

Health Insurance Portability and Accountability Act

and

Administrative Simplification

Overview

Nebraska SNIP

The Nebraska SNIP Task Group has been established to meet the immediate need to assess HIPAA Administrative Simplification implementation readiness and to bring about the coordination necessary for successful compliance.

Table of Contents

Introduction	1
Background	1
Enforcement	2
Impact	3
Required Standards.....	3
Transactions and Codes Sets	4
Administrative Simplification Compliance Act	4
Privacy Standard.....	5
Individually Identifiable Information.....	7
Key Privacy Concerns	8
Information Security Standard.....	9
Unique Identifier Standard	9
Providers	9
Health Plans	9
Employer	10
Patient.....	10
Regulation Timetable and Status	10
Resources	12
Nebraska SNIP	12
HIPAA Web Sites	13
Implementation Strategies	14

Introduction

The Health Insurance Portability and Accountability Act (HIPAA) Administrative Simplification standards and resulting rules will have a significant impact on you and health care organizations. As required by Congress in HIPAA, the standards cover health plans, health care clearinghouses, and those health care providers who conduct certain financial and administrative transactions electronically. The HIPAA required health care standards are:

- transactions and code sets, (final rule published)
- privacy, (final rule published)
- security,
- and identifiers.

Compliance with HIPAA Standards for Electronic Transactions is required by October 16, 2002. The Administrative Simplification Compliance Act allows entities to request a one year extension to this date by submitting a request for approval along with a compliance plan. Compliance with HIPAA Standards for Privacy of Individually Identifiable Health Information is required by April 14, 2003. HIPAA's mandates will affect everyone in health care and the regulations apply to, among others:

- All health plans, including government programs, HMOs, indemnity insurers, and employer benefit plans.
- All health care providers, including any person or institution that furnishes health care services or supplies.
- All health care clearinghouses – those companies that are retained by plans, providers, and payers to help process health care business transactions.

Background

The Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191) was enacted as part of a broad Congressional attempt at incremental health care reform. Having its roots in health care reform proposals of the early 90's, the primary intent of HIPAA is to provide better access to health insurance, limit fraud and abuse, and reduce administrative costs.

The "Administrative Simplification" aspect is contained in Title II, Section F and was an addendum to several original insurance reform proposals. The Administrative Simplification aspect of HIPAA requires the United States Department of Health and Human Services (HHS) to develop standards and requirements for maintenance and transmission of health information that identifies individual patients. The required health care standards are; transactions and code sets; privacy; security; and identifiers.

These standards were designed to:

- Improve the efficiency and effectiveness of the health care system by standardizing the interchange of electronic data for specified administrative and financial transactions; and
- Protect the security and confidentiality of electronic health information.

The requirements outlined by the law and the final and proposed regulations promulgated by HHS are far-reaching. All health care organizations that maintain or transmit electronic health information must comply with transactions, code sets and privacy. All health care organizations must comply with security and identifiers (proposed rules). This includes health plans, health care clearinghouses, and health care providers, from large integrated delivery networks to individual providers.

In the August 17, 2000 Federal Register, Health and Human Services published regulations adopting standards for eight electronic health care transactions and code sets. The final regulations on transactions and codes sets are the first in a series of regulations. On December 27, 2002, President Bush signed the Administrative Simplification Compliance Act. This Act provides a one-year extension for compliance to the Transactions and Code Sets standard.

Health and Human Services (HHS) released proposed privacy regulations in 1998. Final privacy regulations were delayed because HHS received over 50,000 public comments on the proposed regulations. In the December 28, 2000 Federal Register, HHS published regulations adopting standards for privacy. Because of an administrative glitch, HHS delivered the appropriate paperwork to Congress on February 13, 2001 making the new effective date 60 days from that date, or April 14, 2001. On February 28, 2001, HHS opened the privacy standards for a new 30 day comments period, but did not delay the implementation. Compliance is required by April 14, 2003.

Enforcement

How will compliance with the new standards be evaluated? Currently, no federal agency has been tasked or funded to conduct compliance surveys of transactions, although this may change with future regulations. Initially, health care organizations will be expected to monitor their own compliance.

The Department of Health and Human Services' Office for Civil Rights (OCR) is responsible for enforcement of the privacy standards. A person who believes that a covered entity is not in compliance may file a complaint with the Secretary of Health and Human Services, who may investigate. HHS may also conduct compliance reviews.

In either case, HHS will notify the covered entity in writing of noncompliance and attempt to resolve the matter informally when possible. OCR has the authority to impose civil monetary penalties and may refer matters for criminal prosecution.

