our HIPAA Compliance Officer will review and revise this procedure on an annual basis or when necessary.

---

**STANDARD #4: Device and Media Controls**

**Policy**
ePHI must be consistently protected and managed through its entire life cycle, from origination to destruction. All electronic media, including backup copies that contain ePHI must be clearly marked as confidential. We must regularly conduct a formal, documented process that ensures consistent control of all electronic media and information systems containing ePHI that is created, sent, received or destroyed by us. Access to our information systems and electronic media containing ePHI must be provided only to authorized workforce members who have a need for specific access in order to accomplish a legitimate task.

---

**IMPLEMENTATION SPECIFICATIONS**

**Media Disposal (Required)**

**Policy**
All of our information systems and electronic media containing ePHI must be disposed of properly when no longer needed for legitimate use. Disposal of all of our electronic media and information systems containing ePHI must be tracked and logged. If an information system or electronic medium containing ePHI is to be reused within our office, its previous data must be completely removed.

**Procedure**
Our HIPAA Security Officer will ensure proper disposal of all of our information systems and electronic media when no longer needed for legitimate use. This disposal will include the ePHI that is received or created by us. If it is to be reused within our office, the information system or electronic media will be erased with a method approved by our HIPAA Security Officer.

**Media Re-Use (Required)**

**Policy**
All ePHI from our electronic media must be removed before such media can be re-used. Failure to remove ePHI could result in it being revealed to unauthorized persons. We must maintain and regularly review a formal, documented process that ensures all ePHI on electronic media is removed before the media is re-used. ePHI on our electronic media must be removed with erase tools that have been approved by our HIPAA Security Officer.

**Procedure**
Our HIPAA Security Officer will be responsible to ensure that all ePHI received or created by us is removed from our electronic media before it can be re-used. It will be erased with tools that have been approved by our HIPAA Security Officer.

**Accountability (Addressable)**

**Policy**
All movement of our information systems and electronic media containing ePHI into and out of our office must be tracked and logged. Those responsible for such movement must take all appropriate and reasonable actions to protect ePHI. This includes both ePHI received and created by us. Workforce members should use only our approved and tracked electronic media to store ePHI. Unless appropriately protected and authorized, ePHI must not be stored on a workforce member’s home computer(s).

**Procedure**
Unless appropriately protected and authorized, ePHI must not be stored on our workforce member’s home computer. Only the HIPAA Security Officer and/or Data Management are the only ones who remove ePHI.

**Data Backup and Storage (during transfer) (Addressable)**

**Policy**
Backup copies of ePHI on our information systems and electronic media must be made regularly. We must have adequate backup systems that ensure that all such ePHI can be recovered following a disaster or media failure. Backup copies of ePHI stored at a secure location must be accessible to authorized employees for timely retrieval of the information. Backup and restoration procedures for our electronic media and information systems containing ePHI must be regularly tested to ensure that they are effective and that they can be completed within a reasonable amount of time.

**Procedure**
Our HIPAA Security Officer backups all ePHI, both created and received by us, on our
information systems and electronic media. These backup copies will be made weekly, monthly
and annually and will be stored in a secure location off-site. Our HIPAA Security Officer will
test our backup and restoration of data regularly to ensure that our procedures are effective.
TECHNICAL SAFEGUARDS

STANDARD #1: Access Control

Policy
Our information systems must support a formal process for granting appropriate access to our information systems containing ePHI. Neither our workforce members nor any software programs can be granted access to information systems containing ePHI until properly authorized. Access to our information systems containing ePHI must be limited to our workforce members and software programs that have a need to access specific information in order to accomplish a legitimate task. Our workforce members must not provide access to our information systems containing ePHI to unauthorized persons.

- IMPLEMENTATION SPECIFICATIONS

Unique User Identification (Required)

Policy
Our information systems must grant user access through unique identifiers that identify workforce members or users, and allow activities performed on information systems to be traced back to a particular individual through tracking of unique identifiers. Unique identifiers must not give any indication of the user’s privilege level. Our HIPAA Security Officer must approve a user naming practice that must be used to create user names for such users.

Procedure
Our HIPAA Security Officer will grant user access through unique identifiers that identify our workforce members and allow their activities to be tracked. These unique identifiers will not give any indication of the user’s privilege level. Our user naming practice must be approved by our HIPAA Security Officer.

