HIPAA Administrative Simplification: Tool Kit For Small Group and Safety-Net Providers

November 2001

Prepared for the
California HealthCare Foundation

by the
Pacific Health Policy Group

Purpose

This document will help small group/solo providers and safety-net providers gain a basic understanding of the HIPAA requirements**.** Key elements of each rule (or proposed rule) are described, followed by some suggestions for how to begin implementation efforts.

Section One: Background & Provisions

Section One provides specific implementation recommendations for each key HIPAA provision. The most important step your organization can take to organize its HIPAA compliance effort is the establishment of a HIPAA steering committee. *Your entire organization is responsible for HIPAA compliance.* Therefore, the understanding, commitment, and involvement of representatives from key clinical and administrative areas are essential to a well-structured compliance program.

The appendices include selected implementation and reference materials:

- Appendix A: Establishing a HIPAA Steering Committee
- Appendix B: Timeline for HIPAA Compliance
- Appendix C: HIPAA Resources on the Internet
- Appendix D: Compliance Questions for Outside Vendors
- Appendix E: Sample Security Policies and Procedures
- Appendix F: Checklist for Current Security Compliance
- Appendix G: Glossary

Section Two: Overview Presentation

Section Two provides a "training tool" for clinicians and senior managers to use in educating themselves and their staff. It provides an overview of the key HIPAA provisions, as well as a general description of the planning and implementation efforts necessary for the organization to achieve HIPAA compliance. The presentation can be distributed to staff as a handout, or it can be presented as a Powerpoint slideshow. The Powerpoint file can be found at http://ehealth.chcf.org.

Disclaimer

This guide is intended to inform others about the requirements for implementing HIPAA Administrative Simplification Requirements as of the date hereof. It is provided with the understanding that the authors and publishers are not engaged in rendering legal or other professional services. To obtain more current information on the requirements, or if legal advice or other expert assistance is required, the services of a competent professional should be sought. The authors and publishers specifically disclaim any liability, loss, or risk incurred as a consequence of the use, either directly or indirectly, of any information presented herein.

HIPAA Administrative Simplification Tool Kit

Section One:

Background and Provisions

Background

What Is HIPAA?

HIPAA stands for the Health Insurance Portability and Accountability Act of 1996 (also known as the Kennedy-Kassebaum Bill). While the primary focus of HIPAA was to improve health insurance accessibility to people changing employers or leaving the workforce, the act also addresses issues related to the electronic transmission of health-related data. Specifically, Title II, Subtitle F of the Act, entitled "Administrative Simplification," mandates national electronic transmission standards and specific protections for individual health information.

What Are the HIPAA Administrative Simplification Provisions?

There are four key provisions:

1. **National standards** for electronic transmission of health care data
2. **Unique health identifiers** for providers, employers, health plans, and individuals
3. **Security standards** to protect electronically maintained health information
4. **Privacy regulations** to protect individual health information

Final regulations for the national electronic transaction standards have been issued, with a compliance deadline of October 16, 2002. Final privacy regulations were issued on December 28, 2000, and ultimately adopted by the new administration on April 14, 2001, resulting in a compliance deadline of April 14, 2003, for most covered entities. The Department of Health and Human Services has announced that final regulations concerning unique health identifiers for providers and employers, as well as the final security regulations, are expected to be released in late 2001 or early 2002. HHS is currently developing regulations governing unique identifiers for health plans, while development of a unique identifier for individuals is currently on hold.

Background (cont'd)

Who Is Affected by the Regulations?

Three types of entities/organizations must comply with the regulations:

1. Health care providers (including physicians, clinics, hospitals, etc.)
2. Health plans
3. Health care clearinghouses[1]

If you submit any claims electronically or store patient records on a computer, you will need to comply with *all* of the new provisions. *All* plans and clearinghouses must comply with all the regulations. If you are a provider and you submit any claims or similar encounter information electronically, you also must comply with the new provisions.

Why worry about HIPAA now? The rules don't take effect for another year.

It's true that the earliest compliance deadline isn't until October 2002. However, *the regulations may require significant changes to your billing and data collection systems.* You may need to develop new policies and procedures to ensure that patient health data is protected. Privacy is currently a hot topic for many people. Your patients may have questions about what steps you are taking to ensure their confidentiality. It also makes good business sense to start preparing today. If you need to purchase any new hardware, software or make other technology modifications, you may be able to incorporate the changes in other upgrades you already have planned. And if you want to out-source some or all of your compliance activities, you will be in a better position to find competent vendors.

[1] Under HIPAA, a clearinghouse converts nonstandard data content and/or format to standard content and format. See Appendix G—Glossary for a more complete definition.

Provision 1: National Standards

General

If you submit claims electronically or plan to do so in the future, you will need to implement the new national transaction standards. While converting to the new standards is likely to incur an initial cost, once implemented, you will be able to submit a claim (in the standard format) to all health plans—including Medicaid and Medicare—and the plan will be required to accept it. Plans will no longer be able to customize the claims submission to suit their specific needs. Therefore, the initial implementation costs are expected to be offset over time by savings through significantly increased administrative efficiencies.

Transaction Standards

Standards have been established for eight administrative and financial health care transactions:

1. Health claims and encounter information
2. Enrollment/disenrollment in a health plan
3. Eligibility for a health plan
4. Health care payment and remittance advice
5. Health plan premium payments
6. Health claim status
7. Referral certification and authorization
8. Coordination of benefits

Standards for the first report of injury and claims attachments have not been adopted; these are expected later in 2001.

The ANSI ASC X12N standard[2] has been adopted for all transactions except pharmacy. For ASC X12N transaction standards, implementation guides and data dictionary, the Washington Publishing Company's Web site (http://www.wpc-edi.com) provides an excellent overview. For *pharmacy*, the standard is the NCPDP Telecommunications Standard Format Version 5.1 and equivalent NCPDP Batch Standard Version 1.0. Information on how to order the implementation guide and other documentation for the proposed retail drug claim standard is available at the National Council for Prescription Drug Programs Web site (http://www.ncpdp.org). (See Appendix C for more Internet resources.)

[2] See Appendix G—Glossary for a complete definition.

Provision 1: National Standards (cont'd)

Code Sets

HIPAA specifies code sets that must be used with the transaction standards. Most organizations are already using these code sets—although often in combination with a set of local codes. *Under HIPAA no local codes will be permitted.* The following code sets have been adopted:

- ICD-9-CM, Volumes 1 and 2 for diseases, injuries, impairments or other health related problems and causes
- ICD-9-CM, Volume 3 for prevention, diagnosis, treatment and management for hospital inpatients
- Combination of HCPCS and CPT- 4 for physician services and other health related services
- HCPCS for all other substances, equipment, supplies or other items
- National Drug Codes (NDC) for prescription drugs
- CDT-2 for dental services

Implementation

The transaction standards and code sets may require the least direct effort on the part of individual practitioners and small groups compared to the other key HIPAA provisions. Many small provider offices contract with a practice management software company or use clearinghouses for patient billing.

