

---

WEDi - Strategic National Implementation Process (SNIP)

# Small Practice Implementation



SNIP

Small Practice Implementation

Version 2.0 – 10/15/2002

Discussion Draft

***Workgroup for Electronic Data Interchange***

*12020 Sunrise Valley DR., Suite 100, Reston, VA. 20191*

*(t) 703-391-2716 / (f) 703-391-2759*

© 2002 Workgroup for Electronic Data Interchange, All Rights Reserved

# Contents

- Small Practice HIPAA Implementation 1**
  - Disclaimer..... 1
  - Background..... 1
  - Application of HIPAA to Small Provider Practices ..... 2
  - What Does Administrative Simplification Mean? ..... 2
  - Transactions..... 3
  - Transactions Compliance Date Extension ..... 4
  - Privacy and Security ..... 5
  - Overview of Awareness Program..... 5
    - Preliminary Awareness Program ..... 5
    - Privacy and Security Self Assessment (#1)..... 6
    - Transactions Self Audit ..... 7
    - Documents..... 7
    - Educational Programs..... 9
  - Trusted Sources ..... 9
  - Costs and Resources ..... 9
  - Risk Considerations..... 10
  - Conclusion ..... 10
  - Other Sources of Information ..... 10
  - Acknowledgements ..... 11
  
- Appendix I: Model HIPAA Privacy And Security Audit For Small Practices 12**
  
- Appendix II: Model HIPAA Transactions Audit 17**
  
- Appendix III: Acknowledgement of Receipt of Notice of Privacy Practices 21**
  - Background..... 21
  - Specifications..... 22
  - Exception to Requirement to Provide Notice ..... 22
  
- Appendix IV: Authorization Forms 23**
  - Background..... 23
  - Specifications: General ..... 23
  - Special Situation: Psychotherapy Notes ..... 24
  - Specifications: Authorizations Requested by Practice for its Own Uses and Disclosures ..... 24
  - HIPAA Authorization Form Checklist ..... 25
  
- Appendix V: Disclosure Without Written Authorization 26**
  
- Appendix V: Disclosure Without Written Authorization 26**
  
- Appendix VI: Notice of Privacy Practices 27**

Background.....	27
Required Elements.....	27
Provision of Notice.....	30
Other Provisions.....	30
HIPAA Notice of Privacy Practices Checklist.....	31

**Appendix VII: Policy Manual 32**

Background.....	32
Notice of Privacy Practices for Confidential Information.....	32
Uses and Disclosures of Confidential Information.....	32
Provision of Notice of Privacy Practices for uses or disclosures to carry out treatment, payment, or health care operations.....	33
Uses and disclosures for which an authorization is required.....	33
Exceptions to the requirement to obtain authorization.....	33
Other requirements relating to uses and disclosures of confidential information.....	33
“De-identification” of Confidential Information.....	33
Limited Data Sets.....	35
Limited Data Sets.....	35
“Minimum Necessary” Provisions.....	35
Marketing Restrictions.....	36
Fund Raising Restrictions.....	37
Access of Individuals to Confidential Information.....	37
Amendment of Confidential Information.....	40
Accounting for Disclosures.....	43
Business Associates.....	43
Complaints to the Practice.....	44
Mitigation.....	44
Refraining From Intimidating or Retaliatory Acts.....	44
Waiver of Rights.....	44
Ensuring Confidential Information is Secure.....	45
Access Control.....	45
Physical Safeguards.....	46
Audit Controls.....	46
Internal Audit of System Activity.....	47
Contingency Planning.....	47
Training.....	47
Sanctions.....	48
Policy Manual Checklist.....	48

# Small Practice HIPAA Implementation

---

## Disclaimer

This document is Copyright © 2002 by The Workgroup for Electronic Data interchange (WEDI). It may be freely redistributed in its entirety provided that this copyright notice is not removed. It may not be sold for profit or used in commercial documents without the written permission of the copyright holder. This document is provided "as is" without any express or implied warranty.

While all 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. If you require legal advice, you should consult with an attorney. The information provided here is for reference use only and does not constitute the rendering of legal, financial, or other professional advice or recommendations by the Workgroup for Electronic Data Interchange. The listing of an organization does not imply any sort of endorsement and the Workgroup for Electronic Data Interchange takes no responsibility for the products, tools, and Internet sites listed.

The existence of a link or organizational reference in any of the following materials should not be assumed as an endorsement by the Workgroup for Electronic Data Interchange (WEDI), or any of the individual workgroups or sub-workgroups of the Strategic National Implementation Process (SNIP).

### *Document is for Education and Awareness Use Only*

The HIPAA Security and Privacy requirements are designed to be ubiquitous, technology neutral and scalable from the very largest of health plans, to the very smallest of provider practices. As the Privacy Rule and a majority of the proposed Security Rule relates to policies and procedures, many covered entities will find compliance not an application of exact template processes or documentation, but rather a remediation based on a host of complex factors unique to each organization.

---

## Background



*Virtually every small practice will be subject to HIPAA. In fact, it has been estimated that over 400,000 small practices need to come into compliance with HIPAA. Few can afford to hire a soup-to-nuts "HIPAA" consultant to help them come into compliance.*

Where are most of these practices with respect to coming into compliance with HIPAA? It is evident from talking to many small practices that while most have heard of HIPAA, and most know something is coming, few have any specific knowledge of HIPAA and few have any information regarding how to comply with HIPAA. Most significantly, many are starting to hear presentations and read information about HIPAA that is often not accurate and some of that misinformation is leading to a high level of anxiety among small practices.

The Small Provider Practice HIPAA Implementation Workgroup was established as a result of the June 19, 2001, WEDI SNIP quarterly meeting in San Francisco. It grew out of discussions regarding how to reach small practices and ensure that they come into compliance with HIPAA. These small practices represent the vast majority of health care providers. WEDI SNIP recognizes that many large, more sophisticated "covered entities" are preparing for HIPAA. However, there is a growing recognition that the success of HIPAA is dependent on health care providers

in small practices becoming informed about HIPAA, evaluating what they need to do to come into compliance with HIPAA (“gap analysis”), developing an implementation plan, and changing their business practices accordingly. There is a great need in this area.

This white paper is intended for use by trusted entities – associations, consultants, and others – to inform small practices about HIPAA. It outlines an awareness campaign, with specific approaches and tools, to enable small practices to come into compliance with the HIPAA requirements. Specifically, the white paper has two central goals:

- to present a strategy to inform small practices about HIPAA using trusted sources; and
- to give specific guidance which can be provided to small practices to enable them to become HIPAA compliant.

It is important to keep in mind that small practices need the basics – not a detailed discussion of the more esoteric points in HIPAA. These practices want simple, straightforward, and, to the extent possible, non-technical information about HIPAA. Where possible, it is recommended that non-technical language be used and that practices be encouraged to keep HIPAA implementation as simple as possible. This white paper uses less technical language that will make more sense to small practices. This white paper is written so that readers can start to think in simpler terms needed to help small practices make sense of HIPAA. More technical specifications are included in the footnotes.

---

## Application of HIPAA to Small Provider Practices



HIPAA applies to “covered entities.” In general, HIPAA applies to a small provider practice if that practice submits claims electronically either directly or through a billing service or “clearinghouse.” HIPAA does not apply to a practice that does not submit any information electronically.<sup>1</sup>

In addition, Sec. 3 of the Administrative Simplification Compliance Act (signed into law in December 2001) contains a section entitled “Enforcement through exclusion from Participation in Medicare” and requires that for claims submitted to Medicare on or after October 16, 2003, “no payment may be made under part A or part B of [Medicare] for any expenses incurred for items or services ... for which a claim is submitted other than in an electronic form specified by the Secretary.” This payment prohibition does not apply to small practices: (i) when there is no method available for the submission of claims in an electronic form; (ii) in the case of a physician, practitioner, facility, or supplier (other than a “provider” of services as defined under Medicare), when the entity has fewer than 10 full-time equivalent employees; and (iii) under such unusual cases as the Secretary may find appropriate.” Note: No guidance has been given regarding what the Secretary might find appropriate.

---

## What Does Administrative Simplification Mean?

The administrative simplification provisions of HIPAA have two parts:

- development and implementation of standardized electronic transactions; and
- implementation of privacy and security procedures to ensure the confidentiality of and prevent the misuse of patient information.

The standardized transactions must be used no later than October 16, 2003 (if you apply for an extension from HHS by October 16, 2002), while the privacy requirements must be implemented by April 14, 2003. The security

---

<sup>1</sup>Technically, HIPAA applies to a health care provider who transmits any health information in electronic form in connection with a transaction covered by HIPAA. It is important to note that electronic form includes diskette, CD, and FTP. These transactions include electronic claims, eligibility requests, and claims status inquiries to health plans, other payors, and clearinghouses. FAXes are not considered electronic transactions.

requirements are not yet finalized, but some security measures must be implemented in accordance with the privacy requirements in order to ensure the privacy of patient information.

---

## Transactions

HIPAA states that any practice that electronically sends or receives certain transactions must send or receive them in a standard format. In addition, a practice is covered by HIPAA if the practice uses any of these standard electronic transmission formats. For practical purposes, for a covered practice, all confidential information – electronic *and* paper – must be protected.

The standard electronic transactions covered by HIPAA are as follows:

### **ELECTRONIC TRANSACTIONS\***

- Claims or Equivalent Encounters (837)
  - Remittance and Payments Advice (835)
  - Claims Status (276/277)
  - Enrollment and Disenrollment in a Health Plan (834)
  - Premium Payment (820)
  - Eligibility Inquiry and Response (270/271)
  - Referral Certification and Authorization (278)
  - Coordination of Benefits (837)
  - First Report of Injury (148)
  - Claims Attachments (275)
- \*Numbers in parentheses designate the technical (ASC X12) designation of the specific electronic standards.

The first three transactions are those most commonly used by practices. In addition, many physicians use electronic eligibility inquiries and responses and referral certifications and authorizations, particularly those involved in managed care.

In theory, a practice will be able to fill out a claim for a patient – regardless of the payor – and submit the claim electronically to any payor. This means that not only will the standardized transactions be required (with set electronic *formats* and data fields), but uniform code sets and *identifiers* also will be used. These are as follows:

### **CODE SETS**

- Diagnosis Codes: ICD-9-CM
- Procedures Codes: CPT-4
- Physician Service Codes: CPT-4
- Inpatient Service Codes: ICD-9-CM
- Other Service Codes: HCPCS (with no more local codes)
- Drug Codes: NDC (may be changed back to “J” codes in hospitals)
- Dental Codes: CDT

### **NATIONAL IDENTIFIERS**

- Provider
- Health Plan
- Employer
- Individual (on hold)

This means that every payor will accept the electronic transactions with the same uniform code sets (e.g., CPT-4 with *no* local codes or payor-specific codes) and with the same national identifiers, e.g., a provider will have a single identifier for all payors, not a different identifier for each payor.

Most small practices will not have to worry about the technical specifications of the transactions and code sets. However, most practices will rely heavily on their patient accounting or practice management system vendors for

assistance in complying with the HIPAA transaction standards (as well as many of the technical components of the security and privacy standards).

The following questions will help practices begin the HIPAA conversation with vendors. Some questions relate to system capabilities to meet HIPAA requirements; others address operational issues, including how the system may help improve efficiencies. **Practices must be sure to ask whether changes will be made as part of a maintenance contract or if there will be additional charges.** They should be encouraged to get the answer in writing.

- When will the software have the capability of exchanging HIPAA-compliant versions of the electronic transactions (listed above)?
- When will the software support the required code sets (listed above)?
- Will it be necessary to add new or different information in order to meet the requirements of the electronic transactions?
- Has the software data base been modified to allow entry and storage of all required and situational data elements used to build the HIPAA transactions?
- Will the software let the practice exchange these transactions directly with payers, or do they have to go through a specific intermediary (a clearinghouse)?
- Has the software received certification that it can, in fact, generate HIPAA compliant transactions? If so, from which certification authority? (**Note:** Certification is not required by the HIPAA regulations; however, it is recommended that a certification authority certify the files, once certification authorities are identified.)
- How can the practice use the software to test the new transaction formats with my major payers?
- When can the practice use software to test the new transaction formats with my major payers?
- Will the practice be able to continue processing claims in existing electronic formats while the testing of new formats is being completed?
- How will the software accommodate the anticipated National Provider Identifier and the National Payer Identifiers?
- If HHS proceeds with the development of a patient identifier, how will the software accommodate it?
- What are the vendor's contingency plans if it cannot deliver the necessary modifications on time?
- Does the vendor assist with disaster recovery and/or emergency operations by providing alternative files, eligibility lists, accounting for disclosures, and so forth?

---

## Transactions Compliance Date Extension

The Administrative Simplification Compliance Act was enacted in December 2001. The legislation granted covered entities – health plans, providers, and clearinghouses – an additional year to implement the HIPAA standard transactions. However, in order to qualify for the extension, a small practice must have submitted to the Secretary, no later than October 15, 2002, “a plan of how the person will come into compliance with the requirements ... not later than October 16, 2003.” There appears to be no way for applying for an extension after that date.

In general, a person who fails to submit a plan and is not in compliance with the HIPAA transaction standards may be excluded from Medicare, unless they are doing all of their business on paper – non-electronic.



***This legislation does not change the April 14, 2003, deadline for implementing the HIPAA Privacy requirements. Small practices will still be required to comply with the privacy standards by April 14, 2003.***

---

# Privacy and Security

Privacy refers to limiting the availability and use of confidential data.<sup>2</sup> Security refers to the systems used to physically and electronically limit access to confidential data. Privacy refers to what must be kept confidential. Security refers to how it is to be kept confidential.

The final privacy rules have been issued and small practices will be required to comply with these rules no later than April 14, 2003. Clarification and changes to the final rule – the final Privacy modification – was published in the August 14, 2002, *Federal Register*. According to the Health and Human Services Fact Sheet which reviewed the August 14, 2002, final Privacy modifications, the changes were made to ensure that the Privacy Rule provides strong privacy protection without hindering access to quality health care.” This White paper includes those final modifications and related requirements.

The final security rules have not been issued. Nonetheless, practices will have to implement appropriate security measures to ensure the privacy of confidential information.

