

Guide to HIPAA Security Implementation for Small Practices

January 2005

James Shirley Management Consultants, Inc.



Making processes better for people

Disclaimer

This document may be freely distributed in its entirety. This document is provide “as is” without any express or implied warranty.

While the information in this document is believed to be correct at the time of writing, this document is for educational purposes only and does not purport to provide legal advice. This information is for reference use only and does not constitute rendering of legal, financial, or other professional advice or recommendations by James Shirley Management Consultants, Inc. You should seek professional advice on the recommendation, guidance and checklists provided in this document.

Guide to HIPAA Security Implementation for Small Practices

Table of Contents

1. Overview	1
A. Is This Guide Right For You?	1
B. Background and Basics	1
C. Recommended Approach	2
2. References and Study	5
A. Great References from WEDI	5
B. Your Study and Learning the Concepts	6
3. Administrative Safeguards	8
A. The Nine Administrative Safeguard Standards	8
B. Check for Successful Implementation	8
4. Physical Safeguards	18
A. The Four Physical Safeguard Standards	18
B. Check for Successful Implementation	18
5. Technical Safeguards	23
A. The Five Physical Safeguard Standards	23
B. Check for Successful Implementation	23
6. Needed Policies and Procedures	27

List of References

1. WEDI Small Practice Implementation White Paper
SNIP – Security and Privacy Workgroup – Version 2.0 – April 2004
[\[http://www.wedi.org/\]](http://www.wedi.org/)
2. Federal Register – Part II – Department of Health and Human Services
45 CFR Parts 160,162 and 164 Health Insurance Reform: Security Standards; Final
Rule
February 20, 2003.

1. Overview

A. Is This Guide Right For You?

This HIPAA Security Guide is for small health care medical practices. A small medical practice is defined as a practice with ten or fewer employees, including physicians.

If you answer yes to following questions, this guide will give you direction on steps you must take to comply with the HIPAA Security Standards [45 CFR Part 160, 162 and 164].

Questions on Using This Guide

[Can you answer “Yes” to each of these questions?]

1. Do you want to do as much as possible yourself without asking for outside help?
2. Are you willing to read and learn about the HIPAA Security Standards?
3. Can you download a file from a website with the Internet?
4. Will you dedicate the needed time and obtain the need resources to develop and implement the HIPAA Security Standards before April 21, 2005?
5. Are you ready to start now?

If you answered “Yes” to all of the above questions, let’s get started. How many weeks are there until April 21, 2005 [the HIPAA Security compliance date]? What does your calendar show? Well, that is all of the time we have. Let’s get it done.

B. Background and Basics

The HIPAA Security Standards are the standards from the Department of Health and Human Services that apply to the security of electronic protected health information (ePHI). If you provide health care services and submit claims electronically, you must comply with these standards.

The HIPAA Security Standards and the HIPAA Privacy Rule are linked and are part of the same set of Department of Health and Human Services regulations. The Privacy Rule focused on a wide range of processes, procedures and guidelines to protect PHI. As you recall, the Privacy Rule protects all PHI, including communication that is oral, written and electronic. The HIPAA Security Standards focus on electronic PHI and put new standards in place to secure PHI and ePHI [electronic protected health information].

In general, the security standards require you to do the following:

1. Ensure the confidentiality, integrity and availability of all ePHI that you create, receive, maintain and transmit.

2. Protect against any reasonably anticipated threats or hazards to the security on integrity of ePHI.
3. Protect against any reasonably anticipated uses or disclosures of ePHI that are not permitted or required under the regulation.
4. Ensure compliance with the standards by your workforce.

C. Recommended Approach

The approach that we have developed requires these steps as shown in Exhibit 1 on page 4 and as described below:

1. Obtain and Study HIPAA Security References.

You will download from the WEDI website a great white paper that describes steps to take for small practice implementation of the HIPAA Security Standards. WEDI is the Workgroup for Electronic Data Interchange that provides freely distributed guides to help with implementation of major national issues, such as HIPAA.

2. Implement Administrative Safeguards.

You will follow the steps to learn and implement the Administrative Safeguards required by the HIPAA Security Standards. These standards focus on management, training, contracts and other administrative matters. Remember the Business Associate agreements from the HIPAA Privacy Rule? You may have to update your agreements with business associates who have access to PHI and ePHI to comply with the new HIPAA Security Standards.

3. Implement Physical Safeguards.

You will follow the steps to learn and implement the Physical Safeguards required by the HIPAA Security Standards. These standards focus on physical actions you must take such as access to your office, computers and media that store ePHI, such as diskettes.