If your office contracts with a software company, contact the vendor to find out what steps it is taking to make its product HIPAA-compliant, when the changes will be complete, and when and how you will receive the updates and appropriate training. You will also need to find out whether you currently collect and store the information required for the HIPAA transactions. Your vendor should be able to tell you whether additional data will be required and give you advice on how to collect and store such data. (See Appendix D for a list of questions you should ask each vendor as part of your HIPAA implementation planning process.)

If your software vendor is not knowledgeable about HIPAA or does not intend to upgrade an existing system to one that is HIPAA-compliant, you will have to decide whether to purchase a new system or use a clearinghouse to convert data into HIPAA-compliant transactions. Under HIPAA, you can send transactions (in any format) to a clearinghouse for conversion to the standard format.

Provision 2: Unique Health Identifiers

General

To simplify the process of sharing health care information electronically, HIPAA mandates the use of unique identifiers for these four entities:

1. providers
2. health plans
3. employers
4. individuals receiving health care services (patients)

It is likely that an individual provider has multiple identifiers—at least one for each health plan or organization with which the provider does business. The U.S. Department of Health and Human Services (DHHS) has proposed the use of the National Provider Identifier (NPI), which was developed by HCFA for Medicare.

Employers and health plans will also have unique health identifiers. The current Employer Identification Number used by the IRS has been proposed for employers. The HCFA Medicare PayerID has been proposed for health plans.

The most controversial of the proposed identifiers, the patient identifier, was on hold until final privacy regulations were approved. Although the privacy regulations have been approved, the DHHS has not yet indicated when the selection and implementation of a patient identifier will occur.

Provision 2: Unique Health Identifiers (cont'd)

Implementation

None of the unique identifier standards have yet been set forth in a Final Rule. Compliance with the standards is required within 24 months of the adoption of the standard (36 months for small health plans, as defined under the Small Business Association's rules as plans with annual receipts of less than $5 million).

The proposed National Provider Identifier appears closest to implementation. DHHS has proposed that NPIs be issued by the National Provider System (NPS) based on information entered into the NPS by one or more organizations known as "enumerators." Under this proposal, providers who participate in Medicare would be enumerated first. These providers would not have to request an NPI; they would automatically receive one. New and non-Medicare providers not yet enumerated who wish to participate in Medicare would receive an NPI as part of the enrollment process.

Similar to Medicare, Medicaid and non-Medicare federal health plans would use existing databases to enumerate and assign NPIs automatically to participating providers. If a provider was already enumerated by Medicare, that NPI would be communicated to the second program. After the initial enumeration, new health care providers who wish to participate in Medicaid or a non-Medicare federal health plan would receive an NPI as a part of the enrollment process.

A provider who does not transact any business with federal health plans or Medicaid but does conduct electronically transactions governed by HIPAA would be enumerated via a federally directed registry. Health care providers would apply to the registry for an NPI.

Provision 3: Security Standards

Health Care Data

Under HIPAA, security standards have been proposed for all patient-specific information stored and/or transmitted electronically. A Final Rule has not yet been published. In the proposed rule, the security standards are grouped into four general categories:

- **Administrative safeguards**. This category includes elements such as: certification of your security program, "chain of trust partner agreements" for entities with which data is shared, formal data backup and recovery plans, security policies and procedures, and staff training.

- **Physical safeguards**. This category includes elements such as: the assignment of an individual to be accountable for security, formal procedures for the receipt and removal of hardware and software into and out of a facility, procedures for limiting physical access to a facility, and other physical safeguards to protect against unauthorized access to information.

- **Technical security measures.** This category includes elements such as: specific mechanisms to limit access to information, audit controls to record system activities, mechanisms for obtaining consent for use and disclosure of health information, measures for ensuring that data has not been altered or destroyed in unauthorized manners, and mechanisms for "authenticating" entities that are accessing information (for example, passwords).

- **Technical security mechanisms**. This category consists of specific protections for facilities that use communications or networks, such as: access controls, alarms (if data is accessed without authorization), audit trails, encryption (if data is transmitted over open networks), and mechanisms for confirming the identity of each entity/person accessing information.

Provision 3: Security Standards (cont'd)

Implementation

Going back to the four categories of security measures, the small provider would meet each requirement as follows:

1. **Administrative safeguards** would be met by developing, implementing, and maintaining an office procedures manual that includes: contingency plans, records processing procedures, procedures for controlling access to health data, procedures for notification if information has been accessed by an unauthorized party, and training procedures/materials. (See Appendix E for sample policies and procedures.)

   If the provider contracts with a third party to process claims, "chain of trust" language would need to be incorporated into the contract with the claims processor.

2. **Physical safeguards** would be met by using locked rooms and/or closets to secure equipment, developing procedures for storing backed-up data, disposing of unneeded data, and logging off when leaving computer terminals unattended. Workstations should be distanced from public areas, and all staff should receive training on security awareness.

3. **Technical security measures** might be met by implementing a "user-based" access model in which each staff person who is granted access to health data is assigned a unique user-name and password combination. Emergency access requirements would be met if two individuals in the office had full access to health information. Software could be purchased to satisfy the audit requirement.

4. **Technical security mechanisms** would likely require the purchase of software with the required elements. For example, if a provider sends data via the Internet, some form of data encryption is required. On the other hand, if the provider sends data to a clearinghouse via a private wire or dial-up connection, the required elements may already be in place.

Provision 3: Security Standards (cont'd)

Implementation for Small Providers

The draft security measures are intended to be *scalable;* that is, small providers will not need to implement the more extensive and technically sophisticated measures that may be required for a large health system. The proposed rule includes an example of how a small provider office might implement appropriate security measures. The example outlines the following actions:

- "Self-certification" of security measures performed by a knowledgeable staff person or vendor
- Development of policies and procedures to address risks to health information
- Development of contingency plans for limiting potential damage to health information—such as a routine process for backing up data and storing back-up media at a different location, obtaining a PC maintenance contract, and arranging for use of a backup PC as needed
- Documentation of personnel security policies and procedures
- Appointment of a staff person with responsibility for implementing the personnel security policies (for example, granting and documenting access to health information, carrying out staff training, etc.)
- Appointment of a staff person (likely the same person as above) with responsibility for "Security Configuration Management and Termination Procedures"; for example, purchase of appropriate hardware/software features (virus-checking software, etc.), obtaining keys and changing combinations or passwords upon termination of employees
- Creating/purchasing mechanisms to track access to data (such as software that automatically keeps an audit trail whenever files are accessed)

Appendix F provides a tool to evaluate, on a preliminary basis, the readiness of your organization to meet the proposed HIPAA security procedures. Because DHHS requires compliance certification, and because compliance will require substantial preparation on the part of many health providers, it is essential that such a preliminary evaluation be performed as soon as possible. Once an evaluation has been performed, your organization can better understand what must be done to achieve HIPAA compliance, and the resources required to do so.

