
Managing the Implementation of HIPAA and the Privacy Rule*

Marjorie A. Satinsky, MA, MBA, FACHE

President, Satinsky Consulting, LLC

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) has been called the most important piece of healthcare legislation since Medicare and Medicaid. Between now and April 14, 2003, medical practices that are covered entities must prepare themselves for compliance with one of four parts of HIPAA, the Privacy Rule, and with related parts of the Security Rule.

This article provides help for those of you who have not yet begun your work on Privacy and for those who have begun to address the challenges of Privacy compliance and need help along the way. It covers the following topics.

- HIPAA Basics: Purpose, History, and Ways in Which HIPAA Can Benefit Your Practice
- HIPAA: Timetable and Penalties
- Preemption of State Law
- Important HIPAA Definitions and Privacy Rule Standards
- Compliance with the Privacy Rule: One Step at a Time
- Challenges and Suggestions for Overcoming Them
- Helpful Resources

HIPAA Basics: Purpose, History, How HIPAA Can Benefit Your Practice

The Health Insurance Portability and Accountability Act of 1996 addressed two major problems in healthcare. One of those problems was the portability of health insurance. Historically, employees who changed jobs could not take their health insurance with them. As job changes have become more prevalent in our society, the portability dilemma has affected more members of the workforce. The portability section of HIPAA permits employees to continue their health insurance without waiting periods or pre-existing condition restrictions under certain circumstances. HIPAA also addressed the need to standardize the transmission of certain administrative and financial information and to simultaneously protect the privacy and security of personal health information.

HIPAA has four sections: Transaction and Code Set Standards, Privacy, Security, and National Identifiers. The Privacy and Security sections fall into HIPAA's Administrative Simplification category. April 14, 2003, is the deadline for compliance with Privacy and related Security requirements.

The HIPAA legislation and subsequent regulations can bring important benefits to medical practices. These benefits include:

- improved accuracy and efficiency in posting accounts receivable;
- automatic posting of payments to your bank account;
- automated insurance eligibility check that tells you who has insurance coverage and the amount of the co-payments and deductibles;
- streamlined claims filing process that can accelerate your reimbursement;
- reduced time that clinical staff spend on administrative processes so they can devote more time to patient care.

HIPAA Timetable and Penalties

Make sure you understand the HIPAA timetable and penalties before initiating the tasks that need to be accomplished by April 2003.

HIPAA Timetable

During the six-year interval since the passage of HIPAA in 1996, the federal government has begun rolling out regulations for each of the four sections. The rollout process is standard, but the timetable for implementation is staggered. For each section, the Department of Health and Human Services (DHHS) issues a proposed rule that specifies a time period for public comment. Based on comments received, the DHHS publishes a final rule that includes effective and compliance dates.

For example, the Transaction and Code Set Standards were issued on October 16, 2000. The original date for compliance was October 16, 2002. In response to the many questions that arose during the period for public review and comment, the government has allowed covered entities, such as your practice, to request a year's extension. Many of you filed for an extension. Your compliance date will be October 16, 2003, although you must begin testing your transactions before then. Also, by mid-2003, the DHHS will publish a proposed claims attachment rule, a supplement to the standard claims transaction rule that has already been issued. The supplement will provide additional information related to claims adjudication.

The proposed Privacy Rule was issued on December 28, 2000. In response to comments made during public review and comment period, the DHHS made many changes and issued the final rule on August 8, 2002, with an effective date of October 14, 2002. The deadline for Privacy compliance is April 14, 2003, just a few months away.

For Security, the DHHS issued the proposed rule in May 1998. A final rule has not yet been issued. When it is, compliance must occur within 24 months. Although compliance with Security Standards isn't imminent, parts of Security do impact Privacy and should be completed by the April 2003 deadline.

With respect to National Identifier standards, the DHHS expects to publish the final provider identifier rule and the proposed payer identifier rule by early spring 2003.

HIPAA Enforcement and Penalties

Although the DHHS has not yet issued a proposed HIPAA enforcement rule, remember that HIPAA contains standards, and standards are requirements. If you have postponed starting on HIPAA Privacy Rule activities because the burden of compliance feels overwhelming, rethink your position. If your practice is a covered entity under HIPAA, you don't have a choice. If you are still filing paper claims and hoping you can remain HIPAA exempt, remember that beginning in October 2003 Medicare plans to refuse to pay claims that are not filed electronically in practices with more than ten employees.