4. Implement Technical Safeguards.

You will follow the steps to learn and implement the Technical Safeguards required by the HIPAA Security Standards. These standards focus on technical items, such as access to your computers (passwords), integrity of ePHI and other technical matters.

5. Develop Any Needed Policies and Procedures.

You may need some new policies and procedures to comply with the new HIPAA Security Standards. You may be able to update or add to your HIPAA Privacy Rule policies and procedures to meet these new requirements.

6. Implement Security Awareness Training for Everyone.

Just as with the HIPAA Privacy Rule, the new HIPAA Security Standards require training for everyone on these new standards. Yes, that is everyone, including the physicians.

7. Put in place a Process for Periodic Evaluation of Security.

The HIPAA Security Standards require that you periodically examine your security to ensure you maintain security of all PHI. When a major change occurs or you have reached a one-year date from your first implementation, you should update your risk analysis. We will put a review on the calendar for your annual security review.

Please go to page 5 we will begin the implementation steps for the HIPAA Security Standards.

2. References and Study

A. Great References from WEDI

The first step in implementing the HIPAA Security Standards is to obtain a reference that will give you the background and guidance you need. As described earlier, WEDI is the Workgroup for Electronic Data Interchange that provides freely distributed guides to help with implementation of major national issues, such as HIPAA. As you will see on the WEDI website, there is an enormous amount of information on HIPAA.

Step 1 – Download and Print the WEDI White Paper.

Download the Small Practice Security Implementation White Paper from the WEDI/SNIP Website [04/30/04 SECURITY: Small Practice Implementation White Paper, Version 2.0]

Sometimes it can be hard to find the document you want. Try these steps to get to the white paper:

- (1) Go to the WEDI web site [<http://www.wedi.org/>]
- (2) Click on “SNIP” that is in the center of the page.
- (3) Click on “SNIP Work Products.”
- (4) Click on “Security and Privacy White Paper and Power Point Presentations.”
- (5) In the list White Papers Completed, click on the sixth one in the list titled “04/30/2004 Security: Small Practice Security Implementation White Paper, Version 2.0, 04/28/04

Print this great white paper. You will use it to learn about and implement the HIPAA Security Standards for your practice.

Before you begin reading the WEDI white paper, look at the list of 18 standards for the HIPAA Security Standards on the next page. Answer these questions as you look over the list of the 18 standards:

1. What do you believe standard number 2 will be about? Will that be an assigned security officer? Who do you believe will be assigned as this responsibility? Will it be you?
2. There are nine standards listed under Administrative Safeguards. What are the topics?
3. What is addressed in the Physical Safeguards?
4. What do the Technical Safeguards address?

Exhibit 1

HIPAA Security Work Plan

Revised: January 27, 2005

		4/21/05											
		[Thur.]											
		Target											
		Feb		Mar				Apr				Date	
		[Weeks to compliance date]	10	9	8	7	6	5	4	3	2	1	↓
Major Project Steps		Assigned to:	2/7	2/14	2/21	2/28	3/7	3/14	3/21	3/28	4/4	4/11	4/18
1	Obtain and study HIPAA Security references.		█	█									
2	Implement Administrative Safeguards.				█	█	█						
3	Implement Physical Safeguards.				█	█	█	█					
4	Implement Technical Safeguards.					█	█	█	█	█			
5	Develop any needed policies and procedures.						█	█	█	█	█		
6	Implement security awareness training for everyone.										█	█	
7	Put in place a process for periodic evaluation of security.											█	

HIPAA Security Standards

The Eighteen Standards

Note: [Numbers in brackets are paragraph numbers in the HIPAA Security Regulations]

Administrative Safeguards [164.308]

1. Standard: Security Management Process [§164.308(a)(1)(i)]
2. Standard: Assigned Security Responsibility [§164.308(a)(2)]
3. Standard: Workforce Security [§164.308(a)(3)(i)]
4. Standard: Information Access Management [§164.308(a)(4)]
5. Standard: Security Awareness and Training [§164.308(a)(5)]
6. Standard: Security Incident Procedures [§164.308(a)(6)]
7. Standard: Contingency Plan [§164.308(a)(7)]
8. Standard: Evaluation [§164.308(a)(8)]
9. Standard: Business Associate Contracts and Other Arrangement [§164.308(b)(1)]

Physical Safeguards [164.310]

10. Standard: Facility Access Controls [§164.310(a)(1)]
11. Standards: Workstation Use [§164.310(b)]
12. Workstation Security [§164.310(c)]
13. Standard: Device and Media Controls [§164.310(d)(1)]

Technical Safeguards §164.312]

14. Standard: Access Control [§164.312(a)(1)]
15. Standard: Audit Controls [§164.312(b)]
16. Standard: Integrity [§164.312(c)(1)]
17. Standard: Person or Entity Authentication [§164.312(d)]
18. Standard: Transmission Security [§164.312(e)(1)]

B. Your Study and Learning Concepts

Step 2 – Read the WEDI White Paper.