WEDI/SNIP will provide guidance to help small practices meet the privacy and security requirements of HIPAA. This guidance will recommend a multi-pronged strategy and will include increasing awareness of HIPAA, providing basic information, and describing what needs to be contained in the HIPAA-required documents. Most of what needs to occur is not technology-related changes. Rather, it relates to business and office practice changes aimed at protecting the confidentiality of patient information.

---

## Overview of Awareness Program

### Preliminary Awareness Program

Surveys suggest that while most small practices have heard of HIPAA, they are generally not aware of the specific requirements of HIPAA. The surveyors go on to show that most small practices believe they already are operating their practices in a fashion that ensures the privacy of patient records for the most part. While this is true, the awareness program needs to inform small practices that HIPAA is coming and give them some sense that they will need to make changes to their practices – no matter how thorough their current privacy policies and procedures.

The first step toward HIPAA compliance in small practices is making the practices aware of HIPAA and starting some basic educational efforts. As providers learn more about HIPAA, more substantive materials can be presented. The goal is to ensure small practices come into compliance with the HIPAA standards in a timely fashion. ***Hopefully you already have completed this step and your providers are aware of HIPAA and its basic requirements.***

Toward that end it is necessary to provide some basic information to providers. Most practices know something is coming, but they don't know what, and they are starting to get some incorrect or misleading information from sources that do not clearly understand HIPAA or are trying to sell unneeded services.

The first message to convey to small practices is that HIPAA is coming and it will need to prepare. Second, the small practice should be advised ***“DON'T PANIC.” At least not yet.*** There is time to come into compliance with the HIPAA requirements, and WEDI/SNIP, working through its partners, is planning to develop materials and strategies to help small practices do so – both the transactions and the privacy and security requirements.

A key to success with the small practices is to communicate to the providers in simple, non-complex terms. For example, providers do not need to know that the privacy regulations only apply to “protected health information.”

---

<sup>2</sup>The rule does not actually address the release of “confidential information.” Rather, it refers to the release of “protected health information (PHI).” For our purposes, referring to “confidential information,” while imprecise, will be more meaningful and understandable to small practices.

Rather, it is sufficient – in the initial steps of building awareness, to use terms providers will understand, e.g., HIPAA will require providers to protect “confidential” patient information.

In addition, an incremental approach is recommended that makes providers aware of some of the key provisions of HIPAA and gets them thinking about some of the big issues related to comply with HIPAA. A comprehensive approach to HIPAA – upfront – will cause anger and confusion and lead small practices to the conclusion that HIPAA is so complex that compliance is impossible.

*Every possible channel should be used to get this message out.* See “Trusted Sources” below (page 9).

## **Privacy and Security Self Assessment (#1)**

Small practices need basic practical information about HIPAA. A good way to engage small practices is to provide them with a preliminary self assessment – a privacy and security walk through of their practice. The self assessment should address a number of key issues, provide an understanding of time limits, and make sure practices understand the need to change business practices.

The information should be in simple terms and should stay away from jargon whenever possible. This means that the information may be imprecise, but that is preferable to providing technical information that is not used. For example, using the term “confidential information” is close enough for practical purposes, and it is an understandable term. The self assessment will have to make clear that it is not using precise terms and is attempting to make the regulations more understandable.

In addition, the self assessment should not be comprehensive. At this point the key is to give small practices a flavor of the issues that need to be addressed, not to overwhelm them. It is important to engage the practices in a process and get them started.

The self assessment can be structured in a number of ways. Possible areas for the self assessment include:

- patient sign in sheets must include only limited information;
- leaving medical charts around the office site and use of clear plastic chart holders on exam room doors;
- the posting of patient schedules;
- holding confidential conversations where they can be easily overheard by third parties;
- computer screens in plain view;
- staff regularly changing passwords and safeguarding access to work areas;
- information accessible only to authorized staff, including medical records, lab reports, and faxes;
- safeguards documented regarding transfer of paper and electronic medical records, orders, images, and lab specimens;
- HIPAA complaint, confidentiality statements and written privacy policies;
- documented policies and procedures when employment terminated, including return of all keys, cards, and change codes and locks;
- employee handbook/documentation HIPAA compliant with respect to security training, termination policies and procedures, etc.;
- documented procedures to protect confidential information, if office equipment or files are taken from the premises;
- policies, procedures and training in place for off-site functions, e.g., transcription, accounting or claims filing;
- inventory of computer systems, and software;
- regular virus check and mitigation program in place;
- disaster plan to include contingency plans in event of systems failure;
- confidential information stored electronically, with appropriate safeguards;
- Internet and phone transmissions secure; and
- protection of e-mail communications that contain confidential information.

Ideally this self assessment will be made available to small practices through sources they trust at no or a minimal charge and not as a teaser seeking to sell further “HIPPA” services. State and national professional associations could fit this bill.

A model self assessment is presented in Appendix I (see page 12). *Hopefully by now you have already provided this kind of basic information to your providers.*

## Transactions Self Audit

Small practices also need basic practical information about the HIPAA transactions. The self assessment should address a number of key issues and make sure practices understand the need to make changes soon.

As with the privacy and security audit, the information should be in simple terms and should stay away from jargon whenever possible. In addition, the self audit should not be comprehensive. The key is to give small practices a flavor of the issues that need to be addressed, not to overwhelm them. It is important to engage the practices in a process and get them started.

The self audit can be structured in a number of ways. The key is for practices to understand what questions to ask their vendors – software companies and clearinghouses (billing services). They also need to understand how to proceed based on the vendor responses.

As with the privacy and security audit, the transactions assessment should be made available through trusted sources free of charge or at a small cost, and not as a teaser seeking to sell further “HIPPA” services. State and national professional associations could fit this bill.

A model transactions self assessment is presented in Appendix II (see page 17).

## Documents

Most small practices do not have a great deal of resources for attorneys and consultants. Nonetheless, all small practices are required to use a number of legal documents in order to comply with the HIPAA regulations. These documents are specified in great detail in the privacy regulations and in the Appendices to this white paper. They include:

- **Notice of Privacy Practices:** Each small practice must make available to each patient or prospective patient a “Notice of Privacy Practices.” The Notice must inform the individual of the uses and disclosures of confidential information that may be made by the practice, and of the individual’s rights and the practice’s legal duties with respect to confidential information (see page 27). Health care providers providing direct care to a patient must secure an acknowledgement that the patient received a copy of the Notice of Privacy Practices no later than the first date of service delivery, beginning April 14, 2003. (In an emergency situation, the acknowledgement must be obtained as soon as reasonably practicable after the emergency treatment.) In instances where the patient does not receive the notice, the provider must document that a “good faith effort” was made to get the notice to the patient. The required documentation may be included in the patient’s medical record.
- **Written Acknowledgement:** After providing the offices’ Notice of Privacy Practices, each practice providing “direct treatment” to a patient must make a good faith effort to get a written “acknowledgment” from that patient or prospective patient demonstrating that the patient had the opportunity to review the practice’s use and/or disclosure<sup>3</sup> of confidential information<sup>4</sup> for treatment,<sup>5</sup> payment,<sup>6</sup> or health care

---

<sup>3</sup>“Use” refers to the use of information inside a covered entity. “Disclosure” refers to the release of information outside a covered entity.

<sup>4</sup>The rule does not actually address the release of “confidential information.” Rather, it refers to the release of “protected health information (PHI)” contained in “designated record sets.” For our purposes, referring to “confidential information,” while imprecise, will be more meaningful and understandable to small provider practices.

operations<sup>7</sup> (see page 17). Small practices might want to consider using a standard form to document that the Notice was provided.

- **Authorization Forms:** A practice must get a signed “authorization” to use or disclose information for most situations beyond treatment, payment, and health care operations. [Use and disclosure for treatment, payment, and health care operations are allowed since the Notice of Privacy Practices describes how information will be used for these purposes. While there are no requirements for providers to develop authorizations, providers may want to do so in some instances as a service to patients and as a protection for the practices (see page 23). [Authorization forms require a lot of state-specific materials, and so will likely vary considerably from state to state.]
- **Policy Manual:** Each practice is required to implement policies and procedures with respect to confidential information that are designed to comply with the HIPAA privacy and security regulations. The policies and procedures must be reasonably designed, taking into account the size of and the type of activities that relate to the confidential information of the practice, to ensure compliance. *Each practice will need to develop a policy manual to demonstrate compliance with this requirement* (see page 32).
- **Business Associate Agreements:** Each practice will need to have written agreements with “business associates” such as liability insurers, attorneys, transcription services, and copy services. [A model agreement is provided in the Preamble for the final Privacy modification.] Written agreements are not needed between a practice and another health care provider, health insurance company or other payors, or clearinghouses. The modifications to the Privacy Rule allow for additional time to be allotted to those practices who already have business associates under contract if those contracts are due to be renewed between April 14, 2003 and April 14, 2004. However, certain components of the rule must be adhered to (such as the requirement that accounting of disclosures must be tracked – even by the business associates), so that practices should do their best to complete business associate contracting by April 14, 2003.

---

<sup>5</sup>“Treatment” means the provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another.

<sup>6</sup>“Payment” is broadly defined and includes the activities undertaken by a physician to obtain or provide reimbursement for the provision of health care. This includes: (1) determinations of eligibility or coverage (including coordination of benefits or the determination of cost sharing amounts), and adjudication or subrogation of health benefit claims; (2) billing, claims management, collection activities, obtaining payment under a contract for reinsurance (including stop-loss insurance and excess of loss insurance), and related health care data processing; (3) review of health care services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges; and (4) utilization review activities, including precertification and preauthorization of services, concurrent and retrospective review of services.

<sup>7</sup>“Health care operations” refers a large number of activities, including (1) conducting quality assessment and improvement activities; (2) reviewing the competence or qualifications of health care professionals; (3) underwriting, premium rating, and other activities relating to the creation, renewal or replacement of a contract of health insurance or health benefits, conducting or arranging for medical review; (4) legal services, and auditing functions, including fraud and abuse detection and compliance programs; (5) business planning and development; (6) business management and general administrative activities including management activities, customer service, and resolution of internal grievances.

## Educational Programs

Many small practices will find direct educational programs a great help in coming into compliance with the rules. It is important to develop focused programs aimed at meeting the needs of small practices. Such programs need to provide practical information and need to recognize that most small practices do not have a great deal of resources for educational programs (they must be priced very reasonably) and for the most part they cannot afford HIPAA consultants. Ideally these programs will be sponsored by trusted partners, e.g., state societies representing the practices.

The programs will need to highlight the policies and procedures that must be followed by practices and must provide practical advice. Much of the basic information is detailed in this white paper developed by the Small Practice Implementation Sub-Workgroup. It is important to let practices know that there is time to come into compliance and that comprehensive educational programs are being developed to meet their needs.

---

## Trusted Sources



It is important that small practices receive information regarding HIPAA from trusted sources. This information needs to be distributed to physicians, podiatrists, physical therapists, acupuncturists, clinical psychologists, and many others. These practices need to receive the information from sources they trust, e.g., membership societies. The information must come from a believable source, a source that practices view as working for – not against – them.

There are a variety of possible trusted sources for practices.

- If there is a regional SNIP, the regional SNIP and its partners, especially representatives of small practices involved in the regional SNIP, may develop and distribute HIPAA materials to practices.
- Some local or state governmental agencies may facilitate the development and distribution of materials or encourage representatives of small practices to help their members become HIPAA compliant. Departments of public health and other governmental agencies that are directly affected by confidentiality and privacy laws or that license or regulate practices may be in a good position to facilitate action.
- Individual provider associations – working alone or in concert with other associations – may take the lead and develop materials for their members. It is important to keep in mind there is a high level of interaction among different providers types, and that small provider groups may want to work together in a coordinated fashion. For example, physicians often refer to speech therapists, psychologists, and other groups of providers.
- Many providers have good relationships with their payors and would consider them trusted sources.

---

## Costs and Resources

Small practices will have to expend significant resources to ensure that they are in compliance with HIPAA. Each practice will have to

- take time to understand the basics of HIPAA;
- undertake an initial practice audit and evaluate policies and practices which need to be revised;
- develop or adopt a number of documents for use by its practice;
- change policies and procedures as necessary to make them HIPAA compliant;
- complete a final audit to ensure the practice is HIPAA compliant; and
- on an ongoing basis, monitor the practice to ensure it remains HIPAA compliant.

These costs may be significant, and will doubtlessly require significant time of individuals in the practice.

It is hoped that trusted sources that provide small practices with support will enable them to become HIPAA compliant in an efficient and straight forward fashion.

---

## Risk Considerations



A small practice's decisions regarding the depth and breadth of the changes it needs to make to implement HIPAA can be influenced by physical factors such as its size, and by business factors such as acceptable levels of risk.

- A. **Critical: Size**: The larger a provider practice, the more its resources and the greater its potential cache of confidential information. Accordingly, larger practices are expected to put more resources into addressing issues related to patient privacy and the security of patient information. Even the smallest practices, e.g., solo provider offices, are required to comply with the standards.
- B. **Critical: Sophistication**: The more sophisticated a provider practice and its information systems, the more precisely the practice will be expected to comply with the regulations.
- C. **Policy/Procedure: Decision Making**: Small practices have different decision making (management) structures in place. Those structures may have to change to ensure that appropriately qualified and trained personnel are making decisions related to patient privacy and the security of information. The particular decision making structure and authority within a practice must ensure compliance with the regulations.



While all practices must comply with the regulations, practices with a history of compliance issues with HHS related to other programs (e.g., Medicare and Medicaid) should be particularly careful to demonstrate compliance, as they are most likely to come under further HHS scrutiny. In addition, practices have to be sensitive to any particular needs and concerns of their communities. To the extent possible, practices should meet the expectations of their patients.

---

## Conclusion

The task of ensuring that small practices come into compliance with HIPAA is significant. It will require a concerted effort by many individuals and organizations. It is hoped that the plans outlined in this white paper will provide a road map for trusted sources to provide consistent information to practices. It also is hoped that the information in the white paper can be used by trusted sources to design specific guidance for their small practices.

Trusted sources are encouraged to use the approaches and information included in this white paper. WEDI/SNIP expects that such organizations will acknowledge WEDI/SNIP as the source of the approaches and the information, and contact WEDI/SNIP if any questions arise regarding the use of this copyrighted white paper.