The DHHS has designated the Office of Civil Rights (OCR) to be responsible for implementing HIPAA. The OCR has the right to:

- investigate complaints received from individuals and organizations that believe that a covered entity, such as your medical practice, is not complying with HIPAA's Privacy Rule standards;
- assist covered entities in achieving compliance with the Privacy Rule;
- make determinations regarding exemptions to state law preemption.

At this point, we believe the government will not audit your practice for HIPAA compliance or schedule a site visit to your office. Rather, if individuals or organizations file complaints within 180 days of the alleged occurrence, the OCR will respond to the complaint and may investigate your practice. If there is an investigation, you must comply with the OCR's request to provide documentation of HIPAA compliance activities. Improper use or disclosure of protected health information (PHI) can result in both civil and criminal penalties, including fines and imprisonment.

Preemption of State Law

HIPAA and the Privacy Rule contain general guidelines for the relationship between federal and state laws. For example, the regulation says that the state law will prevail if the state law is more stringent than the federal law. The North Carolina Medical Society is currently assessing the impact of those guidelines and expects to support legislation to bring North Carolina law into conformance with HIPAA, with certain exceptions that will be outlined in the law. HIPAA specifically provides that state law prevails in the instances of reporting diseases, child abuse, birth or death, public health surveillance and investigation. It is believed that North Carolina statutes related to parental access to minor records would prevail over any HIPAA requirements.

Important Goals, Definitions, and Privacy Rule Standards

One of the most challenging aspects of HIPAA and the Privacy Rule is the introduction of new concepts. I recommend that you learn the concepts before taking specific action steps.

Start with the big picture of Administrative Simplification and focus on its three goals:

- improve the efficiency of healthcare delivery by standardizing electronic data interchange of administrative transactions between providers and payers;
- protect the privacy and security of individually identifiable healthcare information;
- empower patients by giving them new rights related to their individually identifiable health information.

The last goal is truly a reverse in the idea reflected in North Carolina practice guidelines that physicians are the owners of medical information about their patients. The Privacy Rule gives patients rights regarding their medical records and calls on physicians to help ensure those rights. In effect, physicians become the custodians of the records on behalf of their patients.

When you are clear about the goals of Administrative Simplification, move on to the 12 important HIPAA definitions and Privacy Rule standards. If you understand these clearly, you will make the compliance job easier for yourself. I've listed these items below and provided short explanations in Appendix 1.

- Covered Entity
- Protected Health Information (PHI)
- Individually Identifiable Health Information (IIHI)
- De-Identified Data
- Limited Data Set
- Patient Control over Health Information
- Limitations on Use and Disclosure of PHI
- Notice of Privacy Practices
- Authorization to Use or Disclose PHI
- Business Associates
- Marketing
- Personal Representatives

Compliance with the Privacy Rule: One Step at a Time

Compliance with the Privacy Rule includes five types of activities: learning the basics, developing and implementing policies and procedures, training your staff, documenting your activities, and ongoing monitoring. I suggest you organize your specific tasks within these major categories.

Although you will need to take many steps to achieve compliance, the steps aren't hard. They can be puzzling if you don't understand the important concepts. They can be confusing if you don't develop a logical

work plan. They can be time consuming if you don't know what resources are available to you and how to use them to help your practice.

To help you understand the scope of your work, I've listed the important steps in Appendix 2. The order in which you perform these tasks is optional and should be related to the ways in which you use internal and external assistance. Two of the earliest steps are the most important because they set the stage and tone for the remaining steps. These critical early steps are designation of a Privacy Official for your practice and walking around your practice to determine the gaps between the Privacy standards and your current operations and physical set-up.

HIPAA and the Privacy Rule require you to designate a Privacy Official for your practice. Use the sample job description in Appendix 3 to help you tailor specifications for your practice and designate the most appropriate person for the position.