The Small Practice Security Implementation White Paper has 31 pages of narrative and tables. Read the white paper and make a list of topics that specifically apply to your practice. Answer these questions as you read the white paper:

1. Do understand the difference between “Required” and “Addressable” standards?
[See page 5].
2. Do you understand what will be required in the sanction policy? [See page 8]
3. Who must receive security awareness training? [See page 13]

4. What does the contingency plan standard address? [See page 16]
5. What would cause your Business Associate agreement to be updated? [See page 19]
6. What is included in device and media controls? [See page 23]

3. Administrative Safeguards

There are nine standards that must be examined as you implement the Administrative Safeguards of the HIPAA Security Standards. We will review each of the nine standards and 21 implementation specifications described in the white paper.

A. The Nine Administrative Safeguards [Standards]

As listed earlier, here are the nine standards that are described in the WEDI white paper:

1. Standard: Security Management Process [§164.308(a)(1)(i)]
2. Standard: Assigned Security Responsibility [§164.308(a)(2)]
3. Standard: Workforce Security [§164.308(a)(3)(i)]
4. Standard: Information Access Management [§164.308(a)(4)]
5. Standard: Security Awareness and Training [§164.308(a)(5)]
6. Standard: Security Incident Procedures [§164.308(a)(6)]
7. Standard: Contingency Plan [§164.308(a)(7)]
8. Standard: Evaluation [§164.308(a)(8)]
9. Standard: Business Associate Contracts and Other Arrangement [§164.308(b)(1)]

Let's look at each one and what is suggested by the WEDI white paper to see what implementation issues you must address for the HIPAA Security Standards.

B. Checklist for Successful Implementation.

1. Standard - Security Management Process

The first standard describes security management processes you must implement.

Implement policies and procedures to prevent, detect, contain and correct security violations.

Here is the first implementation specification.

A. Risk Analysis (Required) – Implementation Specification

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 your organization.

Checklist:

1. Walk through you office and list the potential risks to ePHI by using the list of standards on page 6 of this guide and the descriptions of the implementation specifications you read about the WEDI white paper.
2. Look at your current practices and list what should be changed to improve security.
For example:
 - a. Individuals are not unique (for one person only) assigned user names and passwords.
 - b. Users are not automatically logged off their computers after a predetermined time.

B. Risk Management (Required) – Implementation Specification

Implement security measures sufficient to reduce risks and vulnerabilities to reasonable and appropriate levels.

Checklist:

1. Decide what risks you will review periodically, such as updating the firewall software as described in the WEDI white paper. Make a list of these risks.
2. Decide the time frame you will use to review each of the risks on your list.
For example:
 - a. Ensure annually that your firewall and anti-virus software is updated and current.
 - b. If there is a significant change, such as in personnel, you will review security risks.

C. Sanction Policy (Required) – Implementation Specification

Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures. That is, you must have a sanction policy in place and use it against your workforce for violating security policies and procedures.

Checklist:

1. Ensure you have a sanctions policy as described in the WEDI white paper on page 8.

D. Information Systems Activity Review (Required) – Implementation Specification

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

Checklist:

1. Implement a procedure for regular audits of the use of confidential information.
For example:
 - a. Ensure you annually review the list of people authorized to use confidential information.
 - b. If you have a firewall and Internet access you should review security incident tracking reports regularly.

2. Standard - Assigned Security Responsibility

The second Administrative Safeguard standard describes the requirement for someone to be designated as the security official. This person is responsible for developing and implementing your security policies and procedures.

A. Assigned Security Responsibility (Required) – Implementation Specification

Identify the security official who is responsible for the development and implementation of the policies and procedures required by the HIPAA Security Standards.

Checklist:

1. Select one person as the Security Official and document who that persons is in your practice. You may want to use the same person who was designated as the Privacy Official.

3. Standard - Workforce Security

The third Administrative Safeguard standard describes workforce policies and procedures.

Implement policies and procedures ensuring all member of your workforce have appropriate access to ePHI and preventing others who are not authorized from obtaining access to ePHI.

A. Authorization and /or Supervision (Addressable) – Implementation Specification

Implement procedures for the authorization and/or supervision of workforce members who work with ePHI or in locations where it might be accessed.