---

## Other Sources of Information

*Any other URLs, papers or organizations that would be a resource for this subject need to be identified and included in the paper.*

WEDI/SNIP Web Site – [snip.wedi.org](http://snip.wedi.org)

Workgroup for Electronic Data Interchange (WEDI) [www.wedi.org](http://www.wedi.org)

Other sources of HIPAA privacy and security information can be found on the WEDI/SNIP Web site at <http://snip.wedi.org/public/articles/index.cfm?Cat=48>.

---

# Acknowledgements

WEDI/SNIP would like to express its appreciation to the authors for their efforts in preparing this White Paper:

Paul Barringer  
Smith Anderson Blount Dorsett Mitchell & Jernigan

\*\*Lesley Berkeyheiser, Principal  
The Clayton Group, LLC

\*\*Gerald "Jud" E. DeLoss, Esq.  
Barnwell, Whaley, Patterson & Helms, LLC

\*\*William G. Esslinger, Jr., Vice President, General Counsel  
& Chief Privacy Officer  
Greenway Medical Technologies

Steven M. Fleisher, Legal Counsel  
California Medical Association

\*\*Nelson Hazeltine, President  
iVista Group

Robert John Kane, Legal Counsel  
Illinois State Medical Society

Libby Lincoln, Vice President, Law and Health Policy  
Midwest Medical Insurance Company

Sue Miller, Corporate Compliance Manager  
IDX Systems Corporation

Victoria Sterling, Senior Vice President & General Counsel  
OMSNIC (OMS National Insurance Company RRG)

\*\*LuAnn Weis, Medical Practice Consultant  
HealthCare Solutions of NJ

**Small Provider Implementation Sub-Workgroup Leader:**

\*\*Andrew H. Melczer, Ph.D.  
Vice President, Health Policy Research  
Illinois State Medical Society

**\*\*Involved in October 2002 Revision of Version 2.0**

# Appendix I: Model HIPAA Privacy And Security Audit For Small Practices

THIS IS A MODEL AUDIT. IT WILL NEED TO BE CHANGED TO MEET THE PARTICULAR NEEDS AND CIRCUMSTANCES OF ANY TRUSTED SOURCES DEVELOPING AN AUDIT.

The health care industry must come into compliance with the new privacy and security requirements of the Health Insurance Portability and Accountability Act (HIPAA). These requirements apply to payors, institutions, and health care professionals and providers, from the largest multi-state integrated delivery networks to solo practice professionals.

*All individuals involved in the health care delivery system must start now to prepare for HIPAA.* Actually, HIPAA does *not* apply to all health care providers. Rather, it only applies to those who engage in “standardized electronic transactions,” as defined by the federal government. For example, if you submit claims or perform eligibility checks electronically, either directly or through a third party, e.g., a billing service, then you are subject to the HIPAA privacy and security requirements. In addition, if you perform any transactions electronically, the information in both your *electronic and paper* records are covered by HIPAA.

The manner in which individuals need to prepare for HIPAA implementation varies depending on the size and technological sophistication of the individuals involved. This HIPAA Privacy and Security Audit, developed by the Illinois State Medical Society, focuses on solo and small practice health care professionals. Such practices tend to have less technological sophistication, and do not, for the most part, have the resources to hire consultants to help them meet the HIPAA privacy and security requirements.

*This audit is intended to be a starting point for solo and small practice professionals.* This includes physicians, dentists, physical and occupational therapists, psychologists, social workers, and all other health care professionals. This audit provides professionals with a list of 20 considerations. Each of these considerations is presented in the form of a statement. Depending on how you respond to these considerations, you can determine how much you will have to do to prepare for HIPAA. To assist you in thinking about the changes you may have to make in your office, a series of suggestions are presented under each consideration regarding how to ensure your practice meets the HIPAA privacy and security requirements.

*This audit is a preliminary step. It is not intended to be comprehensive and it is not intended to provide a comprehensive guide to meeting the HIPAA privacy and security requirements.*

Further information will be developed by WEDI/SNIP over the next several months. These documents will help you to prepare for HIPAA. In the meantime, it is important that you become aware of, and get a start toward, meeting the HIPAA requirements.

For further information or to comment on the audit, please contact \_\_\_\_\_.

The following 20 considerations are intended to help you audit your practice and to determine if you will need to make any changes to meet the privacy and security requirements of the Health Insurance Portability and Accountability Act (HIPAA).

**If you answer any of the following statements “False” you may need to change office procedures.**

- 1. My office uses a patient sign in sheet that does not include confidential patient information.** \_\_\_\_\_ True \_\_\_\_\_ False

A sign-in sheet will allow patients who come into your office later to learn the identity of other patients who came to your office earlier. This is acceptable, so long as the sign-in sheet does not contain confidential patient information such as reason for the visit. In some cases this information seems very innocent. However, some physicians specialize in patients with sensitive issues or conditions, e.g., cancer, psychological problems, or pregnancy, and simply disclosing that an individual has had an appointment with you for a specific purpose may be a breach of patient confidentiality. At a minimum, the sign-in sheet should be changed periodically during the day.

- 2. My office does not place patient schedules in any places that may be seen by patients or other non-staff individuals.** \_\_\_\_\_ True \_\_\_\_\_ False

Some practices print out the schedule for the day and post it for the professional staff. Often the schedule is posted where it may be seen by a patient – either in an examination room, in a corridor, or on a door. This may result in the unauthorized disclosure of patient information. As with consideration 1. above, disclosing information about a patient may be a breach of patient confidentiality.

- 3. In my office, all confidential conversations take place to the maximum extent possible in areas that cannot be overheard by other patients or non-staff individuals.** \_\_\_\_\_ True \_\_\_\_\_ False

Conversations may be easily overheard in many settings. For example, a receptionist may schedule appointments or provide test results over the telephone. This requires taking and verifying the name of the caller, as well as discussion of medical information, e.g., the reason for the appointment or the results of the tests. If patients and others are sitting in the waiting room, they may hear this exchange of confidential information, and this could represent an unauthorized disclosure of patient information. The same is true of conversations between staff members in the hallway and if a professional takes a call from a patient in the presence of another patient, e.g., in an exam room or if a professional dictates notes to a recording device. (Providers must use their best professional judgment to reduce the risk of such information being shared, but do not have to guarantee it can never occur. Further, in general structural changes are not necessary.)

- 4. In my office patients and non-staff individuals cannot gain access to our computers or fax machines and cannot view our computer screens.** \_\_\_\_\_ True \_\_\_\_\_ False

Offices use computers for a variety of reasons, including billing, accounts receivable, scheduling, and medical records. Usually computers and fax machines are placed only in the reception area, although sometimes they are throughout the office, including in patient exam rooms. It is important that only staff members can gain access to the fax machines and computers. These restrictions include restricted physical access as well as restricted viewing access. In addition, computers should have screen savers so that unauthorized people cannot read the information if they happen to wander into a restricted area, and computers should be password protected. When the staff person steps away from their computer for a period of time, the computer should automatically logout and the staff person should be required to re-enter his or her password.

- 5. Each computer user in my office has a personal computer password, these passwords change on a regular basis, and passwords of terminated employees get deleted immediately.** \_\_\_\_\_ True \_\_\_\_\_ False

It is important to ensure that each person in your office has access only to the computer(s) and information to which they are entitled. Toward that end, each user needs to have his or her own password. In addition, passwords need to be kept confidential (i.e., not shared with anyone else) and need to be changed on a regular basis to ensure security. Passwords must *never* be left on “Post-it” notes next to the computer.

- 6. In my office patients and other non-staff individuals do not have any opportunity to access patient medical records, laboratory reports, and faxes. \_\_\_\_\_ True \_\_\_\_\_ False**

Paper medical records are located in a number of places around the office, including the receptionist area, bins in the exam rooms, on the professional’s desk, and at check out. It is vital that no patient or non-staff individual have access to any medical records at any place in the office. For most offices, this will require a change in the manner in which medical records are handled and stored.

- 7. My office has formal documented procedures to ensure patient confidentiality when transferring paper files, orders, images, and specimens to other offices. \_\_\_\_\_ True \_\_\_\_\_ False**

It is very important that every office have formal policies for the transfer of confidential patient information outside its office. Your office staff must understand these policies. You must make sure that only appropriate information is transferred and that it is transferred to the proper individuals. (You may need specific authorization from a patient to transfer information.) If you use e-mail, you must ensure that the e-mail is secure. If you use couriers, you must ensure that they will keep the information confidential in transit and will deliver it only to authorized individuals. If you use a transcription service, you must ensure that the transcription service can keep your information confidential in compliance with the HIPAA requirements. Even if you currently have such policies, they will have to be reviewed to ensure that they meet the HIPAA requirements, and you may have to change your agreements with your business associates to ensure that they comply with the HIPAA requirements. Keep in mind that HIPAA does not restrict the confidential information that can be shared between providers.

- 8. My office has formal documented procedures for the acceptance of confidential patient information from outside of our office. \_\_\_\_\_ True \_\_\_\_\_ False**

As with records you send offsite, you will need to have formal policies for accepting confidential patient information from outside your office and keeping it confidential, including e-mail. Your office staff must understand these policies. Even if you have such policies in place, they will have to be reviewed to ensure that they meet the HIPAA requirements.

- 9. My office has confidentiality statements in place and we make patients aware of our confidentiality policies. \_\_\_\_\_ True \_\_\_\_\_ False**

HIPAA requires each health care professional to have Notice of Privacy Practices confidentiality statements. These statements must be posted in a prominent place in your office. In addition, patients must receive the Notice of Privacy Practices and acknowledge receipt of that Notice. The Notice will allow you to release their confidential information for billing and other purposes. Even if you have confidentiality policies in place and make patients aware of your policies, they will have to be reviewed to ensure they meet the HIPAA requirements.

- 10. My office has formal privacy and security procedures regarding access to confidential information, access to computer information, and access to areas of the office that may contain confidential information. \_\_\_\_\_ True \_\_\_\_\_ False**

Unauthorized personnel must never have access to confidential information. Your office must have formal policies and procedures to ensure that only appropriate staff and other individuals gain access to confidential information. This may mean limiting access to certain parts of your office, to certain computers, or to certain programs or files in your computers. (For example, if you have separate accounting staff, they do not need to see patient encounter notes, just the billing form prepared by the treating healthcare professional, while the cleaning staff should not be able to see any confidential information.)

- 11. My office requires the return of all keys and other items that allow access to the office and to computer files when a person no longer is authorized to access information.** \_\_\_\_\_ True \_\_\_\_\_ False

Unauthorized personnel must never have access to confidential information. This includes all staff and other individuals who may have, at one time, been authorized to have such access. Your office must have formal policies and procedures to ensure the return of all keys and other items that allow access to information, both physical access and computer access.

- 12. My office has formal privacy and security policies for all office personnel, training for all office personnel, and the training of each individual is documented.** \_\_\_\_\_ True \_\_\_\_\_ False

All office personnel must receive training about your privacy and security policies and records must be kept of the training. The policies must detail which personnel have access to different kinds of confidential information in different circumstances, personnel clearance procedures, procedures to be followed when a member of the office staff is terminated, and procedures for identifying and correcting potential problems. The training requirements should be included in your human resources policy manual or booklet. In addition, you must have a formal policy manual that details all of your privacy and security procedures. Even if you have a policy manual in place, it will have to be reviewed to ensure that they meet the HIPAA requirements.

- 13. If my office uses laptops or other portable equipment that holds confidential patient information, this equipment is secure and can only be accessed by authorized personnel.** \_\_\_\_\_ True \_\_\_\_\_ False  
\_\_\_\_\_ NA

Many offices use portable equipment, including laptops, calendars, and “personal assistants.” All of these devices may contain confidential information that must be kept secure in an appropriate fashion. Your office must have policies and procedures regarding the setup, use, security and disposal of this equipment.

- 14. My office has policies and procedures in place to ensure patient confidentiality by off-site contractors, such as billing and accounting services.** \_\_\_\_\_ True \_\_\_\_\_ False

You are responsible for ensuring your confidential information remains confidential, even when it is sent off-site. This is not a concern when you send information to another health care provider or a health insurance company – they also are required to comply with the privacy rule and protect the information they receive. In addition, most billing services will be covered by the rules, although you need to double check with them. However, many businesses are not covered by the rules, e.g., auditors and software vendors. You need to have agreements with these businesses to ensure the confidentiality of any patient information they will see or transfer.

- 15. My office has a comprehensive survey of all of our computer systems, including all software.** \_\_\_\_\_ True \_\_\_\_\_ False

The security rules require you to keep a complete listing of your computer systems, including all software. This will help you manage your systems and help to detect any problems that might lead to a breach of patient confidentiality. Remember: Confidential information is contained in billing and accounting records and in letters to patients and other health care providers, as well as in the medical records.

- 16. My office has a disaster plan to protect patient information, contingency plans in the event of a computer systems failure, performs regular virus checks, and corrects any identified problems.** \_\_\_\_\_ True \_\_\_\_\_ False

You must ensure that you can access confidential information, even in the case of a disaster. For computer records, this can be fairly simple – backup the computer files on a daily basis and store the backup offsite. For paper records, this can be more difficult. In addition, you must ensure your confidential information is safe and cannot be seen or altered without your permission. Electronic information – including billing records and correspondence – is subject to attack if it is not protected from computer viruses and unauthorized intruders (hackers).

**17. All confidential information – paper and electronic – is stored with appropriate safeguards.** \_\_\_\_\_ True \_\_\_\_\_ False

You must ensure that all confidential information is protected from inappropriate access. This includes both electronic and paper records. For electronic records, you need to use passwords and other methods to ensure that only authorized people have access to information. For paper records, you will need to ensure your records are stored in a secure manner.

**18. Internet transmissions, including e-mail, and telephone conversations are secure.** \_\_\_\_\_ True \_\_\_\_\_ False

You must be sure that internet and telephone conversations are secure. In the case of the internet – most commonly e-mail – you must ensure communications are “encrypted.” In the case of telephone conversations, you must make reasonable efforts to ensure that others are not listening in, e.g., on a second telephone. In most cases, the staff needs to have some assurance of the identity of the person with whom they are communicating.

**19. My office has patients sign a form acknowledging receipt of my Notice of Privacy Practices.** \_\_\_\_\_ True \_\_\_\_\_ False

Patients must sign a form acknowledging receipt of your Notice of Privacy Practices allowing you to release their confidential information for treatment, billing and other purposes. Even if you have such a similar form in place, you need to review it to ensure that it meets the HIPAA requirements.