Provision 4: Privacy Regulations

Background and Consent

A Final Rule on privacy was published December 28, 2000, under the Clinton administration. The Bush administration re-opened the comment period and ultimately approved the regulation, effective April 14, 2001. Many national health associations publicly voiced concerns with the Final Rule. In response to these concerns, on July 6, 2001, Secretary Tommy Thompson of the Department of Health and Human Services issued guidance on the Privacy Rule.

While this document is based on the Privacy Rule as published on December 28, 2000, the guidance issued in July 2001 offered clarification including:

- A client's consent need only be obtained once by a specific provider
- DHHS expects to change the privacy rule to permit pharmacists to fill prescriptions phoned in by a patient's doctor before obtaining the patient's written consent
- DHHS may reevaluate the Privacy Rule to ensure that parents have access to specific information about the health and well-being of their children

Under the final Privacy Rule (effective April 14, 2001), individually identifiable health information may not be used or disclosed unless a patient's permission is obtained or disclosure is specifically permitted under HIPAA.[3] Patient consent is required for use or disclosure of information for three purposes: treatment, payment, and other health care operations.

The Privacy Rule refers to patient consent and authorization. In general, *patient consent* relates to information used for treatment-related purposes and *patient authorization* refers to disclosure of information for non-treatment purposes (for example, employers).

Generally, practitioners will need to get and retain evidence of patient consent prior to the use or disclosure of health information (except in certain situations, as described below). Most practitioners will likely develop or adopt a standard consent form (or incorporate required language in existing consent forms) for completion during a patient's initial visit. This consent form will then be maintained in the patient's file.

[3] HIPAA explicitly allows disclosure of patient health information *without* consent for the following situations: emergency circumstances, identification of the body of a deceased person or the cause of death, public health needs, research, oversight of the health care system, judicial and administrative proceedings, limited law enforcement activities, and activities related to national defense and security.

Provision 4: Privacy Regulations (cont'd)

Other Key Provisions

- **The "minimum necessary" concept**: This applies to the use of health information and requires that reasonable efforts be made to limit the information to the "minimum necessary" to accomplish the intended purpose (for example, a covered entity may not use the contents of an entire medical record, except when the entire medical record is reasonably necessary). As a practical matter, providers will need to evaluate how they use information within their own organization. They will need to consider whom they grant access to, and whether that person really needs access to all the information they currently get.
- **Notice**: Covered entities must provide a "notice of privacy practice" to each individual. The notice must describe the patient's rights and the entity's legal responsibilities with respect to protected health information.
- **Written contracts/agreements**: For all "business associates" with which protected health information is shared, a written agreement must be in place that provides for appropriate safeguarding of such information. This standard does not apply when information is being shared with a health care provider for the purpose of treatment.
- **Designation of a privacy officer**: Every covered entity (including individual practitioners) must designate a privacy officer who is responsible for the implementation of and ongoing adherence to privacy policies and procedures.
- **Development of policies and procedures**: Each entity must develop policies and procedures and provide staff training to ensure that health information is protected.
- **Rights of individuals**: The rules provide significant rights to patients, including the right to inspect and receive a copy of their protected health information, and to request amendments to such information. Amendments might include additional test results and/or diagnoses performed by another provider that would be incorporated into the record.[4]

  Individuals have the right to receive an accounting of disclosures of protected information. However, disclosures for treatment, payment or health care operations, and certain other disclosures are exempted from this accounting. Individuals have the right to request restrictions on the use and disclosure of information that go beyond those provided in the rule (entities are not required to agree with such requests).

[4] Providers have the right to deny inclusion of an amendment for a variety of reasons. In response to a denial, the patient may file a Statement of Disagreement that becomes part of the record. The provider can similarly file a rebuttal to the Statement, should s/he so choose.

Provision 4: Privacy Regulations (cont'd)

Implementation

Compliance with the Privacy Rule will not be required until April 14, 2003, but providers are advised to start compliance activities earlier. Providers can take the following preliminary steps to comply:

1. **Review existing practices**: Do you have written policies and procedures in place? If so, consider appointing someone within the office to compare existing procedures against the rules. If not, someone within the office must be appointed to create policies and procedures that comply with the rules. (See Appendix E for sample security policies and procedures.)

1. **Conduct preliminary staff training**: It is good practice to remind office staff about the need to preserve confidentiality of individual health information. In many cases, information may be disclosed accidentally—through casual conversations with co-workers or family members, forgetting to secure information by locking file cabinets or leaving records open on computer screens, or by not destroying papers that contain confidential information.

3. **Watch for more information** in journals, association mailings, and online publications or at conferences and workshops. Many compliance resources are already available, including some model policies and procedures. (See Appendix C for Internet resources.)

Early compliance efforts will help address patient concerns regarding privacy issues (the Association of American Physicians and Surgeons reports that 87 percent of its members have had a patient request that information be withheld from their medical records). Early compliance steps will also give providers additional (and likely necessary) time to develop a more comprehensive compliance plan.

Appendix A: Establishing a HIPAA Steering Committee

The steering committee should include individuals who represent the entire organization and its uses of health care information. The following five positions form the core of any HIPAA steering committee. (Other positions—largely dependent on the size of your organization—which should be considered for ad hoc membership, are included on the following page).

Core Committee Members

- **Senior Level Manager/HIPAA Compliance Officer:** While information technology is a major component of HIPAA compliance, HIPAA initiatives may be better managed as a strategic business rather than as an IT issue. A senior-level manager who is well informed of the business issues and technology aspects associated with HIPAA compliance should be selected to lead the HIPAA compliance effort.
- **Physician Representation:** Successful compliance with HIPAA regulations requires the cooperation and inclusion of physicians to address information accessibility and appropriateness.
- **Nursing/Allied Health Professional Representation:** Many of the changes associated with HIPAA compliance will affect the organization's day-to-day operations. It is essential to the success of HIPAA initiatives to include clinicians who are able to articulate the effect of HIPAA implementation on clinical operations.
- **Chief Information Officer/Information System Consultant:** HIPAA will have a tremendous impact on existing technology, as well as require the consideration of new technology to effectively support a comprehensive compliance strategy. The involvement of the CIO (or whomever is responsible for the information systems in your organization) is critical to successful HIPAA implementation efforts.
- **Legal Counsel:** Security and privacy regulations require numerous written policies, binding procedures, forms of agreements and contractual provisions. Legal counsel must be involved in developing these documents. In addition, documented participation by legal counsel on the HIPAA compliance steering committee may mitigate penalties in the case of adverse events.