[Remember, “Addressable” does not mean optional. It means that you must decide how to address this implementation specification, if you do not follow the implementation specification statement. And, you must document your decision on how you will address it.]

Checklist:

1. Develop written procedures for granting and revoking access to ePHI and computer systems in your practice.

B. Workforce clearance procedure (Addressable) – Implementation Specification

Implement procedures to determine that the access of a workforce member to ePHI is appropriate.

Checklist:

1. Ensure your policies and procedures only allow authorized members of your workforce to have access to confidential information after receiving appropriate clearances.
2. Ensure you do basic employment screening of potential employees.
3. Ensure up-to-date records are kept on keys and access cards to your office.

C. Termination procedures (Addressable) – Implementation Specification

Implement procedures for terminating access to ePHI when the employment of a workforce member ends.

Checklist:

1. Ensure you have appropriate termination procedures when an employee leaves your workforce to prevent unauthorized access to ePHI. Use the guidelines at the top of page 11 in the WEDI white paper to develop your procedures.
2. Ensure your procedures document each termination and the person responsible for the termination documentation.

4. Standard - Information Access Management

The fourth standard describes the issues you must consider concerning access to ePHI:

Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of the HIPAA Security Standards.

A. Isolating Health Care Clearinghouse Function (Required) – Implementation Specification

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.

As stated in the WEDI white paper, this does not apply to small health care practices. However, you must document in your policies and procedures that this implementation specification does not apply to your practice.

Checklist:

1. Document in your policies and procedures that this implementation specification regarding isolating a health care clearinghouse function does not apply.

B. Access authorization (Addressable) – Implementation Specification

Implement policies and procedures for granting access to ePHI, for example, through access to a workstation, transaction, program, process, or other mechanism.

Here you must develop policies and procedures for granting access to ePHI. Follow the guidelines described in the WEDI white paper.

Checklist:

1. Document authorization for access and level, define times and document roles.
[WEDI white paper, page 12, first full paragraph on the page.]
2. Define rules for granting access based on the minimum amount of ePHI needed by each person in your workforce to do her or his job.
[WEDI white paper, page 12, second full paragraph on the page.]

C. Access establishment and modification (Addressable) – Implementation Specification

Implement policies and procedures that, based upon your practice's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.

For this implementation specification you must develop policies and procedures which will establish access for people in your workforce to computer workstations, transactions, programs or processes you use to handle ePHI.

Checklist:

1. Document access establishment and modification with policies and procedures.
[WEDI white paper, page 12, the last three paragraphs on the page.]

5. Standard - Security Awareness Training

The fifth standard describes training that is required for **all members of your workforce**:

Implement a security awareness and training program for all members of your workforce (including management).

Everyone in your office must learn about the HIPAA Security Standards and what her or his responsibilities is under these regulations. The WEDI white paper gives you a great outline of what to include in the training:

1. Document the training [have an agenda, date, handouts and sign-in log].
2. Train on vulnerabilities of ePHI and your policies and procedures to protect ePHI.
3. Describe methods you will use to report security problems.
4. Keep your training records [who, what, when, why] for six years.
5. Use periodic refresher training to maintain security awareness.
6. If significant changes occur in the practice, such as a new computer system, new training may be needed regarding the changes.

Checklist:

1. Follow the guidelines in the WEDI white paper on page 13, using the checklist above to develop and implement the needed training for everyone in your practice.

A. Security reminders (Addressable) - Periodic security updates– Implementation Specification

This is an action item that goes beyond preparing policies and procedures. You are communicating to your workforce regularly (monthly or quarterly) regarding security of confidential information.

Checklist:

1. Set up a time, such as quarterly, for periodic security reminders.
2. Document that you are providing the periodic updates.
3. Communicate quickly on security incidents and corrective actions changes taken.

B. Protection from malicious software (Addressable) – Implementation Specification

These policies and procedures are for guarding against, detecting, and reporting malicious software. This implementation specification focuses on steps you should take to avoid viruses and other software that can put the confidentiality, integrity and availability of your ePHI at risk.

The WEDI white paper has several great suggestions on steps you should take on page 14.

Checklist:

1. Ensure you have anti-viruses software and it has frequent updates.
2. Do not allow anyone to bring diskettes or software into your office.
3. Inspect computers regularly for unauthorized software.
4. Ensure operating system and software patches are promptly installed as recommended by the vendors.

C. Log-in monitoring (Addressable) – Implementation Specification

These policies and procedures describe what you will do to monitor log-in attempts and how you will report discrepancies.

WEDI recommends that you set your software to an established number of attempts to log in and when that number of attempts is exceeded, the system will lock up.