**20. My office has confidentiality statements on all faxes and e-mail sent by the office staff.** \_\_\_\_\_ True \_\_\_\_\_ False

All faxes and e-mail should state the confidential nature of the contents and have instructions should the fax or e-mail be misdirected.

***This audit is a preliminary step. It is not intended to be comprehensive and it is not intended to provide a comprehensive guide to meeting the HIPAA privacy and security requirements.***

**Further information will be developed over the next several months. These documents will help you to prepare for HIPAA. In the meantime, it is important that you become aware of and get a start toward meeting the HIPAA requirements.**

***For further information or to comment on the audit, please contact \_\_\_\_\_.***

# Appendix II: Model HIPAA Transactions Audit<sup>8</sup>

THIS IS A MODEL AUDIT. IT WILL NEED TO BE CHANGED TO MEET THE PARTICULAR NEEDS AND CIRCUMSTANCES OF ANY TRUSTED SOURCES DEVELOPING AN AUDIT.

Health care professionals, including those in small practices, must come into compliance with new electronic transmission requirements of the Health Insurance Portability and Accountability Act (HIPAA). These requirements apply to payors, institutions, health care professionals and providers, from the largest multi-state integrated delivery networks to solo practice professionals.

Most small practices conduct at least some of their business electronically. Many submit claims electronically, either directly from their offices or through a billing service. Others receive electronic payment and remittance information from health plans.

Effective October 16, 2003, many common electronic transactions must use uniform national standards. These standards have been promulgated as part of the Administrative Simplification provisions in HIPAA, passed by Congress in 1996.

If your practice does any of the following *electronically*, either directly or through a billing service or other vendor, then effective October 16, 2003, you must use the HIPAA standards:

- submit claims;
- receive claim payment and remittance information;
- query insurance companies about the status of a claim;
- receive information about the status of a claim;
- query insurance companies about the eligibility of a patient to be covered for services;
- receive information about patient eligibility;
- send referral authorizations; or
- receive referral authorizations.

These standards are very complex and confusing.

*The good news is that you do not have to worry about all the technical details of the standards.*

---

## **Wasn't the compliance date October 16, 2002? Has compliance been delayed by one year to October 16, 2003?**

Yes. The date for compliance with the electronic standards has been delayed a year for those entities that have filed for the one year delay.

---

<sup>8</sup>This transactions audit was developed by the Illinois State Medical Society (ISMS) and ISMIE Mutual Insurance Company for its member and policyholder physicians and is used here with the permission of ISMS and ISMIE Mutual.

### **Why are the standards beneficial for small practices?**

Your practice will be able to fill out a claim for a patient – regardless of the health plan – using the standard format, and then submit the claim electronically to any health plan. Not only must health plans accept the standard transactions (with set formats and data fields), but uniform code sets and identifiers will also be used: the coding for each part of the claim will be the same, regardless of the health plan. In other words, every health plan must accept electronic transactions with the same uniform code sets (e.g., CPT-4 with no local codes or plan-specific codes).

Most small practices won't have to worry about the technical specifications of the transactions and code sets. Most practices will be able to rely heavily on their practice management system vendors or billing services to meet the standards.

### **What does my practice have to do to make sure I'm ready for the new standards?**

Most small practices who send or receive information electronically use a practice management or billing software system or a billing service. Practices depend on their vendors – the companies selling the software and the billing services – to make sure electronic information is sent to health plans in the right format, and that electronic information from the health plans is read and used appropriately.

You should:

- Ask your software vendors if they have or are developing software updates that will allow you to use the standard transactions.
- Ask your billing service if it is updating its systems so to use the standard transactions.

If your software vendor will not make your software “HIPAA compliant” or your billing service is not going to be “HIPAA compliant,” you may need to find a new software vendor or a new billing service.

### **What specific questions should I ask my software vendors and billing services?**

You'll need to attain assurances that your software vendors and billing services can meet the requirements in the standard transactions. And you'll need to get these assurances in writing.

Make sure your practice management software or billing service is able to:

- Send claim forms to the health plans using the standard format. If it cannot, you may not be able to bill electronically and your payments from health plans may be slower – or stop – for some period of time. You must be able to send claims to health plans in the standardized format.
- Collect all information needed to complete the standard claim form. This may not be identical to the information you currently collect.
- Handle payments electronically. Chances are you will want to be paid electronically or at least get an electronic “remittance advice” – an electronic explanation of benefits. Make sure you can receive, process, and automatically post information. Automating the posting of payment information will increase accuracy and enable more efficient patient billing. It also will ease the administrative burden in your practice.
- Query health plans about the status of a claim. If you want to have the ability to track claims with health plans, you'll need to ensure you can send a standardized query, using information previously entered when the claim was submitted: You don't want to re-enter duplicate information. You also should make sure you can send a single query anytime or a number of queries at one time.
- Receive electronic query responses. You'll need to ensure that you can process claim status query responses, and post the relevant information to your accounts.

*NOTE: Some health plans cannot provide claims status information to you. You may wish to check with the major health plans with whom you conduct business to see if this is an option. If not, encourage the plans to implement an electronic claims status process.*

- Check patient eligibility electronically. Practice personnel often spend a great deal of time on the phone trying to verify eligibility. Being able to automate this process may save your practice time and reduce your administrative hassle. You'll need to make sure that you are ready to submit eligibility inquiries using the standard format.
- Process an electronic eligibility response. Some plans can provide detailed information about the specific benefits for which a patient is eligible, while other plans may simply indicate that the patient is in fact insured.

*NOTE: Some health plans cannot provide electronic eligibility information to you. You may wish to check with the major health plans with whom you conduct business to see if this is an option. If not, encourage the plans to implement electronic eligibility verification.*

- Electronically send and receive referral authorizations. Practice personnel often spend a lot of time seeking approval for referrals and to verify referral authorizations. This can be done electronically. If you want to reduce the time your staff is spending on the phone handling referrals, make sure you send referral requests and receive responses. You'll also need to automatically update the patient information when a request is approved or denied.

*NOTE: Some health plans cannot provide electronic referral authorizations. You may wish to check with the major health plans with whom you conduct business to see if this is an option. If not, encourage the plans to implement electronic referral authorizations.*

#### **What other key concerns do I need my software vendor or billing service to address?**

- If you have a practice management system in your office, ask your software vendor for a "HIPAA-compliant" version. Keep in mind that October 16<sup>th</sup> is too late. You'll need the software in time to make sure it works. Your vendor should certify that it has tested the software and that it meets the HIPAA requirements. Ask your vendor how and where you can test your updated system to ensure it is "HIPAA compliant."
- If you are using a billing service, ask its representatives to confirm on what date the service will be HIPAA compliant. You also need to ask it to certify that it has tested its systems to ensure that they meet all the requirements in the new HIPAA standards.

#### **What other key concerns do I need my software vendor or billing service to address?**

- If you have a practice management system in your office, you need to ask your software vendor when they can get you a "HIPAA-complaint" version. Keep in mind that October 16<sup>th</sup> is too late. You need the software in time to make sure it works. You need your vendor to certify that it has tested the software and that it meets the requirements. You also should ask your vendor how and where you can test your updated system to ensure it is "HIPAA compliant."
- If you are using a billing service, you need to ask them when it will be HIPAA complaint. You also need to ask it to certify that it has tested its systems to ensure that they meet all the requirements in the new HIPAA standards.

**What if my software vendor or billing service cannot certify to me in writing that they will be HIPAA compliant in time?**

Make sure your vendor or service is aware of HIPAA and the need to come into compliance. If it will not be ready, you have a couple of options:

- If your software vendor will not be ready:
  - You may need to find a new software vendor. This may be a large and expensive undertaking that you want to avoid.
  - OR
  - You may be able to find a billing service that will take the information from your practice management system and put that information into a standard transaction.
- If your billing service will not be ready, you may need to find a new billing service.

**I have about a year to come into compliance. Why do I need to be concerned so far ahead of time?**

Most practices update their computer systems only occasionally. You'll need to start planning now to update your systems, so you can meet the HIPAA standards. In addition, it would be prudent to have the standard transactions in place at least 6 months before the deadline so you can test them to assure they meet the standards and are accepted by your third party payors. Finally, if your software vendor or billing service cannot meet the HIPAA standards, you will need time to find a new vendor or service.

**SOFTWARE OR BILLING SERVICE CHECK LIST:**


- " Send standard claim form
- " Need additional information to send standard claim form
- " Receive, process, and automatically post standard electronic remittance and payment advice
- " Send a standardized claim inquiry, using information previously entered
- " Process claim status query responses
- " Automatically update billing information based on claim status query responses
- " Ready to submit eligibility inquiries using standard format
- " Process eligibility responses from the health plan
- " Automatically update patient insurance information based on eligibility response
- " Send referral requests and receive responses to requests
- " Automatically update billing information based on referral request responses
- " Ready with all transactions tested far in advance of October 16, 2003 deadline

For further information or to comment on this guidance, please contact \_\_\_\_\_.

# Appendix III: Acknowledgement of Receipt of Notice of Privacy Practices

---

## Background

 **Critical:** *Each practice must get a signed acknowledgement that each direct treatment patient has received its Notice of Privacy Practices or must document a good faith effort to provide the Notice and receive a written acknowledgment of receipt. This will allow the practice to use or disclose<sup>9</sup> confidential information<sup>10</sup> for treatment,<sup>11</sup> payment,<sup>12</sup> or health care operations.<sup>13,14</sup>*

---

<sup>9</sup>“Use” refers to the use of information inside a covered entity. “Disclosure” refers to the release of information outside a covered entity.

<sup>10</sup>The rule does not actually address the release of “confidential information.” Rather, it refers to the release of “protected health information (PHI)” contained in “designated record sets.” For our purposes, referring to “confidential information,” while imprecise, will be more meaningful and understandable to small provider practices.

<sup>11</sup>“Treatment” means the provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another.


<sup>12</sup>“Payment” is broadly defined and includes the activities undertaken by a physician to obtain or provide reimbursement for the provision of health care. This includes: (1) determinations of eligibility or coverage (including coordination of benefits or the determination of cost sharing amounts), and adjudication or subrogation of health benefit claims; (2) billing, claims management, collection activities, obtaining payment under a contract for reinsurance (including stop-loss insurance and excess of loss insurance), and related health care data processing; (3) review of health care services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges; and (4) utilization review activities, including precertification and preauthorization of services, concurrent and retrospective review of services.

<sup>13</sup>“Health care operations” refers a large number of activities, including (1) conducting quality assessment and improvement activities; (2) reviewing the competence or qualifications of health care professionals; (3) underwriting, premium rating, and other activities relating to the creation, renewal or replacement of a contract of health insurance or health benefits, conducting or arranging for medical review; (4) legal services, and auditing functions, including fraud and abuse detection and compliance programs; (5) business planning and development; (6) business management and general administrative activities including management activities, customer service, and resolution of internal grievances.

<sup>14</sup>Generally the requirements for consent forms are found at § 164.506 Consent for uses or disclosures to carry out treatment, payment, or health care operations.

---

# Specifications


 **Policy/Procedure:** There are no specific requirements for the acknowledgement form. It can be very simple and straightforward. It should be clear that the patient is acknowledging receipt of the Notice and be written in plain language.



Keep in mind that provision of the Notice does not permit another provider to use or disclose confidential information in most instances. The exceptions to this requirement are discussed in the next section.

---

## Exception to Requirement to Provide Notice

 **Critical:** There are two exceptions to the requirement to provide Notice:

- First, no Notice is required if a provider has an “indirect treatment relationship” with the individual, i.e., the health care provider delivers health care to the individual based on the orders of another health care provider or the health care provider typically provides services or products, or reports the diagnosis or results associated with the health care, directly to another health care provider, who provides the services or products or reports to the individual.
- Second, no Notice is required in emergency treatment situations, if the practice attempts to provide the Notice as soon as reasonably practicable after the delivery of such treatment.

# Appendix IV: Authorization Forms

---

## Background



A practice must get a signed “authorization” to use or disclose information beyond treatment, payment, and health care operations.<sup>15</sup> [Use and disclosure for treatment, payment, and health care operations is allowed as described under your Notice of Privacy Practices as discussed above.] ***While there is no requirement in HIPAA for providers to develop authorizations, providers may want to do so in some instances as a service to patients. In addition, some state laws may require an explicit authorization, e.g., prior to testing a patient from HIV.***

For example, a parent may ask a physician to send certain confidential information about their child to a camp or school. The physician has two options. First, the physician can provide the information directly to the parent and allow them to release it to the camp or school. Second, the physician can use an authorization form to allow them to send the information directly to the camp or school. Keep in mind that this later approach may be burdensome on practices. ***Each authorization has to be specific to the release under consideration.*** The specific requirements for authorizations are outlined below.

In addition, practices may have to develop authorizations in some circumstances if they are required by state law to release information for other than treatment, patient, and health care operations or to gain a specific patient release, e.g., for HIV testing.



***Keep in mind that confidential information may be released for payment and health care operations only to health plans and their agents, and business associates of the practice. The definition of health plans does not include life insurance companies, automobile insurance companies, or workers' compensation carriers. These are not covered under HIPAA, and if a patient wants information submitted to one of these companies, an authorization will be required, unless otherwise required by state or federal law.***

---

## Specifications: General

**🔑 Policy/Procedure:** An authorization must be written in “plain language” and must contain:

- a ***description of the information*** to be used or disclosed;
- the name or other specific identification of the person(s), or class of persons, authorized to make the requested use or disclosure;
- the name or other specific identification of the person(s), or class of persons, to whom the practice may make the requested use or disclosure;
- an ***expiration date or an expiration event*** that relates to the individual or the purpose of the use or disclosure;
- a statement of the individual’s ***right to revoke*** the authorization in writing and the exceptions to the right to revoke, together with a description of how the individual may revoke the authorization;
- a statement that information used or disclosed pursuant to the authorization may be subject to redisclosure by the recipient and no longer be protected by this rule;


---


<sup>15</sup>Generally authorizations are discussed at §164.508: Uses and disclosures for which an authorization is required.


- *signature of the individual and date;*
- if the authorization is signed by a personal representative of the individual, a description of such representative's authority to act for the individual; and
- a description of each purpose of the requested use and disclosure.

