Implementation of the HIPAA Security Rule

Marjorie A. Satinsky, MA, MBA
President, Satinsky Consulting, LLC


Ms Satinsky

The passage of the Health Insurance Portability and Accountability Act (HIPAA) in 1996 gave the federal government the ability to mandate the ways in which health care plans, providers, and clearinghouses store and transmit individuals' personal health care information. Until HIPAA's passage, no national or industry standards governed the privacy and security of an individual's health information.

HIPAA has four parts: the Privacy Rule, the Security Rule, Transactions and Code Sets Standards, and National Identifiers. There is overlap between the Privacy and Security Rules, so if your practice meets HIPAA's definition of a Covered Entity and you already comply with the Privacy Rule, you have a head start on the Security Rule.

The deadline for Security Rule implementation for health care providers is April 21, 2005. If you are one of a handful of practices that does not file claims electronically, but are a health plan administrator, your compliance date is not until 2006. If you are like most of my clients, you are procrastinating about beginning the process of assessing your current status and taking steps that are appropriate for your practice. To help you meet that compliance date, in this article I compare and contrast the Security and Privacy Rules and tell you why I find Security to be the more challenging of the two. I provide a brief refresher on HIPAA as well as descriptions of the goals and important sections of the Security Rule. Finally, I make suggestions for successful implementation and tell you what pitfalls to avoid. At the end of the article, I provide a list of helpful resources and a glossary.

Comparison Between the Privacy and Security Rules

The Privacy and Security Rules complement each other. Privacy protects personal health information (PHI), and Security protects a subset of PHI, electronic protected health information (EPHI). Examples of EPHI are electronic data transactions, e-mail communications, practice management systems, personal digital assistants, text pagers, and Web site portals. Paper-to-paper faxes are not considered to be EPHI, but computer-generated faxes are. Voice telephone communications are not considered to be EPHI, but computer-based voice response units are.

Although there are general similarities in the implementation of both the Privacy and Security Rules, you need to be aware of the differences as well. To implement both Rules, you need to compare your current practice with specific standards, identify gaps between your existing situation and the standards, take corrective action, document your actions, monitor compliance on an ongoing basis, and train your staff regularly. Both Rules include written policies and procedures, Business Associate Agreements, a concept called "minimum necessary" need to know, employee sanctions for breach, designated responsibility, and preventive safeguards.

Although the two Rules have many areas of overlap, I think that the differences between them make the implementation of the Security Rule more challenging. These differences are: breadth of coverage, degree of direction, allowable management discretion, and responsibility(ies) for implementation.

With respect to breadth of coverage, the Privacy Rule deals primarily, although not exclusively, with your business operations, and so you can satisfy the Privacy requirements by designating responsibility and by developing and implementing specific policies and procedures. The Security Rule covers administrative, physical, and technical safeguards, as well as parts of your business operations, so compliance goes well beyond responsibility and policies and procedures. Depending on what you learn about your practice during the gap and risk analyses steps in your process, you may decide to make major modifications in your physical facility and technical data security.

"If your practice meets HIPAA's definition of a Covered Entity and you already comply with the Privacy Rule, you have a head start on the Security Rule"

With respect to direction, the Security Rule is more directive about securing EPHI than the Privacy Rule is about securing PHI. In my opinion, this difference is related to the complexity of security. Think about the many ways in which information technology might support your practice. You might have a practice management system, electronic health records, Web-based interactive functions, a lab computer, and many other functions.

The Security Rule allows more management discretion than does the Privacy Rule in two important ways. First, the Security Rule was written to acknowledge differences among practices. It is organized into standards and implementation specifications. The standards contain broad issues that all practices should address, and the implementation specifications support those standards. Implementation specifications can be *required* or *addressable*, giving you a great deal of discretion in what you do. The meaning of *required* specifications is clear; you must meet them. The meaning of *addressable* specifications can be confusing. Addressable doesn't mean optional; it means you must review each specification and implement it or document why you can't. If you can't implement a

particular specification, you must implement another measure that meets the related standard in some other way.