Most practices that have a practice administrator designate that individual as the Privacy Official. Small practices that do not have a formal practice administrator may take a different approach. The physician(s) in the practice may become the Privacy Official(s) and direct the compliance process. In one primary care practice for which I am presently consulting, two physicians share responsibility for HIPAA. They lead the small HIPAA team and interact with the external consultant.

After you designate a Privacy Official, take a walk around your practice so you can compare your current operations and physical facility with HIPAA and Privacy Rule standards. Make sure to use a comprehensive checklist to do this "gap analysis." My preferred checklist divides practice functions into six categories: check-in, check-out, front office general; business office; human resources and training; clinical areas; medical records; and business associates. The checklist references relevant sections of HIPAA and the Privacy Rule and distinguishes between requirements and suggestions. It supplements what you note about your practice with specific action steps and gives you a place to check off progress and completion.

Challenges and Suggestions for Overcoming Them

Two obstacles to moving forward with Privacy Rule compliance are time and money. Let's talk about both issues and ways in which you can address them.

Time

Learning about HIPAA and the Privacy Rule takes time, and hours devoted to compliance are hours subtracted from patient care. Here are practical suggestions:

- Learn about HIPAA in the evening or on weekends, not in the middle of busy office hours when you and your staff are concentrating on patient care. You can give your patients and HIPAA your full attention, but not at the same time.
- Take the initiative to educate yourself. The North Carolina Medical Society sponsored a series of informational sessions in 2002 and these are also available on videotape. Some of the larger physician organizations in the state sponsor group training for multiple practices and may make that training available to non-members. Group training has two advantages: price and the opportunity to share suggestions with other practices.
- Engage outside help that suits your needs. As with any new federal healthcare requirements, HIPAA and the Privacy Rule have created a consulting frenzy. Don't be put off by the barrage of offers. HIPAA is complex but manageable, and you may indeed benefit from external help. If you engage a consultant to work directly with your practice, you have choices. You can ask the consultant to do most of the work, or you can ask for guidance and feedback so you can do most of the work. Both approaches can be effective, provided they meet your needs and budget. Appendix 4 lists training and consultation services that have been reviewed by the North Carolina Medical Society.

Financial

HIPAA has the potential to bring financial gain to your office, to reduce staff time spent on administrative work, and to improve patient satisfaction. Depending on the size of your practice, for \$3,000-\$4,000 (less for group programs) plus the cost of minor physical changes, if any, you can address Privacy Rule compliance in an organized timely way. Make the financial commitment; it's a long-term investment.

Helpful Resources

There are many HIPAA-related products on the market right now. The biggest challenge is determining what will help you the most. Attachment 5 lists books, on-line tools, and useful Web sites. The following general observations can guide you in your selection of resources.

- Books on HIPAA and the Privacy Rule: make sure you have in your office at least one comprehensive book on HIPAA that you can use as a desk reference. Once you master the basics, you need a good resource to help you answer less obvious questions.
- On-line material: some HIPAA and Privacy Rule material has been developed so you can download it from the Web site. This kind of information is particularly helpful when you need sample policies, procedures, and forms. Keep in mind, however, that it may be less comprehensive than the written desk references.
- Bookmark Web sites that provide information and ongoing updates about HIPAA and check these sites regularly. The Frequently Asked Questions (FAQ) sections are particularly helpful and offer good practical advice.

Conclusion

The April 14, 2003, deadline for compliance with the Privacy Rule and relevant portions of the Security Rule is quickly approaching. Begin by understanding HIPAA basics, timetable and penalties, the relationship between federal and state law, and important definitions and standards. Then move on to specific steps. Take advantage of training and consultation that is available in your area. Start now and finish on time.

The author gratefully acknowledges the assistance of Carol Ann Scheele, JD, Associate General Counsel, Health Delivery Systems, North Carolina Medical Society, and Jerome Stracke, President & CEO of Visantis Healthcare Solutions.