 **Critical:** A provider *may not condition the provision to an individual of treatment* on the provision of an authorization, *except:*

- for a research-related treatment; or
- if the purpose of creating the confidential information is for disclosure to a third party, e.g., a life insurance examination.

 **Policy/Procedure:** An individual *may revoke* an authorization at any time, except to the extent that the practice has taken action in reliance of the authorization. Such revocation must be in writing.

 **Policy/Procedure:** A practice must document and retain any signed authorization.

 **Policy/Procedure:** A practice must provide the individual with a copy of the signed authorization.

---

## Special Situation: Psychotherapy Notes



*Psychotherapy notes are handled separately under HIPAA and have additional protections.* Specifically, the regulations state that in most instances a practice must obtain an authorization for any use or disclosure of psychotherapy notes.

No authorization is needed to carry out treatment, payment, or health care operations, given that you have provided the patient with your Notice of Privacy Practices:

- use by the originator of the psychotherapy notes for treatment;
- use or disclosure by the health care provider in training programs in which “students, trainees, or practitioners in mental health” learn under supervision to practice or improve their skills in group, joint, family, or individual counseling; or
- use or disclosure by the practice to defend a legal action or other proceeding brought by the individual.


In addition, an *authorization is not needed* for a use or disclosure:

- that is required by the Secretary to investigate or determine the practice's compliance with the privacy regulations;
- to the extent that such use or disclosure is required by law, and the use or disclosure complies with and is limited to the relevant requirements of such law;
- for health oversight activities;
- for certain disclosures about decedents; and
- to avert a serious threat to health or safety.


All other circumstances require a valid authorization for use and disclosure.

---

## Specifications: Authorizations Requested by Practice for its Own Uses and Disclosures

 **Policy/Procedure:** In those instances where the practice may condition the provision of treatment upon receiving an authorization (see above), the authorization must, in addition to meeting the requirements outlined above, contain the following elements:

- a description of each purpose of the requested use or disclosure;
- a statement that the individual may:
  - inspect or copy the confidential information to be used or disclosed; and
  - refuse to sign the authorization; and
- if use or disclosure of the requested information will result in direct or indirect remuneration to the practice from a third party, a statement that such remuneration will result.

 **Critical:** Recall that there is no requirement for a practice to obtain an authorization if it is only using and disclosing confidential information for treatment, payment, and health care operations.


---


## HIPAA Authorization Form Checklist

Based on the above information, an authorization form must be in “plain language” and include:


- A description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion.
- A description of each purpose of the requested use and disclosure.
- The name or other specific identification of the person(s), or class of persons, authorized to make the requested use or disclosure.
- The name or other specific identification of the person(s), or class of persons, to whom the practice may make the requested use or disclosure.
- An expiration date or an expiration event that relates to the individual or the purpose of the use or disclosure.
- A statement of the individual’s right to revoke the authorization in writing and the exceptions to the right to revoke, together with a description of how the individual may revoke the authorization.
- A statement that information used or disclosed pursuant to the authorization may be subject to re-disclosure by the recipient and no longer be protected by this rule.
- Signature of the individual and date.
- If the authorization is signed by a personal representative of the individual, a description of the representative’s authority to act for the individual.
- Any special provisions included in state law.


# Appendix V: Disclosure Without Written Authorization


 **Critical:** A practice may use or disclose confidential information *without the written consent or authorization of the individual* in certain situations.<sup>16</sup> Keep in mind that state laws must be carefully evaluated.

 **Policy/Procedure:** A practice may use or disclose confidential information to the extent that such use or disclosure is *required by law* and the use or disclosure complies with and is limited to the relevant requirements of such law, e.g., the reporting of communicable diseases to the local public health department. The rule specifically addresses:

- uses and disclosures for public health activities;
- reporting about victims of abuse, neglect or domestic violence;
- disclosures for health oversight activities;
- disclosures for judicial and administrative proceedings;
- disclosures for law enforcement purposes;
- uses and disclosures about decedents;
- uses and disclosures for cadaveric organ, eye or tissue donation purposes;
- disclosures to avert a serious threat to health or safety; and
- uses and disclosures for specialized government functions.

 **Policy/Procedure:** In addition, a practice *may disclose to a family member*, other relative, or a close personal friend of the individual, or any other person identified by the individual, the confidential information directly relevant to such person's involvement with the individual's care or payment related to the individual's health care, unless that patient has requested that such disclosure not occur and the provider has agreed.

 **Policy/Procedure:** In addition, if the individual is not present for, or the opportunity to agree or object to the use or disclosure cannot practicably be provided because of the individual's incapacity or an emergency circumstance, the practice may, in the exercise of professional judgment, determine whether the disclosure is in the best interests of the individual and, if so, disclose only the confidential information that is directly relevant to the person's involvement with the individual's health care.

 **Keep in mind that practices need to keep track of certain disclosures which require an authorization or which can be released without an authorization. It is not necessary to provide an accounting of disclosures made as a result of an authorization. This is addressed further in Appendix VI: Policy Manual.**

---

<sup>16</sup>Generally these are discussed at § 164.512 Uses and disclosures for which consent, an authorization, or opportunity to agree or object is not required.

# Appendix VI: Notice of Privacy Practices

---

## Background



Each small practice must make available to each patient or prospective patient a “Notice of Privacy Practices.” The Notice must inform the individual of the uses and disclosures of confidential information that may be made by the practice, and of the individual’s rights and the practice’s legal duties with respect to confidential information.<sup>17</sup> For direct care patients the provider must document that the Notice was provided or that a good faith effort was made to provide the notice to the patient.

This section outlines the specifications of the Notice of Privacy Practices. This includes the required elements of the Notice, provision of the Notice, joint Notice by related organizations, and documentation requirements. *The Notice will be a long and detailed document and must address state law.*

---

## Required Elements

**⚡ Policy/Procedure:** Each practice must provide the Notice of Privacy Practices written in *plain language*.

**⚡ Policy/Procedure:** The *Notice* must contain the following elements:

- **Header:** The *Notice* must contain the following statement as a header or otherwise prominently displayed: “THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.”
- **Uses and disclosures:** The *Notice* must contain the following information:
  - a description, including at least one example, of the types of uses and disclosures that the practice is permitted to make for each of the following: treatment, payment, and health care operations;
  - a description of each of the other purposes for which the practice is permitted or required to use or disclose confidential information without the individual’s authorization (see above page 26) – the description must include sufficient detail to place the individual on notice of the uses and disclosures that are permitted or required;
  - if a use or disclosure for any purpose described in the two points above is prohibited or materially limited by other applicable law, the description of such use or disclosure must reflect the more “stringent law”<sup>18</sup> – the description must include sufficient detail to place the individual on notice of the uses and disclosures that are permitted or required; and
  - a statement that other uses and disclosures will be made only with the individual's written authorization and that the individual may revoke such authorization as described as above.

---

<sup>17</sup>The discussion on notices of privacy practices is found at § 164.520 Notice of Privacy Practices for protected health information.

<sup>18</sup>The issue of preemption is very complex and is discussed in the Preemption section of the WEDI/SNIP Security and Privacy White Paper. A different preemption analysis must be completed for each state, and small practices will not have the resources to complete such an analysis. As discussed in the White Paper, many associations and state governments are expected to complete preemption analyses that will then become available to small practices.

- **Separate statements for certain uses or disclosures:** If the practice intends to engage in any of the following activities, the Notice of Privacy Practices must include a separate statement, as applicable, that:
  - the practice may contact the individual to provide appointment reminders or information about treatment alternatives or other health-related benefits and services that may be of interest to the individual; or
  - the practice may contact the individual to raise funds for the practice (this provision is unlikely in most small practices, but applies in many larger organizations, e.g., hospitals).

- **Individual rights:** The *Notice* must contain a statement of the individual’s rights with respect to confidential information and a brief description of how the individual may exercise these rights, as follows:

- ***The right of the individual to request restrictions on certain uses and disclosures.***

Section 164.522(a) provides the right of an individual to request restriction of uses and disclosures. A practice must *permit an individual* to request that the practice *restrict* uses or disclosures of confidential information about the individual to carry out treatment, payment, or health care operations and to family members. A practice is ***not required to agree to a restriction*** and may decide not to accept the restrictions and not to treat the individual.

- ***The right to receive confidential communications.***

Section 164.522(b) requires a practice to permit individuals to request and accommodate ***reasonable requests*** by individuals to receive communications of confidential information from the health care provider by alternative means or at alternative locations. A practice may require the individual to make the request ***in writing; may condition the provision of a reasonable accommodation*** on, when appropriate, information as to how payment, if any, will be handled and specification of an alternative address or other method of contact; and ***may not require an explanation*** from the individual as to the basis for the request.

- ***The right to inspect and copy confidential information.***

Section 164.524 provides a right for individuals to access and inspect their confidential health information, ***except for psychotherapy notes***; information compiled in reasonable anticipation of ***legal action or proceeding***; and confidential information related to certain laboratory tests under ***CLIA***. In addition, a practice ***may deny an individual access***, provided that the individual is given a right to have such denials reviewed, in the following circumstances:

- a health care provider has determined, in the exercise of professional judgment, that the access requested is reasonably likely to ***endanger the life or physical safety of the individual or another person***;
- the information makes ***reference to another person*** (unless such other person is a health care provider) and the health care provider has determined, in the exercise of professional judgment, that the access requested is reasonably likely to cause substantial harm to such other person; or
- the request for access is made by the individual’s personal representative and the health care provider has determined, in the exercise of professional judgment, that the provision of access to such personal representative is reasonably likely to ***cause substantial harm to the individual or another person***.

The process for accessing confidential information must be detailed in the practice’s policy manual (see below page 32).

- ***The right to amend confidential information.***

Section 164.526 provides a right for individuals to amend confidential information held by a practice. A practice ***may deny an individual’s request*** for amendment, if it determines that the information that

is the subject of the request was not created by the covered entity; is not part of the confidential record; would not be available for inspection under § 164.524 (see “right to inspect and copy confidential information” above; or *is accurate and complete*.

The process for amending confidential information must be detailed in the practice’s policy manual (see below page 32).


- ***The right to receive an accounting of disclosures of confidential information.***

Section 164.528 provides a right for individuals to receive an accounting of disclosures of confidential information. Disclosure information must be made available for a 6 year period – beginning with the date the practice comes into compliance with this rule (no later than April 14, 2003). A record of disclosures ***does not have to be made when those disclosures are:***


- to carry out treatment, payment and health care operations;
- to individuals of confidential information about them;
- as a result of a signed authorization;
- for the practice’s directory or to persons involved in the individual’s care;
- for national security or intelligence purposes; or
- to correctional institutions or law enforcement officials.

The process for providing an accounting must be detailed in the practice’s policy manual (see below page 32).

- ***The right of an individual, including an individual who has agreed to receive the Notice electronically, to obtain a paper copy of the Notice from the covered entity upon request.***
- **Practice’s duties:** The Notice of Privacy Practices must contain:
  - a statement that the practice is required by law to maintain the privacy of confidential information and provide individuals with notice of its legal duties and privacy practices with respect to such information;
  - a statement that the practice is required to abide by the terms of the ***Notice*** currently in effect; and
  - for the practice to apply a change in a privacy practice that is described in the ***Notice***, a statement that it reserves the right to change the terms of its ***Notice*** and to make the new ***Notice*** provisions effective for all confidential information that it maintains. The statement must also describe how it will provide individuals with a revised ***Notice***.

 **Critical:** A practice needs to highlight this final point about reserving the right to change policies ***or it will not be allowed to retroactively apply any changes to its privacy policies.***

- **Complaints:** The Notice of Privacy Practices must contain a statement that individuals may complain to the practice and to the Secretary of the U.S. Department of Health and Human Services if they believe their privacy rights have been violated, a brief description of how the individual may file a complaint, and a statement that the individual will not be retaliated against for filing a complaint.
- **Contact:** The Notice of Privacy Practices must contain the name, or title, and telephone number of a person or office to contact for further information. The appropriate contact person is the practice’s designated privacy official.
- **Effective Date:** The Notice of Privacy Practices must contain the date on which the ***Notice*** is first in effect, which may not be earlier than the date on which the ***Notice*** is printed or otherwise published.

 **Policy/Procedure:** In addition to these required elements, the Notice of Privacy Practices may include a number of optional elements. Specifically, if a practice elects to limit the uses or disclosures that it is permitted to make, the practice may describe its more limited uses or disclosures in its Notice.

**Key Policy/Procedure:** The practice must promptly revise and distribute its Notice whenever there is a material change to the uses or disclosures, the individual’s rights, the covered entity’s legal duties, or other privacy practices stated in the Notice. Except when required by law, a material change to any term of the Notice may not be implemented prior to the effective date of the Notice in which such material change is reflected.

---

## Provision of Notice

**Key Policy/Procedure:** A practice must make the Notice of Privacy Practices available on request to any person and to individuals as follows:

- A health care provider that has a *direct treatment relationship*<sup>19</sup> with an individual must:
  - provide the Notice *no later than the date of the first service delivery*, including service delivered electronically, to the individual;
  - have the Notice available at the practice site for individuals to request to take with them and must *post the Notice* in a clear and prominent location where it is reasonable to expect individuals seeking service to be able to read the *Notice*; and
  - whenever the *Notice is revised*, make the *Notice* available upon request on or after the effective date of the revision.
- A practice that maintains a web site that provides information about the practice’s services or benefits must prominently post its *Notice* on the web site and make the *Notice* available electronically through the web site.
- A practice may provide the *Notice* to an individual by e-mail, if the individual agrees to electronic *Notice* and such agreement has not been withdrawn. If the practice knows that the e-mail transmission has failed, a paper copy of the *Notice* must be provided to the individual.

---

## Other Provisions

**Key Policy/Procedure:** The practice must incorporate into its Notice any special provisions of state law that relate to the privacy of confidential information. The specific provisions will be determined as a result of a state-specific preemption analysis.