The Security Rule gives you more management discretion than does the Privacy Rule in a second way. Rather than prescribe what you *should* do, it encourages you to determine what you *could* do and then make decisions about what is appropriate for your practice. After you have identified any gaps between your practice and the standards, the likelihood of the occurrence of adverse events, and the estimated cost of fixing your problems, it is up to you to decide what, if anything, you will do and in what order. Thus, the Security Rule relies on your judgment more than the Privacy Rule does, making your job more difficult.

Finally, in my opinion, the two Rules differ with respect to responsibility for taking corrective action. Without exception, the 40 medical practices I have trained about the HIPAA Privacy Rule had the internal ability to develop the policies and procedures that were needed for compliance. These practices sought guidance and feedback from an external consultant, and they did the work themselves. Security is different. Not all practices have the internal expertise to perform comprehensive gap and risk analyses and take corrective action. Many practices will rely on outside experts for some or all of the work.

"Improper use or disclosure of either PHI or EPHI can result in both civil and criminal penalties"

HIPAA Refresher

Before I turn to the substantive part of the Security Rule, I want to remind you about the purpose of the HIPAA legislation and subsequent regulations. HIPAA addressed two major problems in health care. One of those problems was the portability of health insurance, and the difficulty that employees had in taking health insurance with them when they changed jobs. 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 that is transmitted by both electronic and non-electronic means.

With respect to compliance with HIPAA, the Department of Health and Human Services gave the Office of Civil Rights (OCR) responsibility for implementing HIPAA. The OCR has the right to investigate complaints from individuals and organizations that believe a covered entity (such as your practice) is not complying with Security or Privacy Rule standards, assist covered entities in achieving compliance with both Rules, and make determinations regarding exemptions to state law preemption.

The goal for HIPAA compliance is voluntary compliance through technical assistance. The OCR never intended to make regularly scheduled site visits to physician offices or perform practice audits. Rather, if the OCR receives a complaint about your practice within 180 days of an alleged occurrence, it will respond to the complaint and may investigate your practice. Improper use or disclosure of either PHI or EPHI can result in both civil and criminal penalties, including fines and imprisonment. As of the end of September 2004, the OCR had received approximately 9,000 complaints, many of which have been dismissed because they were inappropriate. The first criminal prosecution recently occurred in Seattle.

The relationship between HIPAA and state laws is more of an issue with the Privacy Rule than it is with the Security Rule. The Privacy Rule is a federal regulation, and in most states, including North Carolina, state privacy laws already exist. When the federal and state requirements differ, one of two things happens. In most but not all cases, if the state law is more stringent or restrictive than federal regulations, the state law applies. In some instances, however, the federal requirements "preempt" state law, and you are obligated to abide by the federal standards.

Security Rule Goals

The Security Rule sets forth four goals for covered entities such as your practice. You are required to:

- ensure the confidentiality, integrity, and availability of EPHI that you create, receive, maintain, or transmit;
- protect against any reasonably anticipated threats or hazards to the security, integrity, or availability of EPHI;
- protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required; and
- assure compliance by your workforce.

Making Decisions About Security Measures

I've mentioned that you have discretion in implementing the Security Rule. When you make your decisions, you can take into account the following factors.

- Size, complexity, and capabilities. (For example, small, mid-size, and large practices will have very different characteristics.)
- Technical infrastructure, hardware and software security capabilities.
- Costs of security measures that you estimate
- Probability and criticality of potential risks to EPHI. (For example, in eastern North Carolina, the probability of hurricane damage is great. If there were a hurricane, there would be a significant risk to EPHI.)

Administrative, Physical, and Technical Safeguards

The standards and specifications in the Security Rule are divided into three groupings: administrative, physical, and technical safeguards. The regulation itself contains a good matrix with detailed information on

each section that you can use as a reference. Here's a summary of the three sections. (The manuals and other resources referenced at the end of this article contain specific details.)