Appendix A: Establishing a HIPAA Steering Committee (cont'd)

Other Committee Members

- **Chief Financial Officer:** Consider having the CFO attend the committee meetings during times of key decision-making or when major milestones are approaching. This will help the CFO gain a better perspective of the financial realities associated with HIPAA compliance.
- **Clinical Departments:** Many of the changes associated with HIPAA compliance will affect major clinical departments and affiliates, including, but not limited to: nursing, pharmacy, radiology, surgery, respiratory, clinics, long-term care facilities and home health. It may be prohibitive to include representation from each area, but it's essential to the success of HIPAA initiatives to have key departments represented.
- **Education Department:** Significant education—initially and ongoing—will be required to comply with HIPAA. Include a representative from the education department (or whomever will be responsible for conducting HIPAA educational sessions, for example, Human Resources) to ensure timely and accurate development of employee and patient education during the implementation of HIPAA standards.
- **Facilities Management:** HIPAA contains provisions for ensuring the physical safeguards of patient information. Facilities management (physical plant) representation is important to ensure compliance with these mandates.
- **Risk Management:** Risk identification, assessment, and mitigation are imbedded in HIPAA compliance. Results must be achieved and documented through policies and procedures development and implementation. For this reason, risk management should be represented on the committee.
- **Senior Executives/Board:** Given the enterprise-wide impact of HIPAA plus the potential personal liabilities in the event of an adverse event, regular status reporting to the board or an existing board committee should occur.

Appendix B: Timeline for HIPAA Compliance

The following table is adapted from the HIPAAdvisory (www.hipaadvisory.com) Tentative Schedule for Publication of HIPAA Administrative Simplification Regulations (as revised June 2001).

	NPRM* Published or Expected	Final Rule Published or Expected	Compliance Required†
Transactions and Coding	May 1998	August 2000	October 2002
National Provider Identifier	May 1998	2001‡	TBD
National Employer Identifier	June 1998	2001‡	TBD
Security and Electronic Signatures	August 1998	2001‡	TBD
Privacy	November 1999	December 2000	April 2003
National Health Plan Identifier	2001‡	TBD	TBD
Claims Attachments	2001‡	TBD	TBD
Enforcement	Late 2001‡	TBD	TBD
First Report of Injury	Late 2001‡	TBD	TBD
National Individual Identifier	Withdrawn§		

* Notice of Proposed Rule Making

† Small organizations (as defined by HHS) may have more time to comply. The Privacy Rule has been reopened for comment and the compliance date might subject to further delay.

‡ From Bill Braithwaite's (DHHS) presentation to HIPAA Summit West, June 2001 conference.

§ According to the DHS semiannual Regulatory Agenda published in the Federal Register on November 30, 2000.

Appendix C: HIPAA Resources on the Internet

There are numerous Web sites providing useful background and update information on HIPAA Compliance. The following listing is intended as a starting point and not an exhaustive list.

Web Site	What's There
U.S. Department of Health and Human Services http://aspe.hhs.gov/admnsimp/Index.htm	The proposed Administrative Simplification provisions of HIPAA; milestones and updates
Washington Publishing Company http://www.hipaa.wpc-edi.com	Transaction standards, implementation guides and data dictionary
National Council for Prescription Drug Programs http://www.ncpdp.org	Information on the pharmacy industry and HIPAA including the retail drug claim standard
Data Interchange Standards Association http://www.disa.org	Information on ASC X12 control standards, and X12N standards for electronic data interchange, task groups, and workgroups, including their meeting minutes.
Electronic Healthcare Network Accrediting Commission http://www.ehnac.org/Accreditation/Overview.html	EHNAC is an independent, not-for-profit accrediting body. Its Web site provides information on how organizations can receive HIPAA security accreditation
IBM Corporation http://houns54.clearlake.ibm.com/solutions/healthcare	White Papers on Security and Transaction standards, "Getting Ready for HIPAA" guide and link to IBM publication 2000 Guideline to Health Data Security
Joint Healthcare Information Technology Alliance http://www.jhita.org	Updates on legislation/regulation, telecommunications, and business process re-engineering.
American Hospital Association http://www.aha.org/hipaa	Updates, tools and resources, and links to additional resources. Information on representation/advocacy.

Appendix C: HIPAA Resources on the Internet (cont'd)

Web Site	What's There
Association for Electronic Healthcare Transactions (AFEHCT) http://www.afehct.org/administrative simplification.asp	Background, analysis, information on workgroups.
Health Privacy Project http://www.healthprivacy.org	Current information regarding HIPAA and privacy legislation, fact sheets, testimony.
Massachusetts Health Data Consortium http://mahealthdata.org	Summaries of NPRMs, compliance checklist, legislative background, HIPAA acronyms, and events
California Department of Health Services Medi-Cal www.medi-cal.ca.gov	HIPAA updates including background paper and links to additional resources
HIPAAdvisory by Phoenix Health Systems www.hipaadvisory.com	Good source of information, tools, updates, glossary of terms, and links
Workgroup for Electronic Data Interchange, Strategic National Implementation Process http://snip.wedi.org	Good source for basic information, best practices, conferences and other resources
Accredited Standards Committee X12 www.x12.org	Information on electronic data interchange (EDI) standards
HCFA HIPAA page www.hcfa.gov/hipaa/hipaahm.htm	Good information on HIPAA as it relates to Medicare and Medicaid
California Health and Human Services Agency www.training.cahwnet.gov/HIPAA/default.asp	Schedule and course descriptions for state-sponsored HIPAA courses from HHSDC Training Center

Appendix D: Compliance Questions for Outside Vendors

General

A given application or hardware item might support the performance of one or more of the many HIPAA obligations, but software and hardware are not inherently "HIPAA compliant" in and of themselves. HIPAA compliance is an organizational obligation, not a technical specification.

If your organization contracts with an Application Service Provider (ASP) that owns and operates the applications and host hardware which your organization uses to manage protected health information, that ASP assumes the organization's HIPAA obligations as well.[5]

There are a number of general questions which a provider should ask each vendor who has access to patient information, and/or transmits such data electronically:

1. Who, if anyone, is responsible for your HIPAA compliance efforts? Is this person dedicated to HIPAA compliance efforts or do they have other duties?

2. Has the organization initiated or established a HIPAA compliance planning effort? If so, may we see a copy of the plan? By what date will you be fully compliant?

3. Will your organization abide by specific HIPAA compliance policies and procedures developed by us that are not included in your plan?

4. Do you use or plan to use a subcontractor who would have access to individually identifiable health information? If yes, have you confirmed that they are HIPAA compliant? Will your subcontractors abide by specific HIPAA compliance policies and procedures developed by us that are not included in their plan?

[5] However, if your organization owns and operates hardware and software and does not rely on a vendor to manage protected information, HIPAA compliance obligations cannot be transferred the hardware or software vendor(s).

Appendix D: Compliance Questions for Outside Vendors (cont'd)

Transaction Standards and Code Sets

Providers must ensure that all applicable vendors involved with electronic data transmission and use of code sets have a HIPAA implementation plan. Examples of such vendors include:

- Billing services
- Collection agencies
- Information system hardware and software support consultants
- ASPs or providers of information systems located remotely but hosting data of the practice and its patients
- Virtual Private Network (VPN) that can extend a private network (such as a hospital's) in a secured manner over a public network to include referring physicians

As part of a provider's HIPAA compliance implementation process, the following questions should be asked of each external vendor identified above:

1. Have you conducted a thorough evaluation of the data elements for the standard transactions? What changes will we need to make with respect to collection and entry of information? What training will you offer and when will you begin?

2. Do you currently support HIPAA standard transactions today? If yes, which transactions do you currently support? For those you do not currently support, what is your timeframe for becoming compliant?