Surveyors from the Joint Commission on Accreditation of Health care Organizations (JCAHO) may look for hospital compliance during accreditation surveys, but they will not certify organizations as HIPAA-compliant. It is likely that Medicare validation surveyors may also evaluate HIPAA compliance during on-site surveys.

The law provides for significant financial and civil penalties for violations. In addition to these fines, the OIG may consider noncompliance prosecutable under the False Claims Act.

Failure to Comply with Transaction Standards:

- Each violation: \$100.
- Maximum penalty for all violations may not to exceed \$25,000 per year.

Wrongful Disclosure of Individually Identifiable Health Information:

- Wrongful disclosure offense: \$50,000, imprisonment of not more than one year, or both.
- Under false pretenses: \$100,000, imprisonment of not more than 5 years, or both.
- With intent to sell information: \$250,000, imprisonment of not more than 10 years, or both.

Impact

Unlike Y2K, HIPAA is an enterprise-wide and industry wide issue - not an information technology issue. There are legal, regulatory, process, security, and technology aspects to each rule that must be carefully evaluated before an organization can begin its implementation plan. HIPAA has become a major issue in health care because:

- Implementation timeframes are short - organizations must be in compliance 24 months after the regulations become final.
- Y2K efforts have kept organizations from focusing on HIPAA. Y2K also left some organizations with limited staff and financial resources available.
- Senior executives are clearly responsible for the security and confidentiality of patient health information, yet little has been done in most organizations to protect this information.
- There are significant criminal and civil penalties for non-compliance, as well as serious liability risks for unauthorized disclosure.
- There is no quick fix or easy solution to meet HIPAA requirements.
- Some degree of information technology retooling will be required, as well as major operational and procedural changes.
- Implementation of standards will be expensive. Ongoing costs will involve obtaining and implementing updates to the standards.
- Security and privacy regulations will be the most difficult to implement and maintain because they are broad in scope, less definitive, and require constant vigilance for ongoing compliance.

It is difficult to assess the costs and benefits of HIPAA because these are sweeping changes for which we have no historical experience. Estimated costs of implementation vary widely but will be in the billions of dollars. HHS estimated the regulation to have a 10 year cost of \$17.6 billion for the health care industry. An American Hospital Association commissioned study found that the cost of three key provisions of the privacy rule alone would cost \$22.5 billion over 5 years. Findings from a Tillinghast - Towers Perrin study estimates costs to a mid-sized hospital (200-300 beds) at \$775,000 to \$3.5 million. This study also estimates costs to individual physicians at approximately \$3,000 to \$5,000 and for a typical 50-physician practice, costs could range from \$75,000 to \$250,00. The good news is Moody's says compliance costs for non-profit hospitals will not have an impact on their bond ratings.

Required Standards

The required standards are health care transactions and code sets, privacy, security, and identifiers. A brief overview of the standards is outlined below, followed by practical implementation strategies for health care organizations.

Transactions and Code Sets Standard

In the August 17, 2000 Federal Register, Health and Human Services published final regulations adopting standards for eight electronic health care transactions and code sets. Final rules on transactions and code sets became law 60 days after they were published. Full implementation of all electronic standards and code sets must be by 24 months after 60 day period, or October 16, 2002. (October 16,2003 for small health plans.)

On December 27, 2002, President Bush signed the **Administrative Simplification Compliance Act** (H.R. 3323). This Act provides a one-year extension for compliance to the Transactions and Code Sets standard. Covered entities filing an extension request must comply with the transactions and code sets rule by October 16, 2003. To qualify for the deadline extension, entities must submit a compliance plan to HHS by October 16, 2002. The plan must include a budget, schedule, work plan, and implementation strategy for achieving compliance. The Centers for Medicare and Medicaid Services (CMS) has published a Model Compliance Plan and electronic filing services available at www.cms.gov/hipaa/hipaa2/ASCAForm.asp.

It is estimated that over 400 electronic data information ("EDI") formats are used by various payers. This lack of standardization creates inefficiency and inaccuracy. The new regulations are an effort to reduce paper work and increase efficiency through the use of standardized financial and administrative transactions and data elements for transactions. HIPAA will change this practice by requiring payers to accept the following transaction standards.

- Claims/encounters, eligibility, and related transactions covered in August 17, 2000 Final Rule
 - Claim and encounter information
 - Payment and remittance advice
 - Enrolling and disenrollment of an individual in a health plan
 - Health plan premiums
 - Eligibility for a health plan
 - Referral Certification and Authorization
 - Claim status
 - Coordination of benefits

Electronic Transactions Covered in Future Rule.

