

## **Health Information Privacy Heats Up the Political Agenda**

HIPAA (Health Insurance Portability and Accountability Act)

Legal and Implementation Issues

**Jonathan D. Bogen, MSPH, MBA, CHE**

**President, HealthCIO.com (<http://www.HealthCIO.com>) and Program Chair,**

**New England Health Information Management Systems Society**

P.O. Box 1986, Duxbury, Massachusetts 02331-1986 Phone: (781) 585-6002

### **ABSTRACT**

As we approach the end of the millennium, the patchwork of state and federal regulations regarding health information is coming under a set of federal regulations representing a national information infrastructure. The 1999 legislative calendar is filled with important healthcare regulatory issues, including information technology and privacy issues. Increasingly sophisticated technology presents opportunities in advancing integrated healthcare, improving access and quality of care, and reducing administrative costs. Along with this great promise, however, come increased threats in terms of privacy and confidentiality of medical information.

Information technology offers improvements in quality of care through reducing adverse drug events, duplicative tests and procedures, and availability of patient data on allergies and alerts. The movement towards evidenced-based medicine will be facilitated by access to large clinical data repositories for health services research and medical outcome studies.

## **HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT**

In 1996, the Health Insurance Portability and Accountability Act (HIPAA-PL 104-191) was passed with provisions subtitled Administrative Simplification. The purpose of this subtitle was to improve Medicare under title XVIII and XIX of the Social Security Act as well as the efficiency and effectiveness of the healthcare system through the development of a health information system with established standards and requirements for the electronic transmission of health information. Under HIPAA, the Department of Health and Human Services (DHHS) is responsible for developing national standards to protect the privacy of medical information by August 1999. If legislation has not been enacted by this deadline, then the DHHS will be required to promulgate such standards by regulation (See Legislation Update, page 8).

### **Administrative simplification rule status**

HIPAA will have important implications for all healthcare providers, payers, patients, and other stakeholders. The Administrative Simplification standards are lengthy and complex, with immediate impact being placed on the following areas:

- Standardization of electronic patient administrative and financial data
- Unique identifiers for providers, consumers, and employers
- Changes to most healthcare transaction and administrative information systems
- Privacy regulation and the confidentiality of patient information

The rules dealing with mature standards (ie, transactions and code sets) have been finalized (Table 1). Less mature areas, however, are still pending, including privacy concerns (ie, unique individual identifier) and privacy legislation on medical information (ie, medical records).

HIPAA provisions on financial and administrative transactions have also been finalized. In addition, HIPAA directs the DHHS to adopt standards for unique identifiers for individuals, employers, health plans, and healthcare providers. Vendors of practice management systems, EDI [electronic data interchange], as well as authorization and eligibility clearinghouses will need to comply with these HIPAA requirements. These standards apply to all payers, providers, claim processing clearinghouses, and employers. Payers who have not already adopted these standards will have until February 2000 to comply with the new healthcare EDI standards. Fines and other sanctions will be attached for noncompliance. Of note, the Health Care Financing Administration (HCFA) recently requested for a delay in finalizing HIPAA due to problems associated with Y2K re-mediation. A consortium of healthcare information management associations has opposed this delay, and it is likely an extension will not be granted.

One of the more controversial proposed regulations dealing with unique individual identifiers is likely to be delayed until after 1999. It has been placed on hold pending congressional action due to the controversy resulting from the Notice of Intent that was published in July 1998. The identifier for health plans is the only remaining rule yet to be proposed to Congress.

### **Standard identifiers**

HIPAA allows for the creation and use of unique patient, provider, and employer identifiers. Currently, no law defines a standard for these identifiers, which understandably has always been a source of tremendous confusion among providers. The standardization should result in less costly exchanges of healthcare data.