**Key Policy/Procedure:** The small practice may participate in an organized health care arrangement or may provide services in the context of another facility, e.g., a hospital. In these instances, a joint Notice – covering all the involved parties – is allowed, provided that:

- the health care provider and the other parties in the organized health care arrangement agree to abide by the terms of the Notice for confidential information created or received as part of participation in the organized health care arrangement;
- in addition to the requirements outlined above, the joint Notice:
  - describes with reasonable specificity the entities covered by the Notice;
  - describes with reasonable specificity the service delivery sites to which the joint Notice applies; and

---

<sup>19</sup>A “direct treatment relationship” means a treatment relationship between an individual and a health care provider where the health care provider *does not* deliver health care to the individual based on the orders of another health care provider and *does not* typically provide services or products, or report the diagnosis or results associated with the health care, directly to another health care provider, who provides the services or products or reports to the individual.

- if applicable, states that the entities will share information as necessary to carry out treatment, payment, or health care operations;
- the entities included in the joint Notice provide the Notice to individuals as discussed above. Provision of the joint Notice to an individual by any one of the entities included in the joint Notice will satisfy the provision requirement with respect to all others covered by the joint Notice.

**Key Policy/Procedure:** A practice must document compliance with the Notice requirements by retaining copies of the Notices issued by the practice.

---

## HIPAA Notice of Privacy Practices Checklist

Based on the above information, a Notice of Privacy Practices must: be in “plain language “ and include:

- The required header statement.
- Information on uses and disclosures, including those needing authorization forms, taken account of state laws.
- Separate statements for uses and disclosures related to items such as the provision of appointment reminders and other information, and fund raising.
- A description of the individual patient rights:
  - The right of the individual to request restrictions on certain uses and disclosures.
  - The right to receive or request confidential communications.
  - The right to inspect and copy confidential information, including when a practitioner can deny such a request and the process for contesting any denial of access.
  - The right to amend confidential information, including when a practitioner can deny such an amendment and the process for contesting any such denial.
  - The right to receive an accounting of disclosures of confidential information.
  - The right of an individual, including an individual who has agreed to receive the Notice electronically, to obtain a paper copy of the Notice from the covered entity upon request.
- A statement of the practice’s duties, including the duty to ensure the privacy of confidential information and to inform the patient of any changes in the Notice.
- A statement that individuals may complain to the practice and to the Secretary of DHHS.
- The appropriate contact person in the practice.
- The effective date of the Notice.
- Any optional items.
- Process to obtain written acknowledgment of receipt of Notice.

# Appendix VII: Policy Manual

---

## Background



Each practice is required to implement policies and procedures with respect to confidential information that are designed to comply with the HIPAA regulations. The policies and procedures must be reasonably designed, taking into account the size of and the type of activities that relate to the confidential information of the practice, to ensure compliance.<sup>20</sup> ***Each practice will need to develop a policy manual to demonstrate compliance with this requirement.*** [For a more detailed list of policies and procedures, please refer to the Policies and Procedures White Paper of the WEDI/SNIP Security and Privacy Workgroup at [snip.wedi.org](http://snip.wedi.org).]

Specifically, Section 164.530(j)(1) requires each practice to:

- maintain the ***policies and procedures*** provided for in ... this section ***in written or electronic form***;
- if a communication is required ... to be in writing, ***maintain such writing, or an electronic copy***, as documentation; and
- if an action, activity, or designation is required ... to be documented, ***maintain a written or electronic record of such action***, activity, or designation.



**Critical:** In addition, Section 164.530(a)(1) requires each practice to “***designate a privacy official*** who is responsible for the development and implementation of the policies and procedures of the entity.” Each practice must “designate a contact person or office who is responsible for receiving complaints ... and who is able to provide further information about matters covered by the Notice [of privacy practices].” For most small practices, the “privacy official” will be one of the health care providers or another staff member. This person will be directly responsible for ensuring implementation of the HIPAA privacy and security provisions.

The following sections provide an outline of the policies that must be documented by the practice. These requirements arise directly out of the privacy rule. In some instances, the discussion relates to items that will be included in the Notice of Privacy Practices and are mentioned above. Where possible, these items are cross-referenced and not repeated.

---

## Notice of Privacy Practices for Confidential Information



***The Notice of Privacy Practices is discussed in detail above (see page 27). The policy manual must include a reference to the Notice and must be consistent with the Notice.***

---

## Uses and Disclosures of Confidential Information



Uses and disclosures of confidential information are addressed in several sections of the regulations. ***The policy manual must reflect and be specific and consistent with the Notice of Privacy Practices and any Authorization Forms.***

---

<sup>20</sup>See § 164.530(i) Administrative requirements.

## Provision of Notice of Privacy Practices for uses or disclosures to carry out treatment, payment, or health care operations

Each practice must provide each direct treatment patient with its Notice of Privacy Practices and document that the patient received the Notice.

**Policy/Procedure:** The policy manual must specify procedures for documenting that the Notice was received by the patient.

## Uses and disclosures for which an authorization is required

*While there is no requirement for practices to develop authorizations, practices may want to do so in some instances as a service to patients.* If a practice decides to use authorization forms, it must have Authorization Forms that meet the specifications in the rules (see page 23).

**Policy/Procedure:** The policy manual must specify:

- that the practice does not condition treatment on the provision by the individual of authorization;
- procedures for an individual to revoke in writing an authorization at any time;
- procedures for documenting and retaining the authorization; and
- special considerations related to psychotherapy notes, if appropriate to the practice.

## Exceptions to the requirement to obtain authorization

The rule permits disclosure of confidential information without an authorization (see page 26).

**Policy/Procedure:** The policy manual must clearly outline the circumstances and procedures for such releases. This includes:

- disclosures required by law;
- disclosures to family members; and
- when the individual cannot practicably be provided the opportunity to agree or object.

## Other requirements relating to uses and disclosures of confidential information

There are a number of other requirements related to uses and disclosures of confidential information. These are specified in section 164.514 and include:

- the “de-identification” of confidential information;
- the “minimum necessary” provisions;
- marketing restrictions; and
- fund raising restrictions.

Each of these are discussed below.

### “De-identification” of Confidential Information



The area of “de-identification” of confidential information is complex. *Generally, there is no requirement for a practice to de-identify confidential information. Accordingly, a practice can choose to implement a policy simply stating that it does not de-identify data.*

If a practice decides to develop a policy on the de-identification of information, it must follow the requirements in the rule. According to the rule, information is not individually identifiable if:

- the individual is not identified; or
- if the covered entity has no actual knowledge that can be used to identify the individual.

The rule states that there are two ways in which a practice can demonstrate that it has met this standard:

**1. A person with appropriate knowledge and expertise:**

- applies generally accepted statistical and scientific principles and methods for rendering information not individually identifiable;
- makes a determination the risk is very small that the information could be used by itself or in combination with other available information by the anticipated recipients; and
- documents the analysis and results in making such determination.

**2. Safe Harbor method:**

- remove all of a list of identifiers enumerated in the rule<sup>21</sup>; and
- no actual knowledge that the information that the information can be used alone or in combination to identify a subject of the information.

**🔑 Policy/Procedure:** A practice needs to document all of the initiatives taken to comply with the de-identification standards. These initiatives should include process and procedure development, training programs, implementation and compliance monitoring.



**Critical:** The regulations also allow practices to have information de-identified by a business associate.

---

<sup>21</sup>The following information *must be removed* (including those of the individual, relatives, employers or household members of the individual):

- names;
- all geographic subdivisions smaller than a State, including street address, city, county, precinct, zip codes if the geographic unit of combining all the same three initial digits contains more than 20,000 people;
- if zip contains < 20,000 then changed to 00;
- all elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;
- telephone numbers;
- fax numbers;
- electronic mail addresses;
- social security numbers;
- medical record numbers;
- health plan beneficiary numbers;
- account numbers;
- certificate/license numbers;
- vehicle identifiers and serial numbers, including license plate numbers;
- device identifiers and serial numbers;
- web Universal Resource Locators (URLs);
- internet Protocol (IP) address numbers;
- biometric identifiers, including finger and voice prints;
- full face photographic images and any comparable images; and
- any other unique identifying number, characteristic, or code.

## Limited Data Sets



The area of “limited data sets” is complex. *Generally, there is no requirement for a practice to provide a limited data set. Accordingly, a practice can choose to implement a policy simply stating that it does not provide limited data sets.*

If a practice decides to develop a policy on the provision of limited data sets, it must follow the requirements in the rule. A limited data set must exclude a significant amount of confidential information.<sup>22</sup> A practice may use or disclose a limited data set only for the purposes of research, public health, or health care operations. The practice must enter into a “data use agreement” with the limited data set recipient. The rule requires that such an agreement establish the permitted uses and disclosures of the limited data set by the recipient, who is permitted to use or receive the limited data set, and that the limited data set will remain confidential.

### “Minimum Necessary” Provisions

The final rule requires a practice to make reasonable efforts not to use or disclose more than the “minimum amount of confidential information necessary” to accomplish the intended purpose of the use, disclosure, or request taking into consideration practical and technological limitations.



*When using or disclosing confidential information or when requesting confidential information from another entity, a practice must make reasonable efforts to limit the confidential information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.*<sup>23</sup>



**Critical:** This requirement does not apply to:

- disclosures to or requests by *a health care provider for treatment – health care cannot stop while decisions are made*;
- uses or disclosures made to the *individual*;
- uses or disclosures pursuant to an *authorization*;
- disclosures made to the *Secretary*;
- uses or disclosures that are *required by law*; and
- uses or disclosures that are required for *compliance* with this rule.

**Policy/Procedure:** The rule requires that each practice identify:

---

<sup>22</sup>A limited data set must exclude the following direct identifiers of the individual or of relatives, employers, or household members of the individual:

- (i) Names;
- (ii) Postal address information, other than town or city, State, and zip code;
- (iii) Telephone numbers;
- (iv) Fax numbers;
- (v) Electronic mail addresses;
- (vi) Social security numbers;
- (vii) Medical record numbers;
- (viii) Health plan beneficiary numbers;
- (ix) Account numbers;
- (x) Certificate/license numbers;
- (xi) Vehicle identifiers and serial numbers, including license plate numbers;
- (xii) Device identifiers and serial numbers;
- (xiii) Web Universal Resource Locators (URLs);
- (xiv) Internet Protocol (IP) address numbers;
- (xv) Biometric identifiers, including finger and voice prints; and
- (xvi) Full face photographic images and any comparable images.

<sup>23</sup>Recall that “use” refers to the use of information inside a covered entity that maintains such information. “Disclosure” refers to the release of information outside the covered entity holding the information. “Request” refers to information requested by one covered entity of another covered entity.

- those *persons or classes of persons*, as appropriate, in its workforce *who need access* to confidential information to carry out their duties; and
- for each such person or class of persons, the category or categories of confidential *information to which access is needed* and any conditions appropriate to such access.

**🔑 Policy/Procedure:** Each practice is required

- to implement *policies and procedures that limit the routine use, disclosure, or request of confidential information to the amount reasonably necessary* to achieve the purpose of the use, disclosure, or request and to limit access to confidential information only to those people who need access to the information to accomplish the use, disclosure, or release. For all non-routine use, disclosure, or requests for protected health information, each practice must develop criteria to be used to complete a case-by-case review for each use, disclosure, or request.

**💣 Critical:** *For practical purposes, in small practices nearly every provider and staff member will need access to all of a patient’s confidential information. Nevertheless, it may be possible to define general job categories such as receptionist, billing clerk, and clinical assistant and then further assign access control limitations.* Keep in mind that this refers to the “use” of information by the practice, not to “disclosure” of information to other entities. Disclosure must still be limited.

**💣 Critical:** Where it is unclear what particular information needs to be used, disclosed, or requested, the minimum necessary requirements may be interpreted to require the covered entity to make some effort to limit the amount of information used, disclosed, or requested. Standard requests can have standard responses. The use of a standard set of data to respond to a standard request may be reasonable, but must be balanced with the ability of the practice to provide more focused information.

**💣 Critical:** Covered entities must make “reasonable” expenditures to implement technologically feasible approaches to ensure compliance with the minimum necessary requirements. The final rule does not indicate what is a “reasonable” expenditure to ensure compliance with these requirements; however, the rules do indicate that compliance is “scalable” so that a small practice will only have to do what is reasonable under the circumstances.

## Marketing Restrictions

The rule states that a practice is *not required* to obtain an authorization when it uses or discloses confidential information to make a marketing communication to an individual that:

- occurs in a face-to-face encounter with the individual;
- concerns products or services of nominal value; or
- concerns the health-related products and services of the practice or of a third party and the communication meets the applicable conditions specified in the rule.

A business associate may undertake allowed marketing communications on behalf of a practice.

The final Privacy modification clarifies the definition of marketing. Of particular relevance to small providers is the following: The definition of marketing “excludes a communication made to an individual ... (2) For treatment of that individual; or (3) For case management or care coordination for that individual, or to direct or recommend alternative treatments, therapies, health care providers, or settings of care to that individual.” In general, this means that most providers can continue to provide the kinds of information and products to patients that are related to the ongoing treatment of the patient.

**💣 Critical:** The rule requires each practice to specify in its Notice of Privacy Practices if and under what conditions it will engage in marketing to patients.

**🔑 Policy/Procedure:** If a practice engages in marketing, it must have policies and procedures that meet the following conditions:

- the communication must:
  - identify the practice as the party making the communication;
  - if the practice has received or will receive direct or indirect remuneration for making the communication, prominently state that fact; and
  - except when the communication is contained in a newsletter or similar type of general communication device that the practice distributes to a broad cross-section of patients, contain instructions describing how the individual may opt out of receiving future such communications;
- if the practice uses or discloses confidential information to target the communication to individuals based on their health status or condition:
  - the practice must make a determination prior to making the communication that the product or service being marketed may be beneficial to the health of the type or class of individual targeted; and
  - the communication must explain why the individual has been targeted and how the product or service relates to the health of the individual; and
- the practice must make reasonable efforts to ensure that individuals who decide to opt out of receiving future marketing communications are not sent such communications.

*All other marketing to patients is generally prohibited by the HIPAA regulations unless an authorization is secured.*

## Fund Raising Restrictions



**Critical:** This will not apply to most small practices as they do not normally engage in fund raising activities for their practices.



**Policy/Procedure:** If a practice plans to engage in fund raising:

- the practice is prohibited from using or disclosing confidential information for fund raising purposes unless a statement regarding such fund raising is included in the practice's Notice of Privacy Practices;
- the practice must include in any fund raising materials it sends to an individual a description of how the individual may opt out of receiving any further fundraising communications; and
- the practice must make reasonable efforts to ensure that individuals who decide to opt out of receiving future fundraising communications are not sent such communications.