3. Do you have the standard Code Lists available electronically? Can you upload them to our system automatically? If yes, when do you plan to do this?

Appendix D: Compliance Questions for Outside Vendors (cont'd)

Security Procedures

Providers must ensure that all vendors involved with electronic data storage and transmission have a HIPAA-compliant security plan. As part of a provider's HIPAA security planning process, the following questions should be asked of each external vendor:

1. Does your system identify and authenticate individual users? If so, what mechanism does it use to identify and authenticate users (for example, password, token card plus password or PIN, fingerprint)? How are remote users identified?

2. What access control provisions does your system and organization support? Does it allow for application-, role-, user-ID or some combination of these to define access by individual? Are there access control overrides for emergencies?

3. How does your system allow my organization to monitor access of individually identifiable health information (IIHI)? What type of audit trail does your system create? What types of routine management reports (including all access and exceptions) can be generated?

4. What is your organization's physical security and disaster recovery plan? How are printouts, storage media, and computers destroyed? How often is the disaster recovery plan tested? What is the plan for emergency data access in case of a disaster?

5. What provisions have been established to protect data accessed remotely, as well as ensure the integrity of data updated remotely? What are the Internet security provisions? Is encryption used for data exchange? Are authentication procedures required for Internet users? Is there periodic verification and maintenance of security measures?

6. What routine system assessments are performed to evaluate the system's vulnerability?

Appendix D: Compliance Questions for Outside Vendors (cont'd)

Privacy Regulations: Business Associate/Vendor Relationships

HIPAA protects the privacy of IIHI by regulating those organizations that create and disclose protected health information. Due to the complexity of the health delivery system, a myriad of individuals and organizations must have access to IIHI in the normal course of business. One outcome of this data sharing is to place the information HIPAA intends to protect into the hands of individuals and organizations over which the law has no immediate authority.

HIPAA resolves this gap in protection by extending the effect of the regulations to "business associates." HIPAA defines a business associate as any organization that performs services to or for your organization where the provision of the service involves the disclosure of IIHI. In short, a business associate is any third party vendor to your organization with whom IIHI is shared.

Examples of typical business associates for a physician practice might include:

- Billing services
- Collection agencies
- Temporary personnel agencies
- Information system hardware and software support consultants
- ASPs or providers of information systems located remotely but hosting data of the practice and its patients
- VPNs
- Maintenance companies capable of remote servicing of clinical equipment

Appendix D: Compliance Questions for Outside Vendors (cont'd)

Privacy Regulations: Business Associate Contracts

For each outside vendor that has access to IIHI, business associate contracts will need to be established to extend applicable HIPAA regulations to the vendor.

To ensure that your organization's vendor relationships are HIPAA compliant, first list all the business associates with whom IIHI is exchanged. All contracts should be reviewed for the requirements listed below. Does each contract:

- Prohibit the use or disclosure of patient data except as permitted by the contract or required by law?
- Establish the permitted and required uses and disclosure of patient data?
- Require the business associate to use appropriate safeguards to prevent and report unauthorized use or disclosure of patient data?
- Ensure that the restrictions and conditions apply to the agents and subcontractors of the business associate?
- Authorize your organization to terminate the contract if the business associate has violated a material term of the contract?

If the answer to any of these questions is no, all missing HIPAA provisions must be included as an amendment to your current vendor contracts.

Appendix E: Sample Security Policies and Procedures

<<Organization Name>>
Policies and Procedures for Data Security: Security Training

Subject: Security Training—<<Organization Name>> Employees and Third Party Vendors	
Date:	
Approval:	**Date:**

POLICY/PURPOSE:

To ensure the ongoing confidentiality of our patients' medical records and/or health information specific to individuals, <<Organization Name>> will provide data security training for all employees and third party vendors who have access to health information specific to a patient "medical records." (Only those third party vendor employees who have access to patients' medical records and/or health information specific to an individual will be required to attend the data security training sessions for <<Organization Name>>.) The reviewer(s) have final discretion regarding the access privileges afforded each position. This training will be mandatory for all new employees and third party vendors.

PROCEDURE:

1. **New Employees/Third Party Vendor Employees Training**

   All new employees and third party vendor employees will be required to attend a data security training session before being allowed access to patient medical records. At the end of the data security training session, each employee will sign an acknowledgment form indicating that they have reviewed, understand, and will comply with <<Organization Name>>'s data security policies and procedures.

   The Security Officer will maintain a record of the attendees at each training session. The immediate supervisor for each new employee must have written acknowledgement from the Security Officer that the new employee has successfully completed data security training prior to granting access to patient medical records.

2. **Annual Update Training Sessions**

   An annual data security training update session will be mandatory for all <<Organization Name>> and vendor employees to review the data security policies/procedures of the

Appendix E: Sample Security Policies and Procedures (cont'd)

office. Each employee will be required to sign an acknowledgment form indicating that they have reviewed, understand, and will comply with <<Organization Name>>'s data security policies and procedures.

The Security Officer for <<Organization Name>> will maintain a record of the attendees at each annual data security update training session. Should employees be unable to attend the session, the Security Officer will review the materials from the session with each such employee within four weeks of the training session.

3. Interim Data Security Training

If change(s) occur in <<Organization Name>>'s data security policies/procedures before the annual update session, interim training materials will be provided to all <<Organization Name>> and vendor employees for review. A signed acknowledgement form stating that they have reviewed, understand, and will comply with the change in data security policies or procedures will be required.

PRIMARY RESPONSIBILITY:

Security Officer

Appendix E: Sample Security Policies and Procedures (cont'd)

<<Organization Name>>
Policies and Procedures for Data Security: User Access

Subject: User Access Privileges Definition—<<Organization Name>> Employees and Third Party Vendors	
Date:	
Approval:	**Date:**

POLICY/PURPOSE:

To establish access privileges at different levels based on the role of the user, their specified relationship with patients and needs for access to patients' medical records and/or health information.

PROCEDURE:

1. Access Definition

Each Medical Office and vendor job description/position will have preliminary patient data access requirements defined by the position's immediate supervisor and Security Officer. These preliminary definitions will be reviewed and approved by the <<Office Administrator, Practice Manager, Management Committee>>; the reviewer(s) have final discretion regarding the access privileges afforded each position. Access privilege definitions shall include:

- Paper records such as patient office and procedure schedules, patient medical records, diagnostic testing reports, insurance documentation, provider invoices, remittance advice, and all other paper records reflecting patient-specific information.
- Electronic records such as patient medical records, diagnostic testing reports, insurance documentation, provider invoices, remittance advice, electronic mail (e-mail) transmissions between the Medical Office and patients, e-mail transmissions between <<Organization Name>> and any third party vendor and all other electronic transmission sent from or received by <<Organization Name>>.

Access privileges shall be restricted to only those data necessary for the employee(s) in each position to successfully perform their job duties. Practitioners and contracted business partners will be held to the above standards for assigning access privileges.

Appendix E: Sample Security Policies and Procedures (cont'd)

The Security Officer for <<Organization Name>> will maintain a record of the access privileges by position.