Administrative Safeguards

- Standards (9): security management process, assigned security responsibility, workforce security, information access management, security awareness and training, security incident procedures, contingency plan, evaluation, Business Associate contracts and other arrangements
- Required implementation specifications (11): risk analysis, risk management, sanction policy, information system activity review, assigned security responsibility, isolating health care clearinghouse function, response and reporting, data backup plan, disaster recovery plan, emergency mode operation plan, written contracts for Business Associates and other arrangements
- Addressable implementation specifications (11): authorization and/or supervision, workforce clearance procedure, termination procedures, access authorization, access establishment and modification, security reminders, protection from malicious software, log-in monitoring, password management, testing and revision procedure, applications and data criticality analysis

Physical Safeguards

- Standards (4): facility access, workstation security, workstation use, and device and media controls
- Required implementation specifications (2): disposal of EPHI and/or hardware on which it is stored, media reuse
- Addressable implementation specifications (6): contingency operations, facility security plan, access control and validation procedures, maintenance records, accountability, data back up and storage

Technical Safeguards

- Standards (5): access control, audit controls, integrity, person or entity authentication, transmission security
- Required implementation specifications (2): unique user identification, emergency access procedure
- Addressable implementation specifications (5): automatic log-off, encryption and decryption, mechanism to authenticate EPHI, integrity controls, encryption

Getting Started with Security

Here are practical steps you can take to comply with the Security Rule by the April 2005 deadline.

- **Designate a Security Official for your practice.** Your Security Official may or may not be the same person as your Privacy Official. You can outsource all or part of the responsibility to someone outside your practice.
- **Form a Security Team.** As with Privacy, Security Rule compliance is not a one-person show. Involve people from different parts of your practice in a team project. I recommend bringing together representatives of administration, a physician, a nurse, a front-office person, and a back-office person.
- **Do your homework.** Attend informational sessions and read about the Security Rule so you are familiar with the purpose, the overall approach, the three safeguards, and the organizational requirements. (I have listed some good resources at the end of this article.)
- **Develop your Work Plan.** One of the major obstacles to successful implementation of the Privacy Rule was failure to organize the work process. I'm convinced that the same will hold true with the Security Rule. Identify what you want to do and who will do it before you start, and keep track of your progress.
- **Take inventory of what's in place.** Every practice is starting from a different place, so begin with a comprehensive "gap analysis." I recommend the *HIPAA Security Tool Kit™ for Small Medical Practices*, available from Simplified Training Solutions, and resources available from the American Medical Association (AMA), Gates Moore & Company, the MGMA, and the North Carolina Information and Communications Alliance, Inc (NCHICA).
- **Analyze potential risks and vulnerabilities** and evaluate the likelihood and cost of each. Remember that an estimated cost that is more than you want to pay does not justify non-compliance.
- **Determine the priorities for your practice.** I saw what happened with the Privacy Rule. Practices saved money by copying policies and procedures from each other without really understanding the essence of what they were doing. This approach won't work for the Security Rule, since the solutions will be different for each practice. Make sure you work through your own issues.
- **Develop a budget for security.** Assume that implementation of the Security Rule will cost money. Make sure you spend your hard-earned dollars wisely. Once you know the priorities for your practice, develop a budget for the various tasks that could be done. Include the cost of allowing your current employees to spend time on implementation. Budget for external consultants if you need them. Include the cost of inexpensive software that you can purchase at your local office supply store and the cost of any physical modifications that you want to make to your of-

"As with Privacy, Security Rule compliance is not a one-person show"

fice. After you have completed your budget, decide what you will do and in what order, taking cost into consideration.

- **Develop, implement, and maintain appropriate security measures.**
- **Train your staff.**
- **Monitor what you have done on an ongoing basis.**

Ensuring Success

Given the complexity of the Security Rule, I think successful compliance in your practice depends on four factors: ensuring physician commitment; starting early; managing the project in an organized and accountable manner; and integrating your Security Policies and Procedures into your ongoing practice operations.

Physician Commitment

"The Security Rule is complex, and successful management requires good organization and accountability"

Physician commitment to compliance with the Security Rule sets the tone for the entire practice. If you understand the importance of the Rule and make it clear to both clinical and non-clinical staff that compliance is mandatory, not optional, you'll motivate your team to do a good job. In my experience with Privacy Rule implementation, I encountered many physicians who took a laissez-faire attitude about compliance, and their staff didn't bother to take the Rule seriously. The results were not surprising: practices that are sadly out of compliance and at great risk. Given the dependence of most practices on information technology to support practice operations, lack of physician commitment to compliance with the Security Rule and the likelihood of lack of compliance can have serious consequences. Conversely, physician support for compliance can reduce the potential of your experiencing problems relating to confidentiality, integrity, and availability of EPHI.