- Claim Attachment
- First Report of Injury

This includes the following electronic transaction standards defined by American National Standards Institute ANSI X12N subcommittee.

148 - First Report of Injury
 270 - Eligibility Request
 271 - Eligibility Response
 275 - Claim Attachment
 277 - Additional Information Response
 276 - Claim Status Request
 277 - Claim Status Response
 278 - Claim Review Request and Response
 820 - Premium Payment
 834 - Enrollment
 835 - Claim Payment
 837 - Claim or Encounter (Dental, Institutional, & Professional)
 Pharmacy transactions: National Council for Prescription Drug Programs (NCPDP)

Code Sets Covered in August 17, 2000 Final Rule.

- Diagnosis and inpatient hospital services: International Classification of Diseases, 9th edition, Clinical Modification (ICD-9-CM). The standard will migrate to ICD-10 in 2001 or 2002, whenever the new system is ready for adoption.
- Procedures: ICD-9-CM Volume III.
- HCFA Common Procedural Coding System (HCPCS). Level I contains CPT-4 codes maintained by AMA and Level II codes are maintained by CMS, Blue Cross and Blue Shield Association and Health Insurance Association of America.
- National Drug Code (NDC).
- Dental services: Current Dental Terminology (CDT).

Future updates to code sets will be handled through Designated Standard Maintenance Organization (DSMO's).

As expected, before the first implementation of transactions and codes set, there are modifications to the standards. In the May 31, 2002 Federal register, two sets of proposed rules were published. The first set of proposed rules adjusted the codes sets and called for the use of NDC codes only in retail pharmacy transactions. The second set of proposed modifications to the claim and encounter standards as originally published. The industry feels these modifications are necessary to make the 835 transactions workable.

In October of 2001, the X12N's Addenda for the HIPAA-adopted Implementation Guides were posted to the Washington Publishing Company (X12N's publisher) website (www.wpc-edi.com/hipaa). These Addenda are referenced in the HHS proposed rules regarding potential changes to the HIPAA Electronic Transactions regulation. With the proposed rule published, there are still a number of steps that must be completed before the changes can be considered final and required for implementation under an additional final HIPAA Electronic Transactions regulation. Completing these steps will likely take several more months!

Privacy Standard

With the 1996 passage of HIPAA, Congress was granted 36 months to pass privacy legislation. In the event Congress failed to meet this deadline, HIPAA authorized HHS to promulgate final regulations to protect patient privacy. HHS published a NPRM for individually identifiable health information on November 3, 1999.

After reviewing more than 50,000 comments, HHS published the final regulations on December 28, 2000. Congress had not received official notice of the new regulations when they were published in the Federal Register because of an administrative glitch. HHS delivered the appropriate paperwork to Congress on February 13, 2001 making the new effective date 60 days from that date, or April 14, 2001. Compliance is required by April 14, 2003.

In the February 28, 2001 Federal Register, a notice was published that Secretary of Health and Human Services Tommy Thompson, reopening the HIPAA privacy act regulations for a new 30 day comment period. On April 12, 2001, after receiving over 24,000 additional comments, Tommy Thompson announced that President Bush would not delay the effective date for the HIPAA Privacy Regulations. This announcement also indicated that HHS would look at issuing guidance and additional rule making as needed.

On July 6, 2001, the Office of Civil Rights (OCR) issued the first in a planned series of guidance on specific requirements for the privacy standards. These guidance included information on:

- Frequently Asked Questions
- Consent
- Minimum Necessary
- Oral Communications
- Business Associates
- Parents And Minors
- Health-Related Communications and Marketing
- Research
- Restrictions On Government Access To Health Information
- Payment

As adapted, the privacy standards outline specific rights for individuals regarding protected health information and obligations of health care providers, health plans, and health care clearinghouses. Some of the key components of the privacy standard are:

- Individually Identifiable Information - information or data that may identify an individual receiving health care services.
- Protected Health Information (PHI) - record set containing individually identifiable information.
- Covered Entity - entity providing health care services and holder of PHI.
- Business Associate - entity using PHI on behalf of covered entity.
- Patient Access - right of patient to copy, amend and request accounting of PHI.
- Minimum Necessary - only necessary information is released to accomplish purpose.
- Consent - patient consent to use PHI for treatment, payment or health care operations.
- Authorization - patient authorization to use PHI for specified purposes.
- Notice of Privacy Practice - an entity's stated policies and procedures related to PHI.
- Privacy Officer - individual assigned by covered entity to oversee privacy practices.
- Complaint Process - method for individual to contact covered entity with complaint or request.