2. Changes in Access Privileges

Access privileges will be reviewed and revised on a periodic basis or as needed to implement changes in limitations to data access, strengthen protections against unauthorized access or other reasons as indicated below:

- Changes in job duties associated with a position
- Disciplinary actions
- Layoffs/terminations
- Termination of contract with third party vendor

It is the responsibility of the immediate supervisor to notify the Security Officer of any necessary change in access privileges. The supervisor and Security Officer will coordinate changes in access privileges for electronic data with the manager of information systems. The supervisor and Security Officer will coordinate changes in access privileges to paper records with the <<Organization Name Manager/Administrator>>.

Any change in access privileges will be recorded and maintained by the Security Officer.

PRIMARY RESPONSIBILITY:

Security Officer

Appendix F: Checklist for Current Security Compliance

Question	Response	Comments/Issues
Policies and Procedures		
Do you have policies and procedures that establish rules for granting or restricting access to a user, PC or computer terminal, transaction, program, or process?	❑ Yes ❑ No	
If yes, do your policies and procedures address individuals working with data as well as those who might have access to data (for example, maintenance staff)?	❑ Yes ❑ No	
Do you have security policies and procedures that determine an individual/entity's initial right of access to a computer terminal/PC, transaction, program, and process?	❑ Yes ❑ No	
Do you have policies and procedures that establish differing levels of access to an individual/entity based upon their job description?	❑ Yes ❑ No	
Do you have policies and procedures that set forth when and why an individual's/entity's right of access to a computer, transaction, program or process would be changed?	❑ Yes ❑ No	
Authorization Control—Do you have policies and procedures to obtain patient consent for the use and disclosure of health information?	❑ Yes ❑ No	
Data Backup—Do you have policies and procedures to document your organization's backup plan, including frequency of backup procedures, duration of retaining backup copies, and location of backup copies?	❑ Yes ❑ No	

Appendix F: Checklist for Current Security Compliance (cont'd)

Question	Response	Comments/Issues
Equipment Control—Does your organization have documented security procedures for marking, handling and disposing of hardware and storage media?	❑ Yes ❑ No	
Formal Mechanism for Processing Records—Does your organization have documented policies and procedures for routine and non-routine receipt, manipulation, storage, dissemination, transmission, and/or disposal of health information?	❑ Yes ❑ No	
Hardware/Software Installation and Maintenance—Do you have policies and procedures documenting how new equipment and/or software will be tested and maintained to ensure security attributes are in place?	❑ Yes ❑ No	
Internal Audit—Are there policies and procedures delineating the frequency of internal audits of your systems to assess system activity and actual or potential security incidents?	❑ Yes ❑ No	
Maintenance of Record Access Authorization—Are there policies and procedures in place documenting access privileges to health information?	❑ Yes ❑ No	
Personnel Security—Does your organization have policies and procedures documenting that all personnel with access to sensitive data have the required authority as well as appropriate clearances?	❑ Yes ❑ No	

Appendix F: Checklist for Current Security Compliance (cont'd)

Question	Response	Comments/Issues
Do employees and contractors sign agreements that delineate individual security responsibilities and accountability for maintaining confidentiality? Are these agreements updated periodically?	❑ Yes, and agreements updated at least annually ❑ Yes, but agreements not updated regularly ❑ No	
Work Station Use—Are there documented policies and procedures delineating functions, use, and physical security of work stations depending upon the sensitivity of data accessed and/or stored at that site?	❑ Yes ❑ No	
Security Incident Report and Response—Does your organization have policies and procedures documenting the mechanisms to document security breach incidents, as well as actions to be taken in response to any security incidents?	❑ Yes ❑ No	
Sanction Policy—Does your organization have policies and procedures governing disciplinary actions, civil or criminal penalties in the event of misuse or misappropriation of health information, and for communicating such policies to all employees and vendors?	❑ Yes ❑ No	
Visitors—Is there a procedure governing the reception and hosting of visitors to control access to sensitive data?	❑ Yes ❑ No	
Termination—Do you have written policies and procedures that delineate the steps to be taken when an employee quits/is terminated, or when user access must be revoked for other purposes? Does the policy address: changing locks/combinations, removal from access lists, revoking user accounts that grant access to information, turning in of keys, etcetera?	❑ Yes, policy addresses all or most listed items ❑ Yes, policy addresses some listed items ❑ No	

Appendix F: Checklist for Current Security Compliance (cont'd)

Question	Response	Comments/Issues
Personnel Training		
Awareness Training—Have all staff and contractors participated in security awareness training including: password maintenance, incident reporting, and viruses?	❑ Yes ❑ No	
Periodic Security Reminders—Are employees, agents, and contractors reminded of security concerns on an ongoing basis?	❑ Yes ❑ No	
User Education—Does your organization have formal training sessions regarding accountability for security of health care information, the importance of virus protection, and rules to be followed in creating and changing passwords and the need to keep them confidential?	❑ Yes ❑ No	

Appendix G: Glossary

Administrative Simplification: HIPAA gives 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 required to protect the security and privacy of personally identifiable health care information.

American National Standards Institute (ANSI): An organization that accredits various standards-setting committees, and monitors their compliance. HIPAA prescribes that the *standards* mandated under it be developed by ANSI-accredited bodies whenever practical.

Application Service Provider (ASP): A vendor that deploys, hosts, and manages access to a packaged application to multiple parties from a centrally managed facility on a subscription basis. The applications are delivered over networks or via the Internet.

Business Associate (BA): A person or organization that performs a function or activity on behalf of a *covered entity*, but is not part of the *covered entity's workforce*. A *business associate* can also be a *covered entity* in its own right. Examples of business associates are:

- A *Third Party Administrator (TPA)* is a *business associate* that performs claims administration and related business functions for a self-insured entity.
- Under HIPAA, a *health care clearinghouse* is a *business associate* that translates data to or from a standard format on behalf of a *covered entity*.
- The HIPAA Security NPRM used the term *Chain of Trust Agreement* to describe the type of contract that would be needed to extend the responsibility to protect health care data across a series of sub-contractual relationships.

Chain of Trust: A term used in the HIPAA Security NPRM for a pattern of agreements that extend protection of health care data by requiring that each *covered entity* that shares health care data with another entity require that that entity provide protections comparable to those provided by the *covered entity*, and that that entity, in turn, require that any other entities with which it shares the data satisfy the same requirements.

Clearinghouse: Under HIPAA, this is an entity that processes or facilitates the processing of information received from another entity in a nonstandard format or containing nonstandard *data content* into standard *data elements* or a standard transaction, or that receives a standard transaction from another entity and processes or facilitates the processing of that information into nonstandard format or nonstandard *data content* for a receiving entity.

Appendix G: Glossary (cont'd)

Code Set: Under HIPAA, this is any set of codes used to define *data elements*, such as tables of terms, medical concepts, medical diagnostic codes, or medical procedure codes. This includes both the codes and their descriptions.