---

## Access of Individuals to Confidential Information

Sections 164.522 and 164.524 allow individuals the right to access to inspect and obtain a copy of their confidential information, for as long as the practice maintains the information. Practices must have in place policies defining:

- to what confidential information individuals have access;
- who can request the information;
- the procedures for requesting information;
- the time frames for responding to a request;
- when the practice can deny access; and
- how an individual may appeal a decision to deny access.

### Covered Information


Generally a practice must provide an individual access to all of his or her confidential information.




**Policy/Procedure:** Each practice should:


- develop policies and procedures for accepting a request;
- document the title(s) of the persons or offices responsible for receiving and processing requests;

- classify confidential information and determine if information is duplicated in different locations in order to efficiently process requests for access; if the same information is maintained in more than one place or at more than one location, the practice is required to produce the information only once per request for access;
- establish a system to track requests (reports should be defined and the mechanism for analyzing and improving performance developed); and
- assign responsibility for managing requests.

 **Critical:** Often a practice uses a “*business associate*” to process, collect, or maintain certain information. If a practice approves a request of access, it must also provide access to information maintained by its business associate(s), unless the information is the same as information maintained directly by the practice.


 **Policy/Procedure:** Each practice should identify:

- what confidential information is maintained by each of its business associates;
- whether its business associates modify the confidential information; and
- the time each business associate will need to retrieve or make the confidential information available to the practice.


 **Critical:** The obligation for a business associate to provide information when requested by a practice should be included in the business associate contract.

### Who Can Request Information


An individual can directly request their information. In addition, an individual other than the subject of the confidential information may be designated as a “personal representative” and be permitted to access the information. Personal representatives often are specified in state law.


 **Policy/Procedure:** Procedures developed by a practice should include:

- procedures necessary to verify the designation of a personal representative;
- sufficient advance notice of a request to permit the practice to verify the designation with the individual who is the subject of the information (e.g., via phone, email or letter), if necessary; and
- a process to identify known instances where a personal representative should not be granted access (e.g., when the practice is informed of an abusive situation, this information should be communicated to the people handling requests for access).

 **Critical:** A practice has discretion to deny access to a personal representative to provide protection to those vulnerable people who depend on others to exercise their rights under the rule and who may be subject to abuse or neglect. This also applies to personal representatives of minors and again may be further restricted by state law.

### Procedures for Requesting Access


 **Critical:** A practice may require that requests for access be in writing, may provide information in a summary form, and may charge a fee for copying records. However, advance written notice must be provided of these rules to the individuals who may request access. The practice can satisfy this requirement by *providing notice in the Notice of Privacy Practices*. In addition, the individual must be given the opportunity to agree in advance to information being presented in a summary form and fees being charged. Practices may choose to develop a request for access form that informs the individual making the request that the response will use summary data and that fees will be charged.

 **Policy/Procedure:** A practice is permitted to charge a reasonable cost-based fee for copying information. If state law specifies fees for copying and mailing information (e.g., per page costs) that include fees for retrieval or handling of information, practices may **not** include such costs in the “reasonable” fee. Practices may find this

especially burdensome since information may be maintained in multiple applications/systems and/or stored off-site in paper format.

*Information created prior to the effective date of the rule is included in the right of access.*

### Time Frames For Responding


 **Critical:** A practice must act on a request for access to information within thirty (30) days when information is maintained on-site and within sixty (60) days when information is maintained off site. An extension of no more than thirty (30) days is allowed if the practice notifies the individual with a written statement of the reason for the delay and the date by which the covered entity will complete the action on the request.

 **Policy/Procedure:** Each practice should:

- develop template letters for use when an extension is needed; and
- establish a tracking system for monitoring and reporting of timeliness of actions.


An individual may request information in a form or format that a practice finds difficult to produce, especially in the allowed time frames. The practice may enter into discussions with the individual to ensure the information is provided in a reasonable format that is acceptable to both the individual and the practice.

### Denying Access

 **Critical:** The rule allows denial of access:

- if access is reasonably likely to endanger the life or physical safety of the individual or another person;
- psychotherapy notes;
- if the information is compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding;
- to certain information maintained by a covered entity that is subject to or exempted from the Clinical Laboratory Improvements Amendments of 1988 (CLIA);
- to information in a correctional institution or of a provider acting under the direction of a correctional institution may deny an inmate's request to obtain a copy of information under certain circumstances;
- to information obtained by a provider in the course of research that includes treatment of the research participants, while research is in progress;
- to information is also subject to the Privacy Act, 5 U.S.C. 552(a). The Act requires government agencies to provide notice of the routine uses of information the agency collects and the rights of individuals have with respect to that information; and
- if the practice obtained the requested information from someone other than a health care provider under a promise of confidentiality and such access would be reasonably likely to reveal the source of the information.


These permissible denials are just that – “permissible.” A practice *may, but is not required to*, provide access to the excepted information. They are a means of preserving the flexibility and judgment of practices under appropriate circumstances. Furthermore, it is expected that most practices will employ these exceptions rarely if at all.

 **Critical:** Although requests for access to psychological notes may be denied, practices that maintain psychological notes are encouraged to provide individual access to these notes when they believe it is appropriate to do so. Also, state law may allow access to these records that goes beyond the federal rules.

 **Policy/Procedure:** Each practice should:

- develop policies and procedures for denying a request;
- develop specific reasons and examples for denying access in various situations, e.g., where the practice does not maintain the information requested; and
- develop template letters for denying access.

## Appealing a Decision to Deny Access


 **Critical:** Individuals may request a review of a denial of access in the following circumstances:

- a licensed health care professional determines that access is reasonably likely to endanger the life or physical safety of the individual or another person;
- the information references another person (unless the other person is a health care provider) and a licensed health care professional determines that access is reasonably likely to cause substantial harm to such other person; or
- access is requested by a personal representative and a licensed health care professional determines that access is reasonably likely to cause substantial harm to the individual or another person or health.

Review must be performed by a licensed health care professional who did not participate in the original decision to deny access. The rule does not specify a time frame to complete a review when requested.

 **Policy/Procedure:** Each practice should:

- designate the licensed health care professional(s) who will review the request to have a denial of access reviewed;
- determine the appeal response time (the Rule is silent on the appeal response time);
- ensure the access request tracking system includes denial status, review of denial and final outcomes; and
- develop template letters for use in denial and review situations.

 **Critical:** Denial of access may also trigger federal or state defined compliance procedures, especially in managed care products. Practices will need to determine if compliance with the rule's procedure will satisfy other federal and/or state complaint procedures, including external appeal to departments of insurance.


---

## Amendment of Confidential Information

Section 164.526 gives an individual the right to have a practice amend confidential information about the individual for as long as the information is maintained. The written policies must address:


- the process for accepting a request for and making an amendment of confidential information;
- how quickly a practice must respond to a request for an amendment of information;
- how to proceed if the originator of the information is no longer available; and
- the process for denying a request for amendment.

### Accepting a Request for and Making an Amendment of Confidential Information

 **Critical:** A practice is allowed to require the request for amendment be in writing and for the requestor to provide a reason supporting a requested amendment if an individual is notified in advance of such a requirement. This advance notice should be included in the practice's Notice of Privacy Practices.


A practice must:

- accept the individual's request for an amendment; and
- identify all of the information affected by the request, including information provided to other entities and business associates.


 **Critical:** Before accepting or denying a request for amendment, practices should have explicit information regarding the reason for the amendment and what is to be amended. The following are minimal data elements that should be included:

- demographic information;

- reason for the request;
- description of the problem – how the information is incorrect or incomplete;
- description of the:
  - administrative information to be corrected, e.g., enrollment information; and/or
  - medical information to be amended including the source if known, date and provider of service;
- specific wording to make the entry correct/complete;
- identification of who may have received the information; and
- identification of who needs to be advised of the amendment, including contact information.

 **Policy/Procedure:** If a request for amendment is accepted, the practice must:

- notify the requestor that the amendment is accepted; and
- obtain the requestor's approval of the relevant persons with whom the amendment needs to be shared, e.g., other providers or business associates with whom the information previously has been shared.

 **Critical:** A practice must amend information when it agrees to the amendment or when notified by another entity that an amendment has been accepted.


A distinction may be made between demographic information used for enrollment or claims processing purposes (e.g., patient name, address or phone number) that can be *changed* versus medical information that must be *amended*. Demographic or enrollment changes may be made without having to maintain a historical file of the change.



*For risk management purposes it is prudent never to change medical information. It should be amended, and the prior information should be noted as being amended, but not deleted. In addition, some state laws prevent information in medical records from being changed or deleted.*

 **Policy/Procedure:** A practice should:

- develop policies and procedures to amend information when a request is accepted or when notified that an amendment has been accepted by another entity;
- develop policies and procedures to cover all media forms maintained by the practice – paper, microfiche, microfilm, or automated data processing – and should specify how amendments will be normalized across varied systems and applications maintained by the practice that contain confidential information;
- develop policies and procedures for sharing amendments with the relevant persons who received the original information, including business associates;
- consider potential malpractice implications if information is altered in a manner not acceptable to state law or standards of practice;
- document in its privacy policy whether demographic information can be changed as opposed to being amended and include this policy in its Notice of Privacy Practices;
- document the title(s) of the persons or offices responsible for receiving and processing requests;
- develop template letters for notification purposes; and
- establish a system to track, report and analyze amendment requests.

 **Critical:** If confidential information is stored electronically, the covered entity will need to assess the application's ability to store the amendment and the ability to provide audit trails of amended data.

### **Time Frames for Dealing with Requests for Amendments**


A practice must act on a request for amendment to confidential information within sixty (60) days. A one time extension of no more than thirty (30) days is allowed if the practice notifies the individual with a written statement of the reason for the delay and the date by which the practice will complete its action on the request.

 **Policy/Procedure:** A practice should:

- develop letters for use when an extension is needed; and

- develop a tracking system for monitoring and reporting of timeliness of actions.


### What if the Originator of the Information is No Longer Available?

 **Critical:** If the individual provides a reasonable basis to believe that the originator of the confidential information is no longer available to act on a requested amendment, the practice must address the request for amendment as though the practice had created the information.

 **Policy/Procedure:** A practice should:

- develop a procedure for determining when the originator of confidential information is no longer available; and
- institute a policy to handle requests for amendments when the originator no longer exists in the same manner that they handle requests for information that the practice has originated.


### Denying a Request for Amendment


 **Critical:** The final rule allows a covered entity to deny a request to amend confidential information if:


- the practice did not create the information (with certain exceptions);
- the information would not otherwise be available for inspection (see above, and subject to state laws); or
- the practice determines that the information in dispute is neither inaccurate nor incomplete.

 **Policy/Procedure:** A practice must:

- provide the denial in writing and include the basis for the denial and how the individual may make a complaint to the practice and the Secretary;
- process denials in sixty (60) days as noted above (the one-time extension of thirty (30) days is allowed if the practice provides the individual with the reason for the delay and the date by which the action will be completed);
- develop policies and procedures for making denials of requests for amendments, including reasons, access by personal representatives, access to psychological records, review procedures, and response times;
- develop letters for use when an extension is needed; and
- establish a tracking system for monitoring and reporting of timeliness of actions.

 **Critical:** An individual may submit a written statement of disagreement with the denial and the basis of such disagreement. If the practice prepares a rebuttal, it must provide a copy to the individual. ***The denial, disagreement and rebuttal must be linked to the confidential information in dispute.***

 **Policy/Procedure:** A practice must have a procedure for linking the denial, disagreement and rebuttal to the confidential information and for releasing that information whenever the confidential information in question is released for any purpose. (If a subsequent disclosure is a standard transaction adopted under the Transaction Rule, that cannot accommodate the denial, disagreement and rebuttal, the practice must separately disclose the additional material to the recipient of the transaction.)


 **Critical:** As noted under access, a denial of amendment may also trigger federal or state defined complaint procedures, especially in managed care products. Practices will need to determine if compliance with the rule's procedure will satisfy other federal and/or state complaint procedures including external appeal to departments of insurance.


---

# Accounting for Disclosures

Section 164.528 provides a right for individuals to receive an accounting of all disclosures of confidential information. Disclosure information must be made available for a 6-year period – beginning with the date the practice comes into compliance with this rule (no later than April 14, 2003). A record of disclosures **does not have to be made when those disclosures are:**

- to carry out treatment, payment and health care operations;
- to individuals of confidential information about them;
- made as a result of a valid written authorization;
- for the practice’s directory or to persons involved in the individual’s care;
- for national security or intelligence purposes;
- to correctional institutions or law enforcement officials;
- made prior to the compliance date (currently April 14, 2003); or
- made more than six years prior to the request.

 **Critical:** *Generally a practice needs to account for all disclosures not made for treatment, payment, or health care operations and made in the absence of an authorization. This includes disclosures required by law such as child abuse and mandated reports to public health agencies.*

 **Policy/Procedure:** A practice must have a procedure for collecting the audit trail information. In addition, the practice must have a policy to release audit trail information when requested and when determined to be appropriate. A practice must provide the accounting within 60 days, subject to a 30 day extension.


---


# Business Associates

The term “Business Associate” is defined as:

a person who acts in a capacity other than as a member of the workforce of a practice to perform or assist in the performance of a function or activity involving the use or disclosure of confidential information, or any other function or activity otherwise governed by the privacy regulations.


Examples of activities or functions that may be performed by a business associate of a practice include: claims processing or administration, data analysis, processing or administration, quality assurance, billing, and practice management. Business associates may also include persons who provide legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to practices, if confidential information is received from the practice in the course of providing such services.

 Before a practice may disclose confidential information to a business associate, “it must obtain **satisfactory assurances** that the business associate will appropriately safeguard the information.” The assurances from the business associate must be provided by means of a **written contract** or other agreement that documents the permitted and required uses and disclosures of confidential information by the business associate. ***The business associate cannot use or disclose the information in any manner that would not be permissible for the practice under the HIPAA privacy regulations.***

 **Policy/Procedure:** Practices will have to ensure that each business associate contractually agrees that it will:

- not use or further disclose the information other than as permitted under the contract or as required by law;
- use appropriate safeguards to prevent use or disclosure of the information other than as provided by its contract;
- report to the practice any use or disclosure not provided for by its contract of which it becomes aware;

- ensure that any agents to whom it provides confidential information agree to the same restrictions and conditions that apply to the business associate with respect to such information;
- afford individuals access their information as required by the rule (see Access above, page 37);
- make information available for amendment and incorporate amendments (see Amendment above, page 40);
- make available information to provide an accounting of disclosures;
- make its internal practices, books and records relating to the use and disclosures of confidential information received from, or created or received by the business associate on behalf of the practice available to the Secretary for the purposes of assessing the practice's compliance with the privacy regulations; and
- at the termination of the contract, if feasible, return or destroy all confidential information received from or created or received by the business associate on behalf of the practice.