Providers will be assigned a unique identifier (national provider identifier or NPI) by an enumerator agency. This identification will be maintained by the National Provider Registry at HCFA. Providers who already have a Medicare assigned identification number will not need to register. The NPI must be used in connection with the electronic transactions identified in HIPAA—ie, provider-to-payer (vice-a-versa) and provider-to-pharmacy--and used by all electronic processing clearinghouses. The NPI will not replace a state license number or DEA – Drug Enforcement Agency number, however. The use of one NPI will be helpful in identifying suspected fraud and abuse across health plans. Employers will also be assigned a unique identifier or they can use their IRS employee identification number.

Unlike other countries with national healthcare system, the United States does not recognize a unique patient identifier. In July 1998, hearings on the individual identifier were held by the National Committee on Vital and Health Statistics. The major concern expressed by the consumer advocates was that the patient identification number would become the de facto standard for identifying individuals from cradle to grave regarding any transaction, not just healthcare related transactions.

### **Transactions**

Efforts are needed to help move health providers to “paperless” medical transactions. By moving medical transactions electronically, information will be exchanged more efficiently, which could result in better service for consumers.

Under HIPAA, every healthcare provider will be able to use a single standard electronic format to bill for services rendered. All healthcare plans would be required to accept these standard electronic claims or claim attachments. Currently, different insurers utilize different electronic and paper claims forms. This creates a confusing and cumbersome system, which tends to take a healthcare provider’s valuable time away from their patient. In addition, standard electronic

formats will foster the move to paperless healthcare transactions, which might lead to a reduction in the high administrative costs inherent in our insurance and reimbursement process.

The electronic claim proposal also includes new standards for other common transactions, including:

- Health claims or equivalent encounter information
- Healthcare payment and remittance advice
- Coordination of benefits
- Healthcare claim status
- Enrollment or disenrollment in a healthcare plan
- Eligibility
- Health plan premium payments
- Referral certification and authorization
- First report of injury
- Health claims attachments

These electronic claim proposals will also be used to report diagnoses and procedures. Thus, health plans will be able to pay providers, authorize services, certify referrals, and coordinate benefits using one standard electronic format per type of transaction.

By using a standard electronic format, providers will be able to inquire about whether a patient has insurance coverage, find the status of a claim, or request authorization for services or specialist referrals. Employers who provide health insurance to their employees and their dependents will also be able to use a standard electronic format to enroll or disenroll employees and to make premium payments.

The American National Standards Institute's Healthcare Informatics Standards Board (ANSI HISB). Upon the passage of HIPAA, ANSI HISB—a voluntary organization with members from almost every major developer of healthcare informatics standards in the United States—offered its services to the DHHS to prepare an inventory of existing healthcare information standards that pertained to the transactions specified by PL 104-191 of HIPAA. Based on the work of ANSI HISB, the Secretary of DHHS decided to recommend the adoption of X12N standards for health transactions excluding the retail pharmacy claim. The ASC X12 standards use the Health Care Claim (837) standard. It is already in use by a number of organizations to support transactions for health care billing, encounter information, and Coordination of benefits between providers, intermediaries and claims clearinghouses. Further information on ASC X12 implementation can be obtained from contacting the Data Interchange Standards Association (DISA) at 703-548-7005. X12N and the National Council for Prescription Drug Programs (NCPDP) standards met all the criteria to measure a standard's suitability. Some organizations, however, favored standards other than X12N for the professional and institutional claim standards. Nevertheless, these organizations wanted to migrate to the X12N claim format. The X12 standard represents the most widely used format for exchanging electronic information.

### **Developing code sets**

Currently, some health plans use regional or local codes for insurance transaction that may differ from plan to plan. To eliminate this confusion, transaction code sets are being proposed as initial HIPAA standards. These codes are all de facto standards that are currently in use by most healthcare plans, clearinghouses, and providers. These national code sets are mandated for use in some federal and state programs, such Medicare and Medicaid. Standards setting organizations (i.e., the Accredited Standards Committee X12N and National Council for Prescription Drug) have adopted these code sets for use in their standards.

### **Implementation**

Generally, HIPAA supersedes any state law. HIPAA should not, however, limit the ability of a State to require a health plan to report, or to provide access to, information for management audits, financial audits, program monitoring and evaluation, facility licensure or certification, or individual licensure or certification.