On August 14, 2002 HHS published modifications to Standards for Privacy of Individually Identifiable Health Information. The modifications affect:

- Consent and Notice
- Minimum Necessary and Oral Communications
- Marketing
- Business Associates
- Parents and Minors
- Uses and Disclosures for Research Purposes
- Uses and Disclosure for which Authorizations are Required
- Other sections of the Privacy Rule

The privacy regulations grant health care consumers a greater level of control over the use and disclosure of personally identifiable health information. In general, health care providers, health plans, and clearinghouses are prohibited from using or disclosing health information except as authorized by the patient or specifically permitted by the regulation. The privacy regulation's applicability is expanded to include all personally identifiable health information, irrespective of media form. There is no longer an exclusion for written medical records never transferred to electronic form or oral communications. The regulations are applicable to all health information held or created by the covered entity.

Health plans and health care providers must inform their patients/beneficiaries of their business practices concerning the use and disclosure of health information. Direct health care providers (Covered Entities) must obtain written consent from a patient for use and disclosure of health information, even if the use or disclosure is related to such routine purposes as treatment, payment or health care operations. A separate, specific authorization is required for non-routine disclosures.

As a component of the consent process, patients are granted the opportunity to request restrictions on the use and disclosure of their health information. Within 60 days of a request, patients are entitled to a disclosure history identifying all entities that received health information unrelated to treatment, payment or health care operations. Patients also have a right to review and copy their own medical records and have the corresponding right to request amendments or corrections to errors within the record.

Health care providers and health plans are required to create privacy-conscious business practices, which include the requirement that only the minimum amount of health information necessary to satisfy the request is disclosed. In addition, business practices should ensure the internal protection of medical records, employee privacy training and education, creation of mechanism for addressing patient privacy complaints, and designation of a privacy officer. Overall, covered entities are encouraged to use de-identified information whenever possible. Once information is in a de-identified form, it is no longer subject to the privacy regulation restrictions.

Protected Health Information is a record that contains individually identifiable information. Information relating to individual patients is de-identified if the following identifiers of the individual or of relatives, employers, or household members of the individual, are removed:

- Names;
- All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census:
 - a. The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and
 - b. The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.
- All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;
- Telephone numbers;
- Fax numbers;
- Electronic mail addresses;
- Social security numbers;
- Medical record numbers;
- Health plan beneficiary numbers;
- Account numbers;
- Certificate/license numbers;

- Vehicle identifiers and serial numbers, including license plate numbers;
- Device identifiers and serial numbers;
- Web Universal Resource Locators (URLs);
- Internet Protocol address numbers;
- Biometric identifiers, including finger and voice prints;
- Full face photographic images and any comparable images;
- Any other unique identifying number, characteristic, or code;
- And the covered entity does not have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information.

Key Privacy Concerns:

With the rule's definitions, standards, and specifications for implementation and documentation, several key concerns emerge:

- Notices of privacy practices must be adopted and provided by covered entities.
- Authorization is needed for use or disclosure of protected information for purposes other than treatment, payment, or health care operations and for use or disclosure of psychotherapy notes. Combining an authorization form with another document is prohibited.
- Only the "minimum necessary" information may be released to accomplish the intended purpose of the use, disclosure, or request for protected health information, except under certain limited circumstances. The "minimum necessary" standard does not apply to disclosures made by providers to other providers for treatment purposes.
- Business associate agreements are required when covered entities disclose protected health information to an organization or person who uses the information to perform a function, activity, or service on its behalf.
- Individual rights include the right to receive a covered entity's notice of privacy practices; and the right to give, withhold, or revoke authorization for uses and disclosures for purposes other than medical treatment, payment, or health care operations and for uses and disclosures of psychotherapy notes.
- A privacy official, who will have responsibility for developing and implementing privacy policies and procedures, as well as ensuring general compliance, must be designated.
- Contact point that will receive complaints and provide further information about the entity's notice of privacy practices must be identified.
- Organizations covered by HIPAA must allow individuals access to their health information. Individuals also have the right to request amendments or corrections to their health information.

Information Security Standard

Despite years of work by standards development organizations (SDO's), there is no recognized single standard for the security of health information that includes all of the components required by HIPAA. So, HHS developed a security standard with input from SDO's and business interests. Published on August 12, 1998, this proposed standard is technology neutral and scaleable for the size and complexity of health care organizations.

At a minimum, all health plans, clearinghouses, and health care providers that transmit or maintain electronic health information must conduct a risk assessment and develop a security plan to protect this information. They must also document these measures, keep them current, and train their employees on appropriate security procedures.