Ms Satinsky is President of Satinsky Consulting, LLC. She earned her BA in history from Brown University, her MA in political science from the University of Pennsylvania, and her MBA in healthcare administration from the Wharton School of the University of Pennsylvania. She is the author of two books: *The Foundation of Integrated Care: Facing the Challenges of Change* (American Hospital Publishing, 1997) and *An Executive Guide to Case Management Strategies* (American Hospital Publishing, 1995). She is also author of a chapter titled Advanced Practice Nurse in a Managed Care Environment that appears in the book *Advanced Practice Nursing: Changing Roles and Clinical Applications*, edited by J.V. Hickey, et al (Lippincott, 1996, and Lippincott, 2000). An adjunct faculty member at the University of North Carolina School of Public Health and the Duke University School of Nursing, Ms Satinsky is also a Fellow of the American College of Healthcare Executives and a member of the Medical Group Management Association. She may be reached at (919) 383-5998 or margie@satinskyconsulting.com.

* *Managing the Implementation of HIPAA and the Privacy Rule* is scheduled for 2003 publication in North Carolina Medical Board Forum. All content copyright © 2003, Satinsky Consulting, LLC.

Managing HIPAA: Appendices

APPENDIX I

Important HIPAA Definitions and Privacy Rule Standards

Covered Entity: HIPAA defines covered entities as health plans, healthcare clearinghouses such as billing services, and any healthcare providers (physicians, hospitals, nursing homes, etc.) that transmit health information in electronic form in connection with a HIPAA transaction.

Protected Health Information (PHI): With few exceptions, PHI includes individually identifiable health information (IIHI) that is held or disclosed by a covered entity regardless of how it is communicated (e.g. electronically, verbally, or in writing). HIPAA and the Privacy Rule spell out specific requirements for obtaining authorization to use or disclose PHI.

Individually Identifiable Health Information (IIHI): Any health information that is collected from a patient; and (1) is created or received by a healthcare provider or other covered entity or employer and (2) that is related to the past, present, or future physical or mental health or condition of an individual; OR the provision of healthcare to an individual, or the past, present, or future payment for the provision of healthcare at your practice; AND that could potentially identify an individual.

De-Identified Data: Covered entities can determine that IIHI has been de-identified and no longer contains PHI that is subject to Privacy Rule restrictions and requirements. The two ways to de-identify IIHI are the safe harbour method and the expert opinion method.

Limited Data Set: PHI that excludes specific, readily identifiable information about patients and their relatives, employers, and household members.

Patient Control over Health Information: HIPAA and the Privacy Rule give patients control of PHI. Covered entities can use PHI without authorization for Treatment, Payment, and Operations (TPO), with specific exceptions. Patients can request restrictions on the use or disclosure of PHI, and they can request that covered entities use alternative ways (e.g. work phone number) to contact them with confidential information.

Limitations on Use and Disclosure of PHI: HIPAA and the Privacy Rule require covered entities to use and disclose the "minimum necessary" PHI to accomplish the intended purpose. There are exceptions to this standard and specific rules for limiting the use of PHI to only those members of the workforce who need it to do their jobs.

Notice of Privacy Practices: Covered entities must develop, post, and distribute this document in order to inform patients about their rights surrounding the protection of their PHI. Covered entities must also use their best efforts to obtain written Patient Acknowledgement of Receipt of the notice.

Authorization to Use or Disclose PHI: The Privacy Rule gives individuals and their personal representatives the right to authorize the use or disclosure of PHI except for treatment, payment, and operations (TPO).

Psychotherapy notes are an exception to the rule. Their release always requires patient authorization.

Business Associates: A person or entity outside of your practice's workforce that is not a covered entity and that must use or disclose PHI to carry out certain functions or activities on behalf of your practice. Your practice must put in place Business Associate Agreements.

Marketing: HIPAA defines marketing as "making a communication about a product or service that encourages the recipients of the communication to purchase or use the product or service." Prior to disclosing PHI for marketing purposes, your practice must obtain written patient authorization.

Personal Representative: A person who, under applicable law, has the authority to act on behalf of an individual in making decisions related to healthcare. Examples are guardians and persons with power of attorney.

APPENDIX 2

Privacy Rule Compliance: One Step at a Time

HIPAA and the Privacy Rule are complex, not unmanageable. Take these steps before April 14, 2003.