Emergency Access Procedures (Required)

Policy
We must have a formal, documented emergency access procedure enabling our workforce members to access the minimum ePHI necessary to treat patients in the event of any emergency. Such access must be authorized by our HIPAA Security Officer. Our workforce members must receive regular training and awareness on our emergency access procedure.

Procedure
If an emergency occurs at our office which will require a workforce member to access ePHI that he or she does not usually have authorization to access, but is required to access in order for a patient to receive treatment, we will do the following:

1. The workforce member involved nearest the emergency situation will be designated to access the patient’s ePHI.
2. The workforce member will access the minimum ePHI necessary to treat the patient; either paper or electronic ePHI may be accessed.
3. A workforce member will review the correct policies and procedures for worker’s compensation and liability procedures found at the front desk of every facility.
4. 911 will be called if emergency is life threatening.
5. The workforce member will log the access to the ePHI; what was accessed and for what treatment reasons on a disclosure log and place in the client’s file.
6. The HIPAA Compliance Officer will audit the access to the ePHI to ensure that appropriate access was made by the workforce member.

**Automatic Logoff (Addressable)**

**Policy**
Our workforce members must end electronic sessions on information systems that contain or can access ePHI when such sessions are completed, unless the information system is secured by an appropriate locking method, e.g. a password protected screen saver. Our workforce members must activate their workstation locking software whenever they leave their workstation unattended for 5 minutes or more. Our workforce members must log off from or lock their workstation(s) when their shift is complete.

**Procedure**
Our workforce members must activate their workstation locking software whenever they leave their workstation unattended for 5 minutes or more. Exceptions to our information systems required inactivity timeout must be approved by our HIPAA Security Officer. Our workforce members must log off from or lock their workstation(s) when their shift is complete.

**Encryption and Decryption (Data at rest) (Addressable)**

**Policy**
Appropriate encryption must be used to protect the confidentiality, integrity, and availability of ePHI contained on our information systems. We must have a formal, documented process for managing the cryptographic keys used to encrypt ePHI on our information systems. Our cryptographic keys must have defined activation and activation dates. No workforce member will implement encryption of data without the knowledge and approval of our HIPAA Security Officer. Our HIPAA Security Officer will maintain documentation with regards to when encryption is utilized.

**Procedure**
This implementation specification is addressable. We have addressed its requirements and have determined that it does not apply to our practice (Access protections are in place throughout our plan).

---

**STANDARD #2:  Audit Controls (Required)**

**Policy**
We must be able to record and examine significant activity on our information systems that contain ePHI. Appropriate hardware, software or procedural auditing mechanisms must be implemented on our information systems that contain ePHI. Logs created by audit mechanism implemented on our information systems must be reviewed regularly. We must develop and implement a formal process for audit log review. Our workforce members should not review audit logs that pertain to their own system activity.

**Procedure**
In coordination with our software vendor, our HIPAA Security Officer will implement electronic mechanisms to create audit logs of user activity on our information systems containing ePHI. This will be done to ensure that workforce members are not attempting to access ePHI to which they have not been authorized. Our HIPAA Security Officer will weekly examine these audit logs for what s/he considers “significant activity”. Our workforce members will not review audit logs that pertain to their own system activity.

---

STANDARD #3:  Integrity

Policy
We must appropriately protect all ePHI contained on our information systems from improper alteration or destruction. Only our properly authorized and trained workforce members may access and use ePHI on our information systems. Such access and use must be provided only to our workforce members having a need to access to specific ePHI in order to accomplish a legitimate task. Such access and use must be regularly revised as necessary.

- IMPLEMENTATION SPECIFICATION

Mechanism to authenticate ePHI (Addressable)

Policy
We must implement appropriate electronic mechanisms to confirm that ePHI contained on our information systems has not been altered or destroyed in an unauthorized manner. Electronic mechanisms used to protect the integrity of ePHI contained on our information systems must ensure that the value and state of the ePHI is maintained and it is protected from unauthorized modification and destruction. Such mechanisms must also be capable of detecting and reporting unauthorized alteration or be capable of detecting and reporting unauthorized alteration or destruction of ePHI. Our workforce members must receive regular training and awareness about the electronic mechanisms used to protect the integrity of ePHI contained on our information systems.

Procedure
This implementation specification is addressable. We have addressed its requirements and have determined that it does not apply to our practice. (See Stand #5 “Integrity Controls”).