Checklist:

1. Determine how many unsuccessful attempts you will allow for log-ins to your computer system [such as 3] and set your computer systems to that number of attempts.
2. The Security Officer should regularly [monthly or quarterly] review any reports that are created by your software on log-in attempt frequencies.

D. Password management (Addressable) – Implementation Specification

These policies and procedures describe what you do to create, change, and safeguard passwords to your computer systems.

Write your policies and procedures using the guidelines from the paragraphs at the top of page 15 in the WEDI white paper. Here are some of the highlights you should consider:

1. Passwords must not be shared or disclosed to others.
2. Sharing passwords is a violation of security policy.
3. Sharing or permitting use of passwords should be reported to the Security Officer.
4. Password management should make passwords robust and difficult to crack.
5. Passwords must remain confidential and never posted on or near a computer.
6. Compromised passwords should be replaced.

Checklist:

1. Follow the guidelines in the WEDI white paper on page 15, using the list above to develop and implement the needed policies and procedures for your practice.

6. Standard - Security Incident Procedures

The sixth standard describes the administrative policies and procedures you should put in place for handling, documenting and resolving security incidents.

A. Response and Reporting (Required) – Implementation Specification

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

This implementation specification focuses on steps you must take when there is a security incident in your practice. Carefully review the issues described in the WEDI white paper at the top of page 16. Use these summary points as a guide to design your administrative standards:

1. Write policies and procedures to identify, report and respond to security incidents.
2. Define what is a security incident [a security breach].
3. Ensure workforce members understand that they are to report security incidents to the Security Officer.
4. The Security Officer should contain security breaches and minimize their damage.

Checklist:

1. Follow the guidelines listed above and in the WEDI white paper on page 16 to develop and implement the needed policies and procedures for your practice.

7. Standard - Contingency Plan

The seventh standard describes what you must do to develop a contingency plan where accidental, natural or intentional incidents lead to damage to ePHI. That is, you must develop a plan on how you will handle a disaster, should it occur.

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.

Your contingency plan [used to handle a disaster] will include these items in the implementation specifications described below:

1. Data backup plan [Required]
2. Disaster recovery plan [Required]
3. Emergency mode operation plan [Required]
4. Testing and revision procedure [Addressable]
5. Applications and data criticality analysis [Addressable]

As described in the WEDI white paper, the focus on the contingency plan is to position your practice to be able to recover lost ePHI. Look over the paragraphs at the bottom of page 16 and the sentences at the top of page 17 so you will have a good understanding of what must be done to create your contingency plan.

A. Data backup plan (Required) – Implementation Specification

Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.

This implementation specification requires that you backup your electronic data, including ePHI.

Read the WEDI white paper on page 17 as a guide on steps you should take to ensure you have needed backup of electronic data.

Checklist:

1. Implement automatic backup procedures recommended by your computer software vendor.
2. Use passwords to protect your backup information to ensure it remains confidential.
3. Store your backup information in a safe location.
4. Test your backup procedures every three to six months or when computer software or hardware are modified.

B. Disaster recovery plan (Required) – Implementation Specification

Establish (and implement as needed) procedures to restore any loss of data.

As its name implies, a disaster recovery plan is required so you can restore lost ePHI. You should be able to keep your disaster recovery plan to a few pages of notes and guidelines, using the ideas in the WEDI white paper on pages 17 and 18.

Checklist:

1. Focus on how you will recover ePHI in a timely manner.
2. Determine how you will identify an alternative computer system to use after the disaster.
3. Determine who will handle contacts with employees, patients and vendors.

C. Emergency made operation plan (Required) – Implementation Specification

Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of ePHI while operating in emergency mode.

This implementation specification asks you to develop procedures to be able to run your practice in an emergency mode.

Checklist:

1. Develop plans on how your practice would operate in an emergency mode.
2. Determine hardware needs for computers, software requirements, temporary work sites, telephone needs and other needs for emergency operations.

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

You are required to periodically review your contingency plan and test to ensure it works. The WEDI white paper has excellent guidelines on steps you should take as described at the bottom of page 18.

Checklist:

1. Set a periodic review date and test your contingency plan to ensure it works.
2. Test your contingency plan with these WEDI questions:
 - Can you timely access computers and sites?
 - Can you load and run necessary programs?
 - Can you load, view and use ePHI?

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

This implementation specification asks you to examine the importance of software, hardware and applications. Additionally, you must document your review of critical application and data.

The short paragraph at the top of page 19 gives you these guides:

1. Review and document your assessment of the importance of software, hardware and applications.
2. Rank each system based on its importance to your practice for disaster recovery and for emergency mode operation.