- Educate yourself in HIPAA and Privacy Rule basics: overview, history, timetable, enforcement and penalties, and relationship between HIPAA and state laws.
- Dig deeper and review one of the many available HIPAA Glossaries so you are familiar with commonly used terms.
- Familiarize yourself with important HIPAA and Privacy Rule Definitions and Standards.
- Use a comprehensive HIPAA Privacy Checklist to walk around your practice and assess your current situation.
- Create a HIPAA Privacy Rule log so you can document in writing the activities that you perform and your accomplishments.
- Develop a HIPAA Privacy Official job description that is tailored to your practice's needs and designate someone within your practice to assume that responsibility.
- Develop and implement policies and procedures for the following:
 - general policies and procedures on PHI;
 - required disclosures: patients, public health purposes;
 - use and disclosure of PHI for treatment, payment, and operations within your practice and with respect to other practices;
 - disclosure of PHI for treatment, payment, and any operations of organized healthcare arrangements;
 - disclosure of PHI to family, friends, and disaster relief organizations;
 - incidental disclosures of PHI;
 - patient authorization to use and disclose PHI;
 - de-identification of PHI using safe harbor or expert statistician methods;
 - use of limited data sets for research, public health, or healthcare operations;
 - verification of identity of person requesting PHI;
 - minimum necessary requirement for using and disclosing PHI;
 - business associates and other vendors;
 - personal representatives who request PHI;
 - marketing;
 - psychotherapy notes;
 - commitment to consistency with notice of privacy;
 - consent forms;
 - general patient rights;
 - patient access to PHI;
 - patient requests for amendments to PHI;
 - patient requests for accounting of uses and disclosures of PHI;
 - patient requests for alternative communications;
 - patient Complaints;
 - general management of privacy rule;
 - privacy official/contact;
 - notice of privacy practices;
 - documentation relating to privacy policy;
 - workforce training;
 - internal sanctions of workforce who violate privacy policy;
 - mitigation;

- no retaliation;
- no waiver;
- safeguards.
- Train all physicians and staff on Privacy Policies.
- Document all training.
- Obtain signed Workforce Confidentiality Agreements from all physicians and staff.
- Develop and implement a methodology for monitoring compliance with the Privacy Rule.
- If your practice uses and discloses PHI for research purposes, develop and implement a Data Use Agreement.
- If your practice participates in an Organized Healthcare Arrangement, develop and implement a policy and procedures regarding disclosure of PHI to another participating entity.
- Read the Security Rule and make sure that relevant requirements are a part of your Privacy activities.
- CELEBRATE!

APPENDIX 3

Sample Job Description: Privacy Official

Practice Name:

Revision Date:

REPORTING RELATIONSHIP: Designate the individual(s) to whom the Privacy Official will be accountable in setting up your Privacy system and in maintaining it. You may want to designate several people.

GENERAL DESCRIPTION: Oversee the development, implementation, and maintenance of and adherence to the practice's policies and procedures related to the privacy and access of patients' protected health information (PHI) in compliance with federal and state laws and the practice's Privacy Policy.

ESSENTIAL DUTIES:

- Maintain current knowledge of applicable federal and state privacy laws, including but not limited to HIPAA and the Privacy Rule.
- Develop, oversee, and monitor implementation of the practice's Privacy Policy and ensure maintenance of the integrity of the Policy at all times.
- Regularly report to the practice governing body and officers (insert applicable term here) regarding the status of the Privacy Policy.
- Collaborate with legal counsel, other HIPAA consultants, management, and committees to ensure that the practice maintains appropriate privacy consent and authorization forms, notices, and other administrative materials in accordance with practice management and legal requirements.
- Patient Complaints: Establish and manage a process for receiving, documenting, tracking, investigating, and taking action on all complaints concerning the practice's Privacy Policies and Procedures in coordination and collaboration with other similar functions, and when necessary, with legal counsel.
- Patient Requests: Establish and oversee practice policies to address patient requests to obtain or amend patient records, restrict the means of communication, or obtain accountings of disclosures; ensure compliance with practice policies and legal requirements regarding such requests and establish and oversee grievance and appeals processes for denials of requests related to patient access or amendments to PHI.
- Privacy Training:
 1. Organize, deliver, and direct the delivery of privacy training and orientation to all members of the workforce (e.g. administrative staff, all clinical staff, including physicians, volunteers, and temporary employees) and other appropriate personnel.
 2. Set up and maintain a system for documenting privacy training.