Starting Early

Given the scope of the Security Rule, April 2005 isn't far away. I think it's imperative to get started as quickly as possible so you can organize your work and set a timetable that's reasonable for you. If you designate your practice manager or someone else within your practice as the Security Official, that person is likely to have other responsibilities as well as security, so give him/her adequate time to organize and implement the project. If you outsource some or all of the Security Official responsibilities, getting an early start will ensure that your outside consultant makes your practice a priority.

Managing the Project in an Organized and Accountable Manner

The Security Rule is complex, and successful management requires good organization and accountability. Help your Security Official structure the tasks methodically and regularly report progress back to you as the owner(s) of the practice.

Integrating Security Policies and Procedures into Your Ongoing Practice Operations

The final key to successful implementation of the Security Rule is the understanding that your Policies and Procedures need to be integrated into your ongoing practice operations. Given the speed with which information technology is changing, you'll need to regularly reevaluate what you have and make ongoing improvements.

Pitfalls

Successful compliance with the Security Rule requires not only attention to important success factors, but also the ability to avoid common pitfalls. I encourage you to avoid making these mistakes as you move along: underestimating the effort that Security Rule compliance requires; not knowing when to ask for help and who to ask; not making compliance participatory.

Underestimating the Required Effort

Your Security Official has a big job. He/she needs to understand the Security Rule, assess your current situation, identify risks and vulnerabilities, assess the cost associated with each problem area, guide you in deciding what to do, develop a budget, do the work, implement corrective action, train your staff, and monitor your program on an ongoing basis. The undertaking isn't small, so you need to allocate sufficient time and money to do the job for your internal staff, external consultants (if you use them), or combination of the two. In my opinion, your Security Official should expect to spend 10 percent of his/her time on security between now and April 2005, and 3 percent thereafter.

Asking for the Right Help at the Right Time

More and more practices are using information technology to help them manage their practices. There is great variety in their approaches and timetables. Likewise, there will be great variety in the ways in which practices approach the Security Rule. Many small practices lack the expertise to do all that is necessary, and so they'll need help from one or more external consultants. I'm not talking about a general information technology consultant, but about a consultant with expertise in security. Other practices will outsource the entire Security Rule compliance function, and still others will outsource just part of it. Seek help at an early stage from a qualified consultant if you think you will need it.

Making the Compliance Process Participatory

I can't say enough for engaging your entire staff in the Security Rule compliance process. Sending a few people out for training and/or making a video avail-

able doesn't do the trick. A more effective approach is identification of not only a Security Official, but of a Security Rule Compliance Team. Let the team deal with the details, and then train the rest of the staff on the essentials. During the team activities and the staff training, encourage questions; you'll get a better result.

Conclusion

It is clear to me, and I hope to you, that you need to address Security Rule compliance immediately. If you take the right steps in a logical order, you'll not only comply with the Rule, but also give yourself the assurance that the information security that supports your practice is safe and sound.

Helpful Resources on HIPAA and the Security Rule

Manuals and Security Risk Assessment Tools

Gates, Moore & Company
www.gatesmoore.com
Authors of *HIPAA Security Rule Manual* that can be purchased on line from the company or through the North Carolina Medical Society.

American Medical Association
www.amapress.com
Handbook for HIPAA Security Implementation available directly from AMA Press or from *Amazon.com.*

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

MGMA
www.mgma.com
Tennant, R.M. and Krupp, A.N. (2004) *HIPAA Toolbox Tool 4. Standards for Electronic Security.* Debuque, IA. Kendall/Hunt Publishing Company.