When the HIPAA rules go into effect, small health plans will have to comply no later than 36 months after the effective date of the final rule, which is effective 60 days after being published in the *Federal Register*. Larger health plans will have 24 months to comply. Healthcare providers and clearinghouses will be required to begin using the standards 24 months after the effective date of the final rule. It appears that most of the HIPAA standards and requirements will not be published until year end 1999.

Entities implementing standards earlier than the suspend date must be able to continue using old standards until the cutoff date. The DHHS recognizes that this will create problems; therefore, comments on early implementation impact and how it might be alleviated are sought. [See ASPE website address at **Table 4 Appendix**]

### **Security and electronic signatures**

HIPAA covers any information (oral or written) that is involved in a healthcare transaction, including patient name, place of employment, personal identifier, and address. HIPAA applies to any healthcare provider, clearinghouse, or plan that electronically maintains or transmits health information pertaining to an individual. HIPAA also mandates a set of rules to be implemented by health providers, payers, and government benefit authorities as well as pharmacy benefit managers, claims processors, or other transaction clearinghouses. The Act mandates that security standards must be applied to preserve health information confidentiality and privacy. These standards address four main areas:

1. Administrative procedures
2. Physical safeguards
3. Technical security services
4. Technical security mechanisms

The Act is sufficiently broad in two areas. First, it specifies security procedures without defining a de facto standard. Second, it presumably covers all electronic identifiable patient information, such as data repositories, outside outcomes databases required by the Joint Commission on Healthcare Organization or National Committee on Quality Assurance, or statewide data sets for rate setting or research purposes. In health services research, trends are more important than individual data, but the security standard may still apply to data even though the individual is not identified.

The security standard applies to individual health information that is maintained or transmitted electronically. This would include information on maintained on CD, computer tape, or other media as well as transmitted using private networks, Internet, Intranets or extranets. This is much broader than the specific transactions defined in the law. The electronic signature standard applies only to the transactions adopted under HIPAA. The security standard was developed with the intent of remaining technologically neutral in order to facilitate adoption of the latest and most promising developments in evolving technology and to meet the needs of healthcare entities of different size and complexity. The standard is a compendium of security requirements that must be satisfied. None of the transactions adopted under HIPAA requires an electronic signature at this time. The solution will vary from provider to provider, but each provider must meet the basic requirements. A concern expressed by healthcare providers is the cost of addressing all or some of the standard, especially when compliance requirements are vague.

The security standard mandates safeguards for physical storage and maintenance, transmission, and access to individual health information. Audit logs of any access to health information management system are required as well as secure workstations. The standard suggests a password-protected workstation that does not have any recording devices attached to be placed in a secure space. The standard also requires safeguards, such as encryption for Internet use. The use of digital signatures for Internet commerce is suggested but is not required by HIPAA.

### **MEDICAL RECORDS PRIVACY**

The issue of medical record confidentiality is a two-edged sword. Patients want their medical history secure and known only to their healthcare provider. Unfortunately, payers, regulatory agencies, service organizations, researchers, marketers, and other third parties are accessing healthcare information. Medical records are generally viewed by more individuals and organizations than any other private, personal record. Electronic health records offer improved efficiency in accessing medical records and presumably lower cost.

Access to an electronic record would overcome serious and frequent problems with availability of the paper record. The threat of easy access to medical information was recently highlighted by an incident at a hospital located in Michigan. A university student was able to access--through the hospital's public web site--private medical data normally used for scheduling (ie, patient names, addresses, phone numbers, social security numbers, employment status, treatments for specific medical conditions, and other data). This incident highlights the need for properly maintained security procedures, such as a simple password requirement to encrypted patient data.

There have also been well-published breaches in the security of paper-based medical records. Paper records inherent limitation is also a safeguard (ie, the sheer size and volume of any paper medical record inhibits massive theft). Conversely, a computerized patient database, if not encrypted and accessed, can be easily copied or changed.