3. Monitor attendance at Privacy Policy training sessions and evaluate participants' understanding of the information presented.
- Practice Compliance: Monitor compliance with Privacy Policy by performing periodic privacy risk assessments at each practice location and by and reporting results to practice board or governing body.
 - Evaluation: Monitor and evaluate, at least annually, the success of the practice's Privacy Policy in meeting the practice's goal for protection of PHI. As appropriate, make recommendations for changes and improvements.
 - Coordinate and participate in disciplinary actions related to the failure of practice members to comply with the practice's Privacy Policy and/or applicable law.
 - Monitor technological advancements related to Protected Health Information (PHI) protection and privacy for consideration of adaptation by the practice.
 - Coordinate and facilitate the allocation of appropriate resources for the support of and the effective implementation of the Privacy Policy.
 - Initiate, facilitate, and promote activities to foster privacy information awareness within the practice.
 - Cooperate with the Office of Civil Rights, other legal entities, and practice officers in any compliance reviews or investigations.
 - Act as point of contact for practice legal counsel and HIPAA consultant in an ongoing manner and in the event of a reported violation.
 - Maintain all Business Associate contracts and Confidentiality Agreements with non-Business Associate vendors and respond appropriately if problems arise.
 - Act as the practice-based point of contact for receiving, documenting and tracking all complaints concerning privacy policies and procedures of the practice.

REQUIRED EDUCATION/KNOWLEDGE/SKILLS: Organization and management skills; training.

REQUIRED EXPERIENCE: Familiarity with administrative and clinical functions of the practice.

PHYSICAL AND MENTAL EFFORT: Willing and able to devote significant effort to learning about new legal and regulatory requirements; ability to translate general requirements into practice-specific policies and procedures.

TIME COMMITMENT: Varies by practice.

SPAN OF CONTROL: Privacy resource for all administrative staff, clinical personnel, and patients, and link with legal counsel and other external consultants.

REQUIRED LEADERSHIP: able to assume strong leadership role.

DECISION-MAKING/INDEPENDENT ACTION: must be self-starter comfortable in taking the initiative and requesting guidance as needed.

APPENDIX 4

HIPAA Training and Consultation Programs Listed by North Carolina Medical Society: December 2002

For additional details and pricing, visit the North Carolina Medical Society Web site or contact specific vendors.

- [HIPAA Consulting and Training Programs for Physicians and Office Managers](#). Vendor: Smith, Anderson, Dorsett, Mitchell and Jernigan, LLP (Raleigh)
- [HIPAA Consulting and Training Programs for Physicians and Office Managers](#). Vendor: HIPAA Regulatory Compliance, PC. (Richmond, VA)
- [HIPAA Privacy: A How-to Guide for Your Medical Practice](#). Vendor: Gates, Moore, and Company, Atlanta, GA (in collaboration with Epstein, Becker, and Green).
- [HIPAA Gap Assessment and HIPAA Education and Training to Physicians and Office Managers](#). Vendor: Smith Moore, LLP in alliance with Health Resources Management.

- [HIPAA Legal Consulting & Assessment](#). Vendor: Harrison Kaplan, Attorney at Law, and Samuel M. Taylor; Attorney at Law. (Raleigh)
- [On-Site Education & Coordination, HIPAA University](#). Vendor: Health Resources Management. (Various locations in North Carolina)
- [HIPAA Privacy Workshops for Physician Groups](#). Vendor: Visantis (Cary) in collaboration with Smith, Anderson, Blount, Dorsett, Mitchell, and Jernigan, LLP and Satinsky Consulting, LLC.

APPENDIX 5

Helpful Resources on HIPAA and the Privacy Rule

There are many helpful HIPAA and Privacy Rule resources in the market place. This list contains books/manuals, Web-based self-assessment tools, and organizations with useful Web sites. Check with your professional or specialty organization to see what they offer. The free HIPAA catalogue available from Medical Arts Press (800.328-2179 or www.medicalartspress.com) is a comprehensive resource not only for books and Web-based material, but also for equipment and furniture that can help with HIPAA and Privacy Rule compliance.