Checklist:

1. Create a checklist to show your review and priority ranking of software, hardware and applications that are critical to your operations.

8. Standard – Evaluation - Required

The eighth standard focuses on the need to regularly evaluate security in your practice. Here is the statement that summarizes the intent of this required standard:

Perform a period technical and non-technical evaluation, based initially upon the standards implemented under the HIPAA Security Standards and subsequently, in response to environmental or operational changes affecting the security of ePHI, that establishes the extent to which your security policies and procedures meet the requirements of this standard.

The WEDI white paper gives you only a few guidelines on what to do for this required standard. The key points are:

1. You must regularly evaluate your security.
2. If changes occur in your practice, such a new computer, security risks may change.
3. Evaluate your security when major changes occur and at least annually.

Checklist:

1. Set up an evaluation schedule to regularly assess security risks in your practice.

9. Standard – Business Associate Contracts or Other Arrangements – Required

You may permit a business associate to create, receive, maintain, and transmit electronic protected health information on your behalf only if the you obtain satisfactory assurances that the business associate will appropriately safeguard information.

This final standard in the Administrative Safeguards focuses on the Business Associate contracts or agreements between your practice and business associates. Business associates came up during the HIPAA Privacy Rule implementation. In general, business associates are vendors of your practice that have access to and use protect health information and ePHI.

As the WEDI white paper describes, the HIPAA Security Standards added a new requirement for your Business Associate contracts or agreements. If the Business Associate becomes aware of a security incident, then the Business Associate must notify you. Additionally, there are other requirements as described in the two paragraphs at the top of page 20.

Checklist:

1. Carefully read the WEDI white paper guidelines at the top of page 20.
2. Review your Business Associate agreements to see if you need to create an addendum or an amendment to existing agreements.
3. Have you lawyer review your Business Associate agreement or contracts to ensure they meet the new security requirements.

4. Physical Safeguards

There are four standards that must be examined as you implement the Physical Safeguards of the HIPAA Security Standards. We will review each of the four standards and the eight implementation specifications associated with the standards.

A. The Four Physical Safeguards [Standards]

As listed earlier, here are the four physical standards that are described in the WEDI white paper:

1. Standard: Facility Access Controls [§164.310(a)(1)]
2. Standards: Workstation Use [§164.310(b)]
3. Workstation Security [§164.310(c)]
4. Standard: Device and Media Controls [§164.310(d)(1)]

As we did with the Administrative Safeguards, let's look at each standard and what is suggested by the WEDI white paper. First, read the introductory comments on Physical Safeguards on page 20 of the WEDI white paper.

B. Checklist for Successful Implementation.

1. Standard – Facility Access Control

Implement policies and procedures to limit physical access to electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.

As the WEDI white paper describes, the focus for these standards is securing access to your office and computers. You must develop and implement written policies and procedures to limit access to your office and computers. All four of the implementation specifications are “addressable.” As described on page 5 of the WEDI white paper, you must consider each addressable implementation specification and decide what is appropriate for your practice. And, you must document your decision and rationale for that decision.

A. Contingency Operations (Addressable) – Implementation Specification

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.

This first implementation standard for the Facility Access Controls standards focuses on contingency operations. In the Administrative Safeguards standards we developed a contingency plan. Now, the focus is in contingency *operations*. Read the short paragraph in the middle of page 21 of the WEDI white paper.

Checklist:

1. Ensure the policies and procedures provide for access by those in your practice who will need access to your office in an emergency.

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

This implementation specification focuses on security of your office and its equipment. As the WEDI white paper describes, you should ensure doors are appropriately locked and that your workforce is vigilant.

Checklist:

1. Develop and enforce policies and procedures on locking doors to your office [back door should always remain locked].

C. Access control and validation procedures (Addressable) – Implementation Specification
Implement procedures to control and validate 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.

This implementation specification focuses on access to your office area by your workforce and others you authorize, as described in the WEDI white paper on page 22.

Checklist:

1. Ensure your policies and procedure describe how physical access is limited to authorized individuals [This may be in your existing policy and procedure manual or in your HIPAA Privacy policies and procedures].

D. Maintenance records (Addressable) – Implementation Specification
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).

Here your policies and procedures set up a process of documenting with records your work in maintaining physical security of your office and equipment.

Checklist:

1. Ensure your policies and procedures establish a method of maintaining records related to repairs and modifications of your office and equipment related to security.

2. 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.

3. Standard - Workstation Security.

Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users.