 **Critical:** According to the rule, a practice is not in violation if its business associate violates its contractual obligations *only when the practice does not* have knowledge of the violation.

---

## Complaints to the Practice



Section 164.530(d) states that a practice must provide a *process for individuals to make complaints* concerning the practice's policies and procedures required by this rule or its compliance with such policies and procedures.

 **Policy/Procedure:** A practice must


- have a procedure in place to document all complaints received, and their disposition, if any; and
- work to mitigate any problems known to the practice (see next section).

---

## Mitigation



Section 164.530(f) states that a practice *must mitigate, to the extent practicable*, any harmful effect that is known to the practice of a use or disclosure of confidential information in violation of its policies and procedures or the requirements of the rule or of any of its business associates.


 **Policy/Procedure:** A practice must have a formal policy implementing this requirement and confirming that it will take all appropriate actions to correct known problems.

---

## Refraining From Intimidating or Retaliatory Acts




Section 164.530(g) states that a practice may not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against individuals or others. This specifically refers to individuals and others who bring issues to the attention of the practice, request access to or amendment of confidential information, or refuse to sign authorization forms. This applies to patients as well as staff.

 **Policy/Procedure:** A practice must have a formal policy implementing this requirement and confirming that it will refrain from intimidating and retaliatory acts.

---


## Waiver of Rights


Section 164.530(h) states that a practice may not require individuals to waive their rights under the rule as a condition of the provision of treatment. This also is addressed in the Notice of Privacy Practices (see page 27).


 **Policy/Procedure:** A practice must document this policy in its policy manual.

---

## Ensuring Confidential Information is Secure

 Section 164.530(c) states that a practice must have in place *appropriate administrative, technical, and physical safeguards* to protect the privacy of confidential information. Such safeguards refer to the security systems used to ensure the privacy of the information. The rule does not specify the safeguards to be used. Rather, the safeguards will be specified in a separate security rule that has not yet been finalized.

 **Critical:** The practice must make efforts to ensure confidential information is protected from unintentional use or disclosure. This may include administrative procedures, physical safeguards, technical security services, and technical security mechanisms.


 **Policy/Procedure:** The practice must “reasonably” safeguard confidential information from any intentional or unintentional use or disclosure. These procedures should be documented in the policy manual. Specific policies and procedures should include:

- designation of a security officer (who also can be the privacy officer);
- a disaster recovery plan, policy on workstation use, procedures for the storage and disposal of health information;
- development and implementation of data access control procedures;
- signing and amending contracts with business associates to protect the security of confidential information;
- providing security awareness training to all practice personnel;
- implementing technical security mechanisms to prevent unauthorized access;
- establishing a reporting and response system for security violations; and
- developing a security violation sanctions policy for the discipline of employees and contractors.

More specific guidance is provided in the following sections that reflect the key provisions in the Security Notice of Proposed Rulemaking (NPRM).


---

## Access Control

 Section 142.308(b)(3) of the Security rule requires practices to implement “access control” policies and procedures to protect against the unauthorized use, disclosure, modification, and destruction of information. This includes information stored on paper, in a computer system, in a personal digital assistant, or in any other format.

 **Policy/Procedure:** Practices must establish and maintain policies and procedures that:

- establish which staff members need access to specific confidential information and in which formats (e.g., paper records, the billing record, or an electronic medical record);
- outline the process for granting access to confidential information (e.g., how is a staff member formally granted the right to access the information);
- periodically review the levels of access granted to each staff member, and document that the review was completed;
- allow for the modification of an individual's rights to access information (either to give him or her more access or less access); and
- establish termination procedures, including removal of access to information and removal from authorized user lists.
- While the NPRM allows for three kinds of access controls – context-based, role-based, and user-based, most practices, given their size and technical sophistication, will likely have user-based policies and procedures, i.e., specific staff members will be granted access to specific information in specific systems.

 **Critical:** Practices need to recognize that access to information may be further limited by federal or state laws. Accordingly, practices must ensure that their policies and procedures accurately reflect the more stringent

requirements in state and federal law relating to sensitive information (e.g. psychiatric information and genetic tests).

---

## Physical Safeguards

☞ **Policy/Procedure:** Practices need to have “physical safeguards” to protect confidential information. Accordingly to the NPRM [Section 142.308(b)(3)(i–ix)], a practice must have appropriate policies and procedures to address each of the following items:

- **Disaster Recovery:** The process for restoring lost information in the event of a disaster, e.g., fire or natural disaster. This could involve storing a “backup” of the information offsite. How it applies to paper records is unclear in the NPRM and needs to be clarified.
- **Emergency Mode Operation:** The process for operating in event of a disaster. These policies and procedures must address how the practice will function in the event that information is temporarily lost.
- **Equipment Control:** The process for moving equipment, including computer hardware and software, to or from a practice. A record must be kept of the equipment and equipment cleaned or all confidential information before disposal or resale.
- **Facility Security Plan:** The process for securing the office, including the exterior and interior of the building from unauthorized access by individuals.
- **Physical Access Authorization Verification:** The process for validating that the individual accessing the information is authorized to access the information. This may involve the use of computer passwords. In a small practice this may be relatively straight forward, as it is likely that each individual in the office will have a need to access most, if not all, of a patient’s information, depending on the circumstances.
- **Maintenance Records:** Records documenting any repairs and maintenance to the physical plant, including the computers, doors, locks, etc.
- **Personnel Access Need-To-Know Procedures:** The process for ensuring that each individual only has access to the information he or she needs to perform their job. This is a potentially complex area, although in a small practice it is likely that each individual in the office will have a need to access most, if not all, of a patient’s information, depending on the circumstances.
- **Visitor Sign-In and Escort Procedures, if appropriate:** This probably will not be needed in most small practices, although the NPRM is not clear on this point.
- **Testing and Revision:** The process for ensuring that testing and revision of equipment and computer programs that involve confidential information is completed only by staff authorized to access the confidential information.


---

## Audit Controls




Each practice must establish an “audit control mechanism” to track and record all access to confidential information. Auditing is important so a practice can identify suspect data access activities, observe if high-risk patterns are present, assess its security program, and respond to potential weaknesses. The mechanism must record who accessed or attempted to access specific confidential information. In addition, who may access the log and how the log will be reviewed must be specified.

Audit control mechanisms, by necessity, will be provided by software featuring that capability. The NPRM states that it is expected that the capability of keeping audit trails will become standard in all health care software in the near future, spurred on by the universal emphasis on health information privacy.

 **Critical:** It is not clear how audit controls apply to confidential information in paper records. It appears that some logging of access to paper records may be required. This could be a burdensome process and clearly is not as simple as implementing a software package that automatically tracks each click of a mouse.


---


## Internal Audit of System Activity

 **Policy/Procedure:** Section §142.308(a)(6) of the NPRM requires practices to have an internal audit process. This process must provide for the ongoing review of who is accessing what specific confidential information. The process must be designed to identify potential security violations by reviewing audit trail and other information to ensure that only authorized individuals are appropriately accessing confidential information.

---


## Contingency Planning

 Section 142.308(a)(3) requires practices to have contingency plans to ensure confidential data are available following any kind of disaster or interruption. As mentioned above, the HIPAA requirements are “scalable.” Accordingly, the contingency planning that will be required in a small practice is expected to be fairly straight forward. Bigger practices and organizations will be required to have more elaborate contingency plans.


 **Policy/Procedure:** As stated in the NPRM, the key elements of a contingency plan include the following:

- **Applications and Data Criticality Analysis:** Each practice needs to evaluate where confidential information resides (e.g., paper and specific software programs) and which systems are critical to the operation of the practice (e.g., if the computer is not working, can the practice still treat patients, or if the fax machine is broken can the practice still order tests and get test results).
  - **Data Backup Plan:** Each practice must back up critical information on a regular and periodic basis. Off site storage of information is recommended. It is not clear how this will apply to small practices using paper medical records.
  - **Disaster Recovery Plan:** A practice must have policies and procedures regarding when a disaster is declared and how confidential information will be restored. For most practices, a temporary loss of information will not be a major concern, as practices usually can postpone patient care for a few hours or a day or can recreate key information quickly in order to continue treating a patient.
  - **Emergency Mode Operation Plan:** The practice must determine how it will operate in an emergency. Some practices may simply close for awhile and others may find that a loss of computer or even paper records simple means gathering additional background information at the beginning of each patient visit or, perhaps, ordering a few extra tests to ensure appropriate decisions are made.
  - **Testing and Revision Procedures:** The practice must have training for all staff about how to handle a disaster and must test all procedures of the disaster recovery plan.
- 

## Training

 Section 164.530(b) states that a practice *must train all members of its workforce* on the policies and procedures with respect to confidential information, as necessary and appropriate for the members of the workforce to carry out their function within the practice. What constitutes adequate training is not specified; however, it is reasonable to assume that members of the practice’s workforce must have sufficient training that they can address issues related to patient confidentiality and are generally aware of the practice’s


privacy and security policies and procedures. At least one individual in the practice must be assigned the responsibility for the development of the training program.

 **Policy/Procedure:** A practice must provide training as follows:

- to each member of its workforce by no later than the compliance date for the practice;
- thereafter, to each new member of the workforce within a reasonable period of time after the person joins the practice's workforce; and
- to each member of the practice's workforce whose functions are affected by a material change in the policies or procedures required by this rule, within a reasonable period of time after the material change becomes effective.

The training must include:


- awareness training for all staff;
- periodic security reminders to staff and contractors about the need to ensure security with emphasis on current security concerns;
- education concerning virus protection and other malicious programs, including how to prevent virus infections and what to do if a virus is detected;
- education about the importance of monitoring login success/failure, and how to report problems; and
- education about the rules relating to creating and changing passwords and the need to keep them confidential.


 **Critical:** Each practice must document that the training has been provided. This is one of the most important things a practice can do to assure itself that it is not running afoul of the rules and is getting the benefits of the increased use of electronic means of practice. Each person trained must sign a confidentiality agreement that is kept on file, stating that they understand the training and to reinforce each person's responsibility to protect and maintain the confidentiality of patient information.

---

## Sanctions

Section 164.530(e) states that a practice must *have and apply appropriate sanctions* against members of its workforce who fail to comply with the privacy policies and procedures of the practice and the requirements of the rule.

 **Critical:** Each practice must document that it has and will apply sanctions as appropriate.

 **Policy/Procedure:** The practice must implement policies and procedures to document its sanctions, how it applies those sanctions, and any sanctions taken.

---

## Policy Manual Checklist

Based on the above information (and not taking account of the NPRM), a Policy Manual must include policies and procedures addressing the following areas:

- Uses and Disclosures of Confidential Information** – Practice must document the requirements for use and disclosure of confidential patient information, including:
  - uses or disclosures to carry out treatment, payment, or health care operations (as described in Notice of Privacy Practices);
  - uses and disclosures for which an authorization is required;
  - exceptions to the requirement to obtain authorization; and
  - other requirements relating to uses and disclosures of confidential information, including:
    - the “de-identification” of confidential information;

- the “minimum necessary” provisions;
- marketing restrictions; and
- fund raising restrictions.
- Access of Individuals to Confidential Information** – Practice must allow individuals the right to access to inspect and obtain a copy of their confidential information, for as long as the practice maintains the information. Practices must have in place policies defining:
  - to what confidential information individuals have access;
  - who can request the information;
  - the procedures for requesting information;
  - the time frames for responding to a request;
  - when the practice can deny access; and
  - how an individual may appeal a decision to deny access.
- Amendment of Confidential Information** – Practice must give an individual the right to have a practice amend confidential information about the individual for as long as the information is maintained. The written policies must address:
  - the process for accepting a request for and making an amendment of confidential information;
  - how quickly a practice must respond to a request for an amendment of information;
  - how to proceed if the originator of the information is no longer available; and
  - the process for denying a request for amendment.
- Accounting for Disclosures** – Practice must provide a right for individuals to receive an accounting of all disclosures of confidential information.
- Business Associates** – Practice must obtain satisfactory assurances that its business associates will appropriately safeguard the information.
- Complaints to the Practice** – Practice must provide a process for individuals to make complaints concerning the practice’s policies and procedures.
- Mitigation** – Practice must mitigate, to the extent practicable, any harmful effect that is known to the practice of a use or disclosure of confidential information in violation of its policies and procedures or the requirements of the rule or of any of its business associates.
- Refraining From Intimidating or Retaliatory Acts** – Practice may not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against individuals or others.
- Waiver of Rights** – Practice may not require individuals to waive their rights under the rule as a condition of the provision of treatment.
- Ensuring Confidential Information Secure** – Practice must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of confidential information.
- Access Control** – Practice must implement “access control” policies and procedures to protect against the unauthorized use, disclosure, modification, and destruction of information.
- Physical Safeguards** – Practice must have “physical safeguards” to protect confidential information including:
  - Disaster Recovery;
  - Emergency Mode Operation;
  - Equipment Control;
  - Facility Security Plan;
  - Physical Access Authorization Verification;
  - Maintenance Records;
  - Personnel Access Need-To-Know Procedures;
  - Visitor Sign-In and Escort Procedures, if appropriate; and
  - Testing and Revision
- Audit Control** – Practice must establish an “audit control mechanism” to track and record all access to confidential information.
- Internal Audit of System Activity** – Practice must an internal audit process to provide for the ongoing review of who is accessing what specific confidential information.
- Contingency Planning** – Practice must have contingency plans to ensure confidential data are available following any kind of disaster or interruption.

- ❑ **Training** – Practice must train all members of its workforce on the policies and procedures with respect to confidential information, as necessary and appropriate for the members of the workforce to carry out their function within the practice.
- ❑ **Sanctions** – Practice must impose sanctions against members of workforce who fail to comply with privacy policies and procedures.