### **Current legislation**

In September 1998, DHHS Secretary, Donna Shalala delivered her recommendation for new health privacy legislation. She stated, "The proposals we are making set a national standard for protecting the security and integrity of medical records when they are kept in electronic form. It is crucial to have these standards, as we move increasingly toward electronic medical records. But it is also not enough. In addition, we urgently need new legal protection to safeguard the privacy of medical records in all forms. The proposals we are making today will help protect against one kind of threat—the vulnerability of information in electronic formats. Now we need to finish the bigger job and create broader legal protection for the privacy of those records."

Currently, Congress is reviewing two bills that will ensure a patient's confidentiality (See Legislation Update, page 8). Under HIPAA, Congress is given until August 1999 to enact privacy protection. If Congress fails to act by that time, HIPAA authorizes the DHSS to implement privacy protection by regulation. Congress has drafted many new regulations legislating protection of medical data from unauthorized release or inappropriate use of health information, including information as part of a health plan participation, payment, or research. The laws mandate large penalties for infractions of the law. At the same time, the legislation attempts to specify exemptions that will include research purposes (ie, public health and clinical research).

All firms that transmit or maintain electronic health information will need to develop a security plan, provide training for employees, and secure physical access to records. Health information regarding individuals must be protected during transmission and maintained in electronic form. Other administrative procedures, physical safeguards, and technical security measures will also be needed.

Congress is currently reviewing the Patient Protection Act of 1999 (HR 4250), which protects patient confidentiality. Section 5001 of this bill addresses the issue of copying protected health information. This bill was originally part of the managed care reform bill that was passed in 1998 and has been re-introduced to Congress this year. In the 1998 bill, it included a provision that would allow the use of protected health information for certain healthcare operations, such as utilization review activities without patient authorization. In addition, the Act requires the Comptroller General to submit to Congress a compilation of state laws on the confidentiality of protected health information and an analysis of the effect of those laws on the provision of, and securing payment for, healthcare. Under HIPAA, the DHHS convened expert panels to make recommendations on privacy. Those recommendations focussed on five principles:

1. Medical information be used only for the purpose for which it was collected
2. Medical records be kept secure
3. Individuals have access to their own records, providing for accountability in the use of records and establishing penalties for their misuse
4. Individual privacy with penalties for their misuse
5. Balance individual privacy with the needs of public health

These recommendations would establish only a minimum basis of health information privacy requirements. Federal standards for the collection, use, and dissemination of health information would not pre-empt state laws that might be more protective of privacy, resulting in significant state-to-state variations in the treatment of health information.

Healthcare practitioners should be aware of the increased risk for invasion of patient's privacy and should help ensure confidentiality. Both the American College of Physicians and the

American Society of Internal Medicine recommend healthcare practitioners should advocate policies to secure the confidentiality of patient records within their institutions.

Until HIPAA final rules are promulgated, it is recommended to have a written policy governing the release of patient data with and without authorizations and to ensure that staff is properly informed on the policy. This policy should be available to any patient requesting this information. In addition, it is important to maintain an audit log of all releases of patient-related data showing when, what agency, and to whom the information was provided. Service organizations should adhere to the same guidelines on confidentiality as the provider organization. Audit logs of any computer access, both successful and unsuccessful, should also be kept in a form that is searchable and produces alerts when repeated, unsuccessful attempts are made.

Furthermore, the network should warn the user about the penalties of unauthorized access, including employment termination as well as more severe penalties. Under HIPAA, proposed penalties for wrongful disclosure of individual health information include:

- For false use of a unique health identifier, a penalty of a fine of no more than \$50,000 and/or imprisonment of up to 1 year
- For obtaining individual health information and the offense is committed under false pretenses: a fine of no more than \$100,000 and/or imprisonment of up to 5 years
- For disclosure of patient individual health information and the offense is committed with intent to sell, transfer, or use individuality identifiable health information for commercial advantage, personal gain, or malicious harm: a fine of no more than \$250,000 and/or imprisonment of up to 10 years

## **SECURITY AND THE INTERNET**

It is apparent to any computer user that there has been rapid explosion in the use of the Internet by organizations and individuals. The universality of the Internet simplifies communication, sharing of data, and transactions. The Internet offers tremendous potential for provider-to-provider communication (eg, physician-to-hospital, physician-to-pharmacy) and consumer-to-healthcare provider communication. Access to healthcare information in rural and underserved areas has improved through the use of telemedicine. It is now common for consumers to access health-related web sites for health information or enter chat rooms between individuals in health-related support groups and health experts.