Simplified Training Solutions
www.simplifiedtraining.com
HIPAA Security Tool Kit (2004) Kirby, J.D

Sites That Have Useful HIPAA/Security Rule Information

American National Standards Institute (ANSI)
www.ansi.org
ANSI standards information and HIPAA-related articles

American Society for Testing and Materials (ASTM)
www.astm.org
Standard guides for health information access, individual rights, data security, CPR, and more

California HealthCare Foundation
www.chcf.org
Free

Centers for Medicare and Medicaid Services (CMS)
www.cms.hhs.gov and ***www.cms.hhs.gov/medlearn*** and ***www.cms.hhs.gov/mailinglists***

Electronic Healthcare Network Accreditation Commission (EHNAC)
www.ehnac.org
HIPAA Security Accreditation information

Department of Health and Human Services (DHHS)
www.hhs.gov
HIPAA rules, comments, listservs

MGMA
www. mgma.com

Massachusetts Health Data Consortium
www.mahealthdata.org
Summaries of rules, compliance checklist, legislative background, HIPAA acronyms

Medicare
www.medicare.gov
Medicare EDI information

North Carolina Healthcare Information and Communications Alliance, Inc. (NCHICA)
www.nchica.org
Multiple HIPAA resources including pre-emption analysis and tools for assessing current Security status of your medical practice

North Carolina Medical Society
www.ncmedsoc.org
Recommended HIPAA reference materials and consultants

Phoenix Health Systems
www.phoenixhealth.com
HIPAAdvisory contains information, tools, updates, glossary of terms, and links

U.S. General Printing Office
www.access.gpo.gov
Numerous databases including the *Federal Register, Congressional Record,* and *Code of Federal Regulations*

Workgroup for Electronic Data Interchange (WEDI)
www.wedi.org
Industry technical reports, HIPAA security matrix, and more. See the Risk Analysis White Paper Working Draft Version1.0, July 2004.

"Let the team deal with the details, and then train the rest of the staff on the essentials"

……..

Glossary

Access: the ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any system resource that creates, maintains, or transmits EPHI.

Access Control: mechanisms and methods of providing access to authorized users while restricting access to others.

Addressable Specification: one of two types of implementation specifications contained in the Security Rule. A covered entity has several choices. It must implement an addressable specification if it is reasonable and appropriate. If not, the covered entity *must document* why it is not reasonable and appropriate and then : (1) implement an equivalent alternative measure, (2) implement a combination of the specification and an alternative, or (3) not implement the specification.

Administrative Safeguards: policies and procedures designed to prevent, detect, contain, and manage security violations. Examples are the selection and execution of security measures and the management of personnel as it relates to protecting EPHI.

Administrative Simplification (AS): Title II, Subtitle F of HIPAA. This section authorizes HHS to (1) adopt standards for transactions and code sets that are used to exchange health data; (2) adopt standard identifiers for health plans, health care providers, employers, and individuals for use on standard transactions; and (3) adopt standards to protect the security and privacy of personally identifiable health information.

Audit Controls: mechanisms employed to record and examine system activity.

Authentication: verification of the identity of a user or other entity as a prerequisite to allowing access to information systems.

Business Associates: a person or entity outside of your practice's workforce who uses or discloses individually identifiable health information (IIHI) or who provides services to a covered entity that involves the disclosure of IIHI. HIPAA Privacy and Security Rules require a Business Associate Contract with these persons or entities.

Centers for Medicare & Medicaid Services (CMS): the agency within HHS that administers the Medicare and Medicaid programs and that is responsible for oversight of HIPAA administrative simplification transaction and code sets, health identifiers, and security standards.

Covered Entities: the types of organizations to which HIPAA ap-

plies, including health plans, clearinghouses, and providers who conduct electronic transactions.

Computer Security Incident: an unusual occurrence or adverse event that occurs on any part of an information system and network.

Demilitarized Zone (DMZ): a network segment outside the internal network that has some security controls in place that are less restrictive than those in the internal network.

Disaster Recovery: a process by which a practice would restore any loss of data in the event of fire, vandalism, natural disaster, or system failure.

Electronic Data Interchange (EDI): electronic exchange of formatted data.

Electronic Protected Health Information (EPHI): individually identifiable health information protected by HIPAA that is transmitted by or stored in electronic media.

Emergency Mode Operation: procedures that enable a covered entity to continue to operate in the event of fire, vandalism, natural disaster, or system failure.

Encryption/Decryption: a method for securing data at rest and electronic transmissions, including e-mail, data files, and electronic transactions by transforming plain text into ciphertext that cannot be accessed without the proper encryption keys.