Books/Manuals

Field Guide to HIPAA Implementation (2002). Chicago, American Medical Association Press. Authors: J. Root, DC, Kibbe, M. Hubbard, C. Hartley. Comprehensive desk reference covering all sections of HIPAA. Available directly from AMA and from Amazon.com.

HIPAA Policies and Procedures Desk Reference (available January 2002). Chicago, American Medical Association Press. Authors: M. Hubbard, K. Glover, C. Hartley. Specific policies and procedures for the Privacy Rule. Available directly from AMA and from Amazon.com.

HIPAA Answer Book (2002 Edition). Rockville, MD, HIPAA Compliance Alert. Easy-to-read alphabetized reference book. Available from publisher (877 397-1496) and through North Carolina Medical Society.

HIPAA Privacy Manual: A How to Guide for Your Medical Practice (October, 2002). Vendor: Gates, Moore, and Company, Atlanta, GA in collaboration with Epstein, Becker, and Green. Practical "how to do it" manual with sample policies and forms. Web or CD-Rom version also available. Available through North Carolina Medical Society or directly from Gates, Moore and Company.

HIPAA: A Short- and Long-Term Perspective for Healthcare (2002). M. Doscher. Chicago, American Medical Association Press. Comprehensive background information and analysis of potential benefits to medical practices.

Privacy Rule Self-Assessment Tools

HIPAA Privacy Manual. Gates, Moore and Company, referenced under books above.

HIPAA EarlyView™ Privacy. Vendor: North Carolina Healthcare Information and Communication Alliance (NCHICA), RTP, North Carolina. Available from NCHICA or through North Carolina Medical Society.

Organizations with Web Sites That Have Useful HIPAA/Privacy Rule Information

- [American Hospital Association](#)
HIPAA Web site
- [American National Standards Institute \(ANSI\)](#)
ANSI standards information and HIPAA-related articles
- [American Society for Testing and Materials \(ASTM\)](#)
Standard guides for health information access, individual rights, data security, CPR, and more
- [Association for Electronic Healthcare Transactions \(AFECHE\)](#)
HIPAA background, analysis, and information on workgroups

- [California HealthCare Foundation](#)
Free HIPAA Administrative Simplification: Tool Kit for Small Group and Safety-Net Providers
- [Centers for Medicare and Medicaid Services \(CMM\)](#)
- [Electronic Healthcare Network Accreditation Commission \(EHNAC\)](#)
HIPAA security accreditation information
- [Department of Health and Human Services \(DHHS\)](#)
HIPAA rules and proposed rules, comments, listservs
- [Healthcare Data Exchange \(HDX\)](#)
The Integrated Healthcare EDI Network. Comprehensive electronic transaction services for the health industry
- [Health Care Financing Administration \(HCFA\)](#)
HIPAA overview and links
- [Health Level 7](#)
Standards for exchanging, managing, and integrating data to support clinical patient care
- [Health Privacy Project](#)
Current information, fact sheets, and testimony
- [HHS Data Council](#)
HIPAA's Administrative Simplification provisions
- [Joint Healthcare Information Technology Alliance](#)
HIPAA privacy information
- [Massachusetts Health Data Consortium](#)
Summaries of National Proposed Rule Modifications, compliance checklist, legislative background, HIPAA acronyms
- [Medicare](#)
Medicare EDI information
- [National Council for Prescription Drug Programs \(NCPDP\)](#)
NCPDP identified standards for HIPAA
- [North Carolina Healthcare Information and Communications Alliance, Inc. \(NCHICA\)](#)
Multiple HIPAA resources including pre-emption analysis and tool for assessing current status of your medical practice
- [North Carolina Medical Society](#)
Recommended HIPAA reference materials and consultants
- [U.S. General Printing Office](#)
Numerous databases including the Federal Register, Congressional Record, and Code of Federal Regulations
- [Phoenix Health Systems](#)
HIPAAAdvisory contains information, tools, updates, glossary of terms, and links
- [Washington Publishing Company \(WPC\)](#)
HIPAA-EDI implementation guides, code lists, and Standard Transaction Format Compliance System (STFCS) information
- [Workgroup for Electronic Data Interchange \(WEDI\)](#)
Industry technical reports, HIPAA security matrix, and more