The WEDI white paper combines discussion of workstation use and security into one topic, discussed in the last half of page 22. Neither standard has an implementation specification but both are required and must be implemented.

Here are some of the key points:

1. You must ensure your computer workstations and other devices are secure and used appropriately.
2. The focus in these standards is *physical security* of your workstations and devices, including being able to view information on computer screens.
3. You must protect mobile devices such as laptop computers, personal digital assistants [PDAs] and other mobile devices.
4. Ensure the physical security of any medical devices with ePHI.

Checklist:

1. Review the key points above from the WEDI white paper and make a checklist of what must be reviewed and implemented for your practice.
2. Develop and implement needed policies and procedures that will comply with these two standards on workstation use and security.

4. 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 [ePHI] into and out of a facility, and the movement of these items within the facility.

This standard focuses physical controls for devices [computers, software and other equipment] and media [diskettes, CDs, DVDs and other forms of media]. The WEDI white paper gives a background on this standard and begins introducing the implementation specifications on page 23. Description of the four device and media controls implementation specifications begins on the following page.

A. Disposal (Required) – Implementation Specification

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.

You must properly dispose of any electronic media that contains ePHI and you must have policies and procedures describing your processes. Here are some key points:

1. Deleting a file or reformatting a hard drive are not enough. The equipment must be cleaned thoroughly before it is removed from your practice.
2. Do not allow computer diskettes to enter your practice after they have been on home computers.

Checklist:

1. Obtain technical help to ensure all ePHI is removed from any old computer that leaves you practice.

B. Media re-use (Required) – Implementation Specification

Implement procedures for removal of ePHI from electronic media before the media are made available for re-use.

This implementation specification describes what you must do to properly clean media, such as diskettes and CDs.

Checklist:

1. Develop procedures to carefully clean media that is reused in your practice with software that thoroughly eliminates old ePHI.
2. Develop and implement procedures to ensure that media [diskettes, CDs, DVDs and other media] are destroyed before leaving your office.

C. Accountability (Addressable) – Implementation Specification

Maintain a record of the movements of hardware and electronic media and any person responsible therefore.

This implementation specification describes what you must do to maintain records of your inventory of computer equipment and media, as described on page 24 of the WEDI white paper.

Checklist:

1. Develop an inventory of your hardware, software, devices (equipment with ePHI) and media.
2. Maintain a list of the inventory when the hardware and electronic media are moved, who moved them and where they are moved to.

D. Data backup and storage (Addressable) – Implementation Specification
Create a retrievable, exact copy of ePHI, when needed, before movement of equipment.

This implementation specification requires that you back up your ePHI.

Checklist:

1. Ensure you have back up procedures that are implemented properly for you ePHI.
2. Implement procedures to keep a backup copy of your ePHI at a secure location away from your office.

5. Technical Safeguards

There are five standards that must be examined as you implement the Technical Safeguards of the HIPAA Security Standards. We will review each of the five standards and the seven implementation specifications associated with the standards.

A. The Five Technical Safeguards [Standards]

As listed earlier, here are the five technical standards:

1. Standard: Access Control [§164.312(a)(1)]
2. Standard: Audit Controls [§164.312(b)]
3. Standard: Integrity [§164.312(c)(1)]
4. Standard: Person or Entity Authentication [§164.312(d)]
5. Standard: Transmission Security [§164.312(e)(1)]

As we did with the Administrative Safeguards and Physical Safeguards, let's look at each standard and what is suggested by the WEDI white paper. First, read the introductory comments on Technical Safeguards on page 24 of the WEDI white paper.

B. Checklist for Successful Implementation.

1. Standard - Access control.

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 as specifies by the HIPAA Security Standards.

A. Unique user identification (Required) – Implementation Specification

Assign a unique name and/ or number for identifying and tracking user identity.

This implementation specification describes what you must do for user identification and passwords, as mentioned earlier under the Administrative Safeguards.

Checklist:

1. Assign user names and passwords for each member of your workforce.

B. Emergency access procedure (Required) – Implementation Specification

Establish (and implement as needed) procedures for obtaining necessary ePHI during an emergency.

This implementation specification states the technical requirements to prepare for an emergency.

Checklist:

1. Ensure you have procedures on how you will obtain ePHI during an emergency.

C. Automatic logoff (Addressable) – Implementation Specification
Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.

This implementation addresses automatic logoff of your computers when members of your workforce are away from their computers for longer than a designated time, as described on page 25 of the WEDI white paper.

Checklist:

1. Ensure you have procedures and that they are implemented for automatic logoff after a predetermined time, such as 10 or 15 minutes.