---

STANDARD #4:  Person or Entity Authentication (Required)

Policy
We must create and implement a formal, documented process for verifying the identity of a person or entity before granting them access to ePHI. The process must be regularly reviewed and revised as necessary. Our HIPAA Security Officer must provide our employees with regular training and awareness about the authentication standard(s). All authentication data, such as passwords and PINs, must be protected with appropriate access controls to prevent unauthorized access. Our employees must not share or reveal their authentication methods to others. Any employee who believes that their authentication method is being inappropriately used, must immediately notify our HIPAA Compliance and/or Security Officer.

Procedure
Our HIPAA Security Officer will implement a process for the verifying of the identity of a person before they are able to gain access to our ePHI. Each employee will have their own individual method for authenticating their identity. Our employees will not share or reveal their authentication method. Our employees will not ask another to share or reveal their authentication method. Authentication attempts to all of our information systems is limited to no more than 3 attempts in 10 minutes. Our HIPAA Security Officer will train all employees on this procedures, and review and revise as needed.

---

STANDARD #5: Transmission Security

Policy
We must appropriately protect the confidentiality, integrity and availability of all data that we transmit over electronic communication networks. Unless risk analysis indicates that there is not significant risk when sending our data over an electronic network, the data must be sent in encrypted form and have controls to safeguard the integrity of the data. Our HIPAA Security Officer must approval all encryption and integrity controls prior to their use.

- IMPLEMENTATION SPECIFICATIONS

Integrity Controls (Addressable)

Policy
Appropriate integrity controls must be used to protect the confidentiality, integrity, and availability of our data transmitted over electronic communication networks. Integrity controls must always be used when our highly sensitive data such as passwords are transmitted over electronic communication networks.

Procedure
In reliance upon our software provider, our HIPAA Security Officer will approve, obtain and implement their electronic mechanisms to ensure the integrity of our ePHI that is transmitted over electronic communication networks.

Encryption (During transmission) (Addressable)

Policy
When risk analysis indicates it is necessary, appropriate encryption must be used to protect the confidentiality, integrity and availability of our data transmitted over electronic communication networks. Encryption must always be used when our highly sensitive data such as passwords are transmitted over electronic communication networks. Our cryptographic keys must have defined activation and deactivation dates.

Procedure
This implementation specification is addressable. We have addressed its requirements and have determined that it is already addressed in our plan. (See Standard #5 “Integrity Controls”).
ORGANIZATIONAL REQUIREMENTS

STANDARD #1: Policies and Procedures (Required)

Policy
We must establish and maintain organizational policies and procedures to address all requirements of the HIPAA Security Rule. We must establish and maintain organizational policies and procedures to ensure and support the confidentiality, integrity, and availability of our ePHI. Our workforce members must be informed of all policies and procedures that apply to them in their individual roles. We must establish policies and procedures for organizational security that incorporates our specific characteristics with respect to:

- The size, complexity and capabilities of our organization
- Our organization’s technical infrastructure, hardware and software capabilities
- The cost of implementing security measures, and
- The probability and criticality of potential risks to our ePHI

We must ensure that our policies and procedures for security are compatible with our culture and strategic planning objectives. Our HIPAA Security Officer and Compliance Officer must conduct an annual formal review of our policies and procedures for security and update them as necessary.

Procedure
Our HIPAA Security & Compliance Officer is responsible for establishing and maintaining organizational policies and procedures to address all the requirements of the HIPAA Security Rule. Our workforce members are trained on the policies and procedures that apply to them according to their job roles. Our HIPAA Security Officer and Compliance Officer will conduct an annual review of our policies and procedures for security and update them as needed.

---

STANDARD #2: Documentation (Required)

Policy
We must maintain the security policies and procedures we implement to comply with the HIPAA Security Rule in written (paper or electronic) form. If an action, activity or assessment is required by the HIPAA Security Rule to be documented, we must maintain a written (paper or electronic) record of the action, activity, or assessment. We must retain such documentation for 6 years from the date of its creation or the date when it last was in effect, whichever is later. We must make such required documentation available to all workforce members responsible for implementing the policies and procedures to which the documentation pertains. Our HIPAA Compliance Officer must review the required documentation annually and update it as needed and in response to environmental and/or operational changes affecting the confidentiality, integrity and availability of our ePHI.

Procedure
Our HIPAA Compliance Officer and Security Officer is responsible to maintain the HIPAA Security policies and procedures that we implement in our office. They are to be maintained for 6 years in either paper or electronic format and made available to those in authority in the case of an investigation. Our HIPAA Compliance Officer and Security Officer will review the documentation annually and update it as needed.