Electronic Data: Data that is recorded or transmitted in a manner that supports automated interpretations of its contents, while *non-electronic data* would be everything else. "Non-electronic" includes data transmitted by fax and audio systems, which is, in principle, transmitted electronically, but which lacks the underlying structure usually needed to support automated interpretation of its contents.

Electronic Data Interchange (EDI): This usually means X12 and similar variable-length formats for the electronic exchange of structured data. It is sometimes used more broadly to mean any electronic exchange of formatted data.

Individually identifiable health information (IIHI): Health information created or received by a health care provider, health plan, employer or health care clearinghouse, that could be used directly or indirectly to identify the individual who is the subject of the information.

Local Code(s): A generic term for code values that are defined for a state or other political subdivision, or for a specific payer.

Minimum Scope of Disclosure: The principle that, to the extent practical, individually identifiable health information should only be disclosed to the extent needed to support the purpose of the disclosure.

National Employer ID: A system for uniquely identifying all sponsors of health care benefits.

National Patient ID: A system for uniquely identifying all recipients of health care services. This is sometimes referred to as the National Individual Identifier (NII), or as the Healthcare ID.

National Payer ID: A system for uniquely identifying all organizations that pay for health care services. Also known as Health Plan ID, or Plan ID.

National Provider ID (NPI): A system for uniquely identifying all providers of health care services, supplies, and equipment.

Small Health Plan: Under HIPAA, this is a health plan with annual receipts of $5 million or less.

Appendix G: Glossary (cont'd)

Standard Transaction: A transaction that complies with the applicable HIPAA standard.

Virtual Private Network (VPN): A virtual private network allows two or more private networks to be connected over a publicly accessed network, like the Internet. VPNs have the same security and encryption features as a private network, while taking the advantage of economies of scale and remote accessibility of large public networks.

X12: An ANSI-accredited group that defines EDI standards for many American industries, including health care insurance. Most of the electronic transaction standards mandated or proposed under HIPAA are *X12 standard*s.

X12NX12 Standard: The term currently used for any *X12 standard* that has been approved since the most recent release of X12 *American National Standards*. Since a full set of X12 *American National Standards* is only released about once every five years, it is the *X12 standard*s that are most likely to be in active use.

HIPAA Administrative Simplification Tool Kit

Section Two:

Overview Presentation

HIPAA Administrative Simplification: Overview Presentation

November 2001

Prepared for the
California HealthCare Foundation
by the Pacific Health Policy Group

CALIFORNIA
HEALTHCARE
FOUNDATION

Overview

What is HIPAA?

- Health Insurance Portability and Accountability Act of 1996 (HIPAA), also known as the Kennedy/Kassebaum Act
- Primary purpose was to improve health insurance accessibility for people changing employers or leaving the workforce
- HIPAA also included "Administrative Simplification" provisions to encourage and protect the electronic transmission of health-related data

Overview

What are the HIPAA Administrative Simplification Provisions?

1. **National standards** for electronic data transmission
2. **Unique health identifiers** for providers, employers, plans, and individuals
3. **Security standards** to protect electronically maintained health information
4. **Privacy and confidentiality** provisions for individually identifiable health care data

Overview

What are the objectives of the Administrative Simplification Provisions?

- Improve efficiency of national health system
- Reduce administrative overhead costs
- Reduce fraud and abuse
- Protect patient rights, including the privacy of patient health data
- Improve quality of care through access to consistent clinical data
- Improve information available for decision-making
- Establish security standards for Internet-based technology

Overview

Why was legislation needed?

Technological advancements have resulted in substantial and increasing electronic transmission of health data, including:

- Rapid growth of health care Internet and intranet applications to transmit and share patient information, such as diagnoses, radiological images, lab tests, and prescriptions
- Advancements in the computerization of patient medical records
- Increasing use of electronic prior authorizations for provider services, as well as claims submission and payments
- Use of e-mail as a communication tool between caregivers and their patients

Overview

Why was legislation needed? (continued)

- Lack of standardization for the collection, storage, and transmission of health data → increased administrative costs AND decreased utility of data
- Increasing health care costs → demand for uniform health care data to evaluate alternative coverage and treatment approaches

Overview

Why was legislation needed? (continued)

Public concerns about privacy bring demands for greater security:

- 20% of consumers believe their health information has been used or disclosed inappropriately.
- 17% of Americans report that they have taken action to avoid the inappropriate use of their information, including providing inaccurate information to health care providers, changing physicians, or avoiding care altogether.
- The Association of American Physicians and Surgeons reports that 78% of its members have withheld information from a patient's record due to privacy concerns and 87% of its members have had a patient request that information be withheld.

Overview

Why was legislation needed? (continued)

"We have laws in this country to protect the personal information contained in bank, credit card, and other financial records. Our citizens must not wait any longer for protection of the most personal of all information—their health records.

"This rule makes sure that private health information doesn't fall victim to the progress of the information and technology age, where an array of data is readily available in computer systems and too often is just a keystroke away from being accessed."

Statement by Tommy G. Thompson
Secretary, U.S. Department of Health and Human Services
Approving the Patient Privacy Rule April 12, 2001

Overview

Who must comply with HIPAA?

1. **Health care providers** or any other person or organization that furnishes, bills, or is paid for health care in its normal course of business
2. **Health plans** that provide or pay the cost of medical care, including Medicare and Medicaid
3. **Health care clearinghouses** that process data elements or transactions

Provision 1: National Standards

Electronic Data Interchange standards have been adopted for:

- Health claims/encounter information
- Enrollment/disenrollment in a health plan
- Eligibility for a health plan
- Health care payment and remittance advice
- Health plan premium payments
- Health claim status
- Referral certification and authorization
- Coordination of benefits

Standards for claims attachments and first report of injury are required but have not yet been adopted.

Provision 1: National Standards

Electronic Data Interchange (continued)

- American National Standards Institute (ANSI) ASC X12N standards have been adopted for most transactions.
- For retail pharmacy, the National Council of Prescription Drug Programs (NCPDP) Telecommunications Standard Format Version 5.1 and equivalent NCPDP Batch Standard Version 1.0 both set the standards.

Provision 1: National Standards

Code Sets

Specific code sets have been adopted:

- ICD-9-CM, Volumes 1&2
- ICD-9-CM, Volume 3
- Combination of HCPCS and CPT-4
- HCPCS (other substances, equipment, supplies, other items)
- National Drug Codes
- CDT-2 (dental services)

NOTE: All local codes will be eliminated.

Provision 1: National Standards

What do they mean for providers?