D. Encryption and decryption (Addressable) – Implementations Specification
Implement a mechanism to encrypt and decrypt ePHI.

This implementation specification describes what you must consider for protecting ePHI sent over an open network, such as the Internet, as described in the WEDI white paper at the top of page 26. As with other “addressable” implementation specification, this requires that you make a judgment based on your practice needs and then document your decision. If you have the technical ability to make the judgment on the needs of your practice to encrypt and decrypt ePHI, make your assessment and document it. If you cannot make that judgment, ask for help from a technical advisor.

Checklist:

1. Make technical assessment on whether to encrypt and decrypt your ePHI that is sent over open networks and document your assessment.

2. Standard - Audit controls

Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI.

This HIPAA Security Standard does not have any implementation specifications, but the standard is required. The WEDI white paper briefly discusses this topic in the middle of page 26.

Checklist:

1. Ensure you have audit controls in place to monitor your electronic systems.
2. Review your audit records regularly to ensure activities are appropriate.

3. Standard - Integrity

Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.

This standard requires that you develop and implement policies and procedures to protect the integrity of ePHI in your practice. The WEDI white paper describes the integrity standard and its one implementation specification on page 26. Here are some key points:

1. Integrity of your ePHI focuses on keeping the ePHI the same as when you received it.
2. WEDI recommends that you can accomplish this standard by complying with the other standards described in the white paper.

A. Mechanism to authenticate ePHI (Addressable) - Implementation specification

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

Read the two paragraphs in the WEDI white paper at the bottom of page 27. This implementation specification describes putting in place appropriate technical processes to authenticate the identity of persons attempting to access ePHI. For small practices the focus of authentication would be on remote access as discussed in the second paragraph.

Checklist:

1. Ensure virus protection, firewall protection, access controls and other administrative and physical safeguards are in place.

4. Standard - Person or entity authentication

Implement procedures to verify that a person or entity seeking access to ePHI is the one claimed.

The WEDI white paper recommends procedures to control access and to determine how to monitor and enforce access.

Checklist:

1. Develop procedures that define access control, monitoring of access and enforcement of access.

5. Standard: Transmission security

Implement technical security measures to guard against unauthorized access to ePHI that is being transmitted over an electronic communications network.

You must implement security measures to protect against unauthorized access to ePHI you transmit over an electronic network. This standard [the LAST ONE!] has two implementation specifications that must be examined and they are both “addressable.”

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

The WEDI white paper has one brief paragraph on integrity controls on page 27. Here are some of the key points of this “addressable” specification:

1. This implementation specification relates to the issues described in the Technical Safeguard.
2. You must ensure ePHI is not improperly modified.
3. You may need to put in systems to control and monitor access to ePHI.
4. You may need to consider auditing changes to ePHI to ensure they are legitimate and are made by authorized people in your practice.

Checklist:

1. Examine how you ensure security of ePHI that you transmit electronically.
2. If you believe it is sufficient, document what you do.
3. If you believe it is inadequate to secure ePHI, change your security measures as you transmit ePHI to ensure it is not improperly modified.

B. Encryption (Addressable) – Implementation Specification
Implement a mechanism to encrypt ePHI whenever deemed appropriate.

Again, this implementation specification is “addressable.” The focus of using encryption is where you believe your computer systems may be at risk. Portable devices or PDAs as mentioned in the WEDI white paper on page 27 can be at risk.

Checklist:

1. Determine if there are applications for encryption that are appropriate for your practice.
2. If encryption is appropriate, obtain software to provide encryption.
3. If you believe encryption is not necessary, document your decision for you HIPAA Security Standards files.

6. Policies and Procedures

Just as you developed and implemented policies and procedures for the HIPAA Privacy Rule, you must develop policies and procedures for the HIPAA Security Standards. Your policies and procedures can be short and focused to meet your needs.

Look over the two paragraphs on page 28 of the WEDI white paper describing policies, procedures and documentation.

Some of your written office policy manual procedures may already cover some of the security issues in the HIPAA Security Standards. For example, you may have termination policy and procedure that addresses many of the suggestions described in the WEDI white paper under the Workforce Security Standard and its implementation specification on Termination Procedures [pages 10 and 11]. Update your policy and procedures to comply with the security standards.

If you need examples of policies and procedures, check with your medical associations your practices belongs to or with lawyers who work in health law.

Checklist:

1. Look through the policies and procedures required by the standards and the implementation specifications and make two lists:
 - a. List of policies and procedures that are need that you do not have.
 - b. List of policies and procedures that you have, but you must modify so they comply with the HIPAA Security Standards.
2. Write needed policies and procedures and update existing policies and procedures.