The proposed security standard is divided into four categories:

- Administrative procedures used to guard data integrity, confidentiality, and availability. These are documented, formal procedures for selecting and executing information security measures. These procedures also address staff responsibilities for protecting data.
- Physical safeguards to guard data integrity, confidentiality, and availability. These safeguards protect physical computer systems and related buildings and equipment from fire and other environmental hazards, as well as intrusion. The use of locks, keys, and administrative measures used to control access to computer systems and facilities are also included.
- Technical data security services to guard data integrity, confidentiality, and availability. These include the processes used to protect, control, and monitor information access.
- Technical security mechanisms. These include processes used to prevent unauthorized access to data transmitted over a communications network.

Unique Identifier Standard

HIPAA mandates the use of unique identifiers for providers, health plans, employers, and individuals receiving health care services (patients). Transaction Standards will be implemented before identifiers are defined.

Providers:

The unique identifier for providers is the National Provider Identifier (NPI), which was developed by CMS for use in the Medicare system. The final provider identifier standard is not expected to change from the proposed rule. It will probably have 10 numeric positions with a check digit as the tenth digit. Implementation of this standard will require HHS to establish a system to assign the identifiers.

Health Plans:

The health plan identifier has been drafted to apply the work that CMS did for a Medicare Payer ID to all health plans nationwide. It is expected to have 10 numeric positions with a check digit in the tenth position.

Employer:

Final regulations on the Standard Unique Employer Identifier were published in the May 31, 2002 federal register. The employer identifier is based on the de facto standard, the Internal Revenue Service assigned Employer Identification Number (EIN).

Patient:

The patient identifier is the most controversial of the proposed identifiers. It is on hold pending comments. However, industry experts speculate that the identifier will consist of approximately ten numeric digits with a check digit. With concerns on privacy, a unique patient identifier may never be established.

For more information, you can review the proposed regulations in their entirety as published in the following Federal Registers:

- National Provider Identifier: May 7, 1998
- National Employer Identifier: June 16, 1998

Regulation Timetable and Status

HIPAA standards and resulting regulations are large and complex. There are not only a number of standards that must be monitored, they each have their own timetable and iterations. The table below provides a brief overview of each standard, major developments and their current status. Information is continually changing and being update. The best method to stay informed is monitoring the web sites included in the resources discussion.

HIPAA Administrative Simplification Regulations and Status

Standard	Description	Status
Standards For Electronic Transactions and Code Sets		
Electronic Transactions and Code Sets	The final rule adopted the initial standards for transactions and code sets.	Published 8/17/2000. Compliance date of 10/16/2002, or 10/16/2003 if compliance extension plan submitted per ASCA.
Claims Attachments	Proposal to adopt a standard for claims attachments, which frequently accompany health care standard transactions.	Estimated publication in fall/winter of 2002.
Revisions to NDC Standard	This proposed rule retracts the NDC code as the standard for drugs in all transactions except retail pharmacies. This proposed rule adopts a newer version of the standard for retail pharmacy claims, and adopts a revised standard for pharmacy remittance advice and prior authorization.	Proposed rule published 05/31/2002.
Transaction for First Report of Injury	This transaction was named in the rule, but no consensus on standard has been reached.	Proposed rule will be developed at the time standard is agreed upon.

HIPAA Administrative Simplification Regulations and Status

Standard	Description	Status
Revisions to Transactions and Code Set Standards	This proposed rule adopts modifications recommended by the DSMO.	Proposed rule published 05/31/2002.
Administrative Simplification Compliance Act (ASCA)	Provides one-year extension for compliance to the Transactions and Code Sets standard. Covered entities must submit a compliance plan by October 16, 2002.	Signed on December 27, 2001. Model compliance plan posted at www.cms.gov/hipaa/hipaa2/ in April of 2002.
Standards for Privacy of Individually Identifiable Health		
Privacy of Individually Identifiable Health Information	The final rule adopted standards for the privacy of personal health information.	Published 12/28/2000 with compliance date of 4/14/2003.
Privacy Guidance	OCR provided answers to general questions for the Privacy Rule.	Issued 7/6/2001.
Modifications to Standards for Privacy of Individually Identifiable Health Information	Modifications affecting Privacy rule.	Adopted August 14, 2002
Information Security Standard		
Security Standards	Standards for the security of health information.	Final NPRM under review with estimated publication in fall/winter of 2002
Standard for Electronic Signature	An electronic signature standard was proposed in the Security NPRM. Comments indicated lack of consensus.	Industry continues to work on this issue and. NCVHS is monitoring progress. Regulation will not be developed until NCVHS has made a recommendation.
Unique Identifier Standard		