- All electronic transactions must be converted to the standard format.
- DHHS cost estimates for non-hospital providers range from $0 (providers with no electronically processed patient claims or encounters) to $10,000 to cover software/system upgrades.
- Additional provider costs not calculated in these estimates could include:
  - Personnel training
  - Possible payment delays while billers and payers convert to the new standardized system

Provision 1: National Standards

What do they mean for providers? (continued)

- DHHS estimates savings per electronically processed claim at $1.49 for physicians and $0.83 for all others. Total savings for non-hospital providers are estimated to range from $0 to over $70,000 between 2002 and 2011.
- Additional potential administrative savings not calculated in these estimates could include:
  - Elimination of multiple transaction formats
  - Common data sets which will facilitate data sharing among entities
  - Possible cash flow increase if providers' ability to electronically bill and collect is substantially improved

Provision 2: Unique Health Identifiers

HIPAA requires unique national health identifiers for employers, providers, health plans, and individuals:

- **Employer Identifier:** expected to be the Employer Identification Number (issued by the Internal Revenue Service)
- **National Provider Identifier:** developed by HCFA for use in the Medicare system
- **Health Plan Identifier:** expected to be the HCFA Medicare PayerID assigned to all health plans nationwide
- **Individual Identifier:** development is on hold

Provision 2: Unique Health Identifiers

What do they mean for providers?

- If the National Provider Identifier (NPI) is selected, Medicare, Medicaid, and other federal health plan providers would be assigned an NPI automatically.
- Other providers would have to apply to a federally directed registry for an NPI.
- Providers will need to modify their billing and other systems to include the new standard Ids.

Provision 3: Security Standards

Security standards for all patient-specific information that is or has been electronically stored and/or transmitted can be grouped into four categories:

1. **Administrative procedure safeguards**—comprehensive security policies and procedures
2. **Physical safeguards**—data integrity, backup, access, workstation location and security training
3. **Technical security mechanisms**—security measures to guard against unauthorized access to data
4. **Technical security services**—measures to protect patient information and control individual access to such information

Provision 3: Security Standards

Security standards (continued):

- The standards establish a minimum threshold for compliance in each of the four categories.
- However, the security standards do not specify particular technology requirements—each organization must assess its own "risk" and develop security measures accordingly.
- Organizations must certify their security programs (either through a self-certification or by a private accreditation entity or vendor). The certification process has not yet been specifically defined.

Provision 3: Security Standards

What do they mean for providers?

- Procedures and systems must be updated to ensure that health care data is protected.
- Written security policies and procedures must be created and/or reviewed to ensure compliance.
- Employees must receive training on those policies and procedures.
- Access to data must be controlled through appropriate mechanisms (for example: passwords, automatic tracking of when patient data has been created, modified, or deleted).
- Security procedures/systems must be certified (self-certification is acceptable) to meet the minimum standards.

Provision 4: Privacy Regulations

Consent/Authorization Provisions

- Individually identifiable health information may not be used or disclosed unless authorized by the patient or is specifically permitted under HIPAA.
- Patient consent is required for the use or disclosure of information for three purposes: treatment, payment, and other health care operations.
- The privacy rule refers to both patient consent and authorization. In general, patient consent relates to information used for treatment-related purposes whereas patient authorization refers to disclosure of information for non-treatment purposes (such as employers, underwriters, or researchers).

Provision 4: Privacy Regulations

Other Key Provisions

- Use of health information for non-treatment purposes must be limited to the "minimum necessary."
- A written agreement must be in place that provides for appropriate safeguarding of health information with all "business associates." This standard does not apply when information is being shared for treatment purposes.
- Development of policies and procedures: Each entity must designate a privacy officer, develop privacy policies and procedures, and provide staff training to ensure that health information is protected.

Provision 4: Privacy Regulations

Patients' Rights Provisions

- Covered entities must provide a "notice of privacy practice" to each patient describing his/her rights regarding protected health information.
- Patients have the right to inspect and receive a copy of their medical records and to request amendments to their records. Though providers have the right to deny inclusion of an amendment, the patient has the right to file a Statement of Disagreement, which becomes part of the record. The provider can file a rebuttal to the Statement, should s/he so choose.
- Patients also have the right to receive an accounting of disclosures of protected information. Individuals may request restrictions on the use and disclosure of information that go beyond those provided in the rule, but providers are not required to comply with those requests.

Provision 4: Privacy Regulations

What do they mean for providers?

- Consent is required for disclosure of identifiable information for treatment, payment, or health care operations (for example: quality assessment and improvement activities, physician qualifications and competence evaluations, medical reviews, and audits).
- Health care providers may refuse treatment if they do not receive an individual's consent.
- Consent is not required for sharing a patient's medical records with another physician when referring the patient to that physician or when billing a patient referred for a specialty consultation.

Provision 4: Privacy Regulations

What do they mean for providers?

Privacy regulations will require authorization for disclosure of identifiable information in all cases when used for ancillary purposes such as:

- Research, such as clinical or market
- Employers or employer groups
- Pre-enrollment underwriting

Authorizations must be written in specific terms and must identify:

- The information to be disclosed
- Persons authorized to make the disclosure
- Persons authorized to receive the information
- "Expiration date" of authorization

Provision 4: Privacy Regulations

What do they mean for providers?

- If an individual refuses to give authorization, providers generally still must provide treatment.
- "National priority" activities are exempt from obtaining either consents or authorizations from individual patients. These include, public health emergencies, law enforcement, and judicial and administrative proceedings.

Preparing for HIPAA

First Steps

Identify project lead and establish HIPAA steering committee:

- Project lead should be someone from management with a broad operational background.
- HIPAA steering committee will need key managers from most, if not all, departments/units, as well as legal counsel.

Begin building awareness:

- Conduct briefings for executive management/department heads and clinical practice leadership.
- Schedule regular "HIPAA Update" sessions where project lead will provide current news (such as the adoption of final rules, key operational issues/challenges, etc.).

Commit resources needed to begin implementation.

Preparing for HIPAA

Next Steps: National Standards/Code Sets

- Identify the transactions you currently send/receive electronically.
- Identify the "trading partners" (organizations with whom your organization shares health information electronically, such as health plans and state medical programs) and vendors you use to prepare/submit such transactions.
- Contact your trading partners and vendors to determine their HIPAA compliance status.
- Compare existing data sets to those defined in the implementation guides for each transaction standard.
- Compare current code sets to HIPAA standards. Remember that local codes are not permitted under HIPAA.

Preparing for HIPAA

Next Steps: Security Standards

- **Gap Analysis.** Compare current security program to the HIPAA standard to identify gaps and develop action plans.
- **Risk Analysis.** Identify the likelihood and impact of adverse actions such as inappropriate disclosure, corruption, or loss of patient information.
- Based on the gap analysis and risk analysis, determine what additional security measures are appropriate and develop a plan for implementation.
- Proposed standards require a "risk assessment," which includes a cost/benefit analysis of security measures.

Preparing for HIPAA

Next Steps: Security Standards (continued)

A critical element of the security standards is the development of comprehensive policies and procedures that govern access to electronic health care information.

There are two broad categories of required policies and procedures:

1. Personnel – Use of patient information by individuals employed by your organization or third parties with authorized access (such as billing vendors)
2. Systems – System security and maintenance of patient data

Preparing for HIPAA

Next Steps: Privacy Regulations

- Appoint someone in your organization to review the existing policies and procedures against the new regulations to identify gaps.
- Conduct preliminary staff training. Even if your existing policies will not meet all HIPAA requirements, it is good practice to review privacy procedures to protect against inadvertent disclosures of information.
- Watch for Bush Administration implementation guidelines that may influence the regulations.