### **Security policy**

HCFA and other government agencies are especially concerned with the security and integrity of information shared on the Internet. In accordance with HIPAA, HCFA issued an Internet Security Policy that provides a generic guideline for security. This policy covers any business using the Internet for either privacy-act data or when sensitive HCFA information is transmitted via the Internet. In 1998, HCFA issued a notice suspending the use of the Internet for Medicare transactions. HCFA was apparently concerned with the security of information in use of the public Internet for Medicare related transactions.

The risks to a healthcare provider of inadequate computer security include harm to a patient, liability of leaked information, loss of reputation and market share, and fostering public mistrust of the technology. Problem areas include the ease in compromising the front line security (ie, usernames and passwords), which can result in easy interception of private data--not to mention hackers who can easily impersonate the intended user. In addition, data integrity and cyber-terrorism are real threats as are the tremendous propagation of new and nasty computer viruses. The usual tools and techniques to protect web-applications include token-based authentication, encryption, smart cards or secure identification cards, and digital signatures. Alternatively, one

may use a private network that has security problems of its own, but avoids some of the problems of a public network.

### **Authentication**

HCFA requires the transmission of privacy-related information to include adequate encryption, authentication or identification of communication partners, and incorporate an effective password/key management system (Table 3).

Authentication is accomplished over the Internet and is referred to as an *in-band process*. This means proving who you are, which may involve one or more of the following: something you are; something you know; or something you have.

Internet authentication involves a combination of something you have (eg, hardware authentication) and something you know (eg, user name and password). Access control refers to what object you have access, such as a physical device or a particular patient directory, database, or other highly sensitive data. Data integrity involves the condition of the data at some point compared to its pure or original state.

### **Electronic mail**

The most common use of the Internet is for electronic mail (e-mail). Many reports predict tremendous increases in the use of e-mail as a communication tool between providers and patients. The confidentiality of e-mail and other forms of sending information, unless protected by strong encryption, can be read by anyone intercepting the information.

### **Due diligence for compliance**

A due diligence is expected of any business using the Internet for sharing information and as a communication medium. Techniques for Internet security are complex and variable. HCFA

requires that the Internet policy be recorded and audited. Any business using the Internet for either privacy-act data or sensitive HCFA information is required to inform HCFA of their intent at: Office of Information Services, HCFA, Security and Standards Group, Division of HCFA Enterprise Standards-Internet, 7500 Security Blvd, Baltimore, MD 21244.

### **CONCLUSION**

In the era of managed care and thin financial margins, the competitiveness of providers may depend on the use of information technology to streamline clinical and other business operations. Nevertheless, increased computerization of medical information requires increased surveillance of policies and procedures to protect the confidentiality of private medical data. Failure to develop, implement, audit, and document information security procedures could result in serious consequences, such as penalties and loss of reputation, market share, and patient trust. It is recommended that providers learn more about HIPAA through publications, seminars, and related web sites (Table 4).

## **Background**

American College of Physicians. Ethics manual, 4th ed. *Ann Intern Med* 1998;128:576-594.

Broccol B, Berritt G. Upcoming regulation of patient information. *J Health Information Managment Sys Soc* 1998;12:15-25.

Health Care Financing Administration. HCFA Internet Security Policy. November 24, 1998.

Health Insurance Portability and Accountability Act of 1996. Public Law. August 1996:104-191.

Hughes LJ. *Actually Useful Internet Security Techniques*. Indianapolis: New Riders Publishing; 1995: chap 1.

NCVHS. Subcommittee on Privacy Standards and Security. DHHS; July 20-21, 1998, Chicago, IL.

Patient Protection Act: Title V: Confidentiality of Health Information, HR 4250, Sec 5003, 1998.