Facility Security Plan: a plan to safeguard the premises and building(s) (interior and exterior) of a covered entity from unauthorized physical access and to safeguard the equipment therein from unauthorized physical access, tampering, and theft.

Gap Analysis: comparison between the requirements of the HIPAA Security and Privacy Rules with the practices, policies, and safeguards that are currently in place.

Firewall: a device that examines traffic entering and leaving a network and that keeps some type of traffic from passing from one network to another network based on a set of rules. For example, a firewall can restrict traffic from the Internet to your practice's internal network.

Health Insurance Portability and Accountability Act of 1996 (HIPAA): a federal law that allows persons to qualify immediately for comparable health insurance when they change their employment relationships. Title II, Subpart F of HIPAA gives the Department of Health and Human Services (DHHS) the authority to mandate the use of standards for the electronic exchange of health care data; to specify what medical and administrative code sets should be used within those standards; to require the use of national identification systems for health care patients, providers, payers (or plans), and employers (or sponsors); and to specify the types of measures that are required to protect the security and privacy of personally identifiable health care information

Individually Identifiable Health Information (IIHI): Any health information (including but not limited to demographic information) that is collected from the patient and (1) is created or received by a health care provider or other covered entity or employer and (2) that related to the past, present, or future physical or mental health or condition of an individual; OR the provision of health care to an individual, or the past, present, or future payment for the provision of health care at your practice; AND that could potentially identify an individual.

Intrusion Detection System (IDS): security alarms that warn of possible inappropriate attempts to access networks, hosts, programs, or data by examining (ie, sniffing) network traffic.

Physical Safeguards: provisions of the Security Rule that protect unauthorized disclosure, modification, or destruction. These safeguards apply to facility access controls, workstation use and security, and standards for device and media controls.

Protected Health Information (PHI): any information in any form or medium that is created or received and that relates to the past, present, or future physical or mental health or condition of an individual or that can be used to identify an individual.

Required Standards: some of the standards in the Security Rule are specifically required. Those that are not are addressable. Covered entities must comply with required and addressable standards.

Risk: probability that a threat will exploit a vulnerability and expose an asset to a loss.

Risk Analysis: identification of vulnerabilities in resources and the threats to those resources in order to determine appropriate safeguards or controls. A risk analysis can enhance a gap analysis, and it is the foundation of a risk management program.

Risk Management: the ongoing process of ensuring that security risks are kept under control. A risk management program should follow a risk analysis.

Safeguards: risk-reducing measures that act to detect, prevent, or minimize loss associated with the occurrence of a specified threat or category of threats.

Scalable: capable of being scaled. The HIPAA Security Rule permits scalability to the needs of individual practices.

Secure Electronic Environment: an environment that has administrative procedures, physical safeguards, and technical security services and mechanisms in place to prevent unauthorized access to EPHI.

Technical Safeguards: technical safeguards apply to access control, audit controls, integrity, person/entity authentication, and transmission security. Four safeguards are required, and the others are addressable.

Technology Neutral: the Security Rule standards are based on the premise that technology changes on an ongoing basis. The Rule is stable yet flexible.

Virtual Private Network (VPN): method for providing secure remote access to the internal network or information systems behind a firewall by establishing a secure tunnel in a public network such as the Internet.

Vulnerability: an inherent weakness or absence of a safeguard that could be exploited by a threat that produces risk in a system.

Workforce: under HIPAA, employees, volunteers, trainers, and others under the direct control of a covered entity, whether or not they are paid by the covered entity.

……..

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). The *Forum* has published several articles by Ms Satinsky, including "Managing the Implementation of HIPAA and the Privacy Rule," in #4, 2002; "How to Determine If Your Practice Could Use a Professional Practice Administrator," in #2, 2003; "Using Information Technology to Improve Patient Care and Communication: A Practical Guide – Part 1," in #1, 2004; "Using Information Technology to Improve Patient Care and Communication: A Practical Guide – Part 2," in #2, 2004; and "Electronic Medical Records and the Development of Electronic Health Records and Electronic Patient Records," in #3, 2004. An adjunct faculty member at the University of North Carolina School of Public Health, Ms Satinsky is a member of the Medical Group Management Association. She may be reached at (919) 383-5998 or *margie@satinskyconsulting.com*.