Short K , Theil B. Preparing for legislative and regulatory issues. *Advances for Health Information Executives* 1999;3:37-48.

<p>Table 1</p> <p style="text-align: center;"><b>Notice of Proposed Rule Making Status</b></p> <p><b>Scheduled to appear before the 106<sup>th</sup> Congress</b></p> <ul style="list-style-type: none"> <li>• Standards for Electronic Transactions and Code Sets</li> <li>• National Standard Health Care Provider Identifier</li> <li>• National Standard Employer Identifier</li> <li>• Security and Electronic Signature Standards</li> </ul> <p><b>Not scheduled to appear in the 106<sup>th</sup> Congress</b></p> <ul style="list-style-type: none"> <li>• Notice of Intent for Individual Identifiers</li> </ul> <p><b>Status not available</b></p> <ul style="list-style-type: none"> <li>• National Standard Identifiers for Health Plans</li> </ul>
---

Table 2  
Proposed Transaction Code Sets

Code Set	Definition
<b>CDT-2</b> (Current Dental Terminology)	Used for reporting dental services
<b>CPT-4</b> (Current Procedural Terminology)	Used for administrative transactions by all physicians to code their services
<b>HCPCS</b> (Health Care Financing Administration Procedure Coding System)	Alpha-numerical codes for medical equipment, injectable medications, transportation services, and other services that are not included in CPT-4
<b>ICD-9-CM</b> (The International Classification of Diseases, Ninth Revision, Clinical Modification)	Classifies both diagnoses (volumes 1 and 2) as well as procedures (volume 3)
<b>NDC</b> (National Drug Codes)	Used for in pharmacy transactions and in some claims in reporting prescription medications

Table 3

### **HCFA Acceptable Approaches**

#### ***Authentication***

- Formal certificate authority-based use of digital certificates
- Locally managed digital certificates, providing all parties to the communication are covered
- Self-authentication as an internal control of symmetric private keys
- Tokens or smart cards; in-band tokens involve overall network control of the token database for all parties

#### ***Identification***

- Exchange of passwords and identities by telephone, US certified mail, bonded messenger, or direct personal contact
- Token or smart cards\*

\* Out-of-band tokens involve local control of the token database with the local authenticated server vouching for specific local users.

Table 4

**World Wide Web Resources**

The following is a listing of sites that offer HIPAA list-serve, which announce via e-mail when changes in NPRM are made

<http://aspe.os.dhhs.gov/admsimp/>

- Information on administrative simplification and the confidentiality of medical records

<http://aspe.os.dhhs.gov/ncvhs/>

- Department of Health and Human Services Data Council site, including the National Committee on Vital and Health Statistics schedule and transcripts of assorted public meetings

<http://www.vxnet.com/HIPAA%20Impact.htm>

- Information on the administrative and financial requirements of HIPAA

<http://www.wpc-edi.com/hipaa/download.html>

Information on HIPAA EDI standards and requirements

<http://www.jhita.org/admsimp.htm>

Joint Information and Technology Alliance web site

### **Addendum: Administrative Simplification Update**

The August 21st deadline for Congress to enact a medical privacy bill according to the provisions of HIPAA (Health Insurance Portability and Accountability Act) has passed. HIPAA is the first ever national regulation on medical privacy and is the most far-reaching federal legislation involving health information management affecting the use, release and transmission of private medical data. Health care providers will need to be in compliance with HIPAA as penalties are significant for non-compliance.

"The privacy of Americans is protected in their bank transactions, their credit card statements, and even their video rentals. Yet, until today, Americans had no federal privacy protections for their medical records, Secretary Shalala said. "These proposed standards are an important step forward in protecting the privacy of some of our most personal information."

On November 3, 1999 the Department of Health and Human Services published the NPRM (Notice of Proposed Rule Making) for Standards for Privacy of Individually Identifiable Health Information. You can download a copy at <http://aspe.os.dhhs.gov/admnsimp/pvcsumm.htm>. You can read it in the Federal Register (November 3, 1999) on pages 59917 through 60065.

The organizations covered under the Federal Privacy regulation include:

- Health care providers who transmit health information electronically
- Health plans
- Health care clearinghouses

The proposed rule only covers personally identifiable and protected "electronic information" only. Protected information includes information on or about a person's health information, health care treatment, or payment. This includes information stored in electronic form, sent electronically, on computer, or hardcopy printouts from any computerized system. Electronic images of documents would be covered but may not include microfiche under this rule. The covered health information cannot be disclosed or used without patient authorization except in cases of treatment, payment or health operations. Other exemptions include

Oversight of the health care system, including quality assurance activities;

- Public health, and in emergencies affecting life or safety;
- Research;
- Judicial and administrative proceedings;
- Law enforcement;
- To provide information to next-of-kin;
- For identification of the body of a deceased person, or the cause of death;
- For government health data systems;

- For facilities' (hospitals, etc.) directories;
- To financial institutions, for processing payments for health care; and

In other situations where the use of disclosure is mandated by other, consistent with the requirements of the other law.

Sanctions include:

For each provision violated, the Secretary of HHS can impose a penalty of up to \$25,000 in any calendar year. Criminal penalties include fines of up to \$50,000 for violations of the privacy regulation, or even more if an action involves "malicious harm" or selling data for commercial advantage. The regulation does not include a "private right of action" – that is, patients cannot sue entities for privacy violations.

***In case you or your facility is just learning about HIPAA, what you must do:***

What You Must Do

- Develop a policy regarding information practices. Providers would provide this notice to each patient at the first service after the effective date of the rule, and post a copy of the notice. Health plans must provide a notice to members at enrollment and at least every 3 years thereafter.
- Allow individuals to inspect and copy their protected health information. Reasonable cost-based fees for copying are permitted.
- Develop a mechanism for accounting for all disclosures of protected health information for purposes other than treatment, payment, and health care operations.
- Allow individuals to request amendments or corrections to their protected health information. Such requests would be accommodated if information created by the provider or plan was determined to be erroneous or incomplete.
- Designate a privacy officer who will be responsible for all necessary activities.
- Provide training to all staff or others who would have access to protected health information in the entity's policies and procedures regarding privacy.
- Establish administrative, technical and physical safeguards to protect identifiable health information from unauthorized access or use.
- Establish policies and procedures to allow individuals to complain about possible violations of privacy.
- Develop and apply sanctions, ranging from re-training to reprimand to termination, for employee violation of entity privacy policies.

- Have available documentation regarding compliance with the requirements of the regulation.
- Develop methods for disclosing only the minimum amount of protected information necessary to accomplish any intended purpose.
- Develop and use contracts that will ensure that business partners also protect the privacy of identifiable health information.

Be prepared to respond to requests for protected health information that do not require consent, such as for public health, health oversight, and judicial activities. Entities must have reasonable procedures for verifying the identity and authority of persons requesting such disclosures.

#### Recommendations to Providers

As previously stated, the HIPAA NPRM allows disclosure without patient authorization for purposes of treatment, payment, and healthcare operations. This would include credentialing activities, quality assurance, and utilization review activities. Agencies working under contract to the provider entity would be bound by HIPAA as well. As patient information is sometimes used for other purposes more related to marketing or to conducting surveys, the provider is obligated to disclose those instances under which circumstances a patient has the legal right of refusal. Under HIPAA, it is now unlawful to use patient information inconsistent with the original authorization. We are all aware of instances of patient data provided to pharmaceutical marketing organizations or other products companies. I'm sure many of you miraculously have received free infant formulas following the birth of your children.

Until HIPAA final rules are promulgated, it is recommended to have a written policy governing the release of patient data with and without authorizations and to ensure that staff is properly informed on the policy. This policy should be available to any patient requesting this information. In addition, it is important to maintain an audit log of all releases of patient-related data showing when, what agency, and to whom the information was provided. Service organizations should adhere to the same guidelines on confidentiality as the provider organization. Audit logs of any computer access, both successful and unsuccessful, should also be kept in a form that is searchable and produces alerts when repeated, unsuccessful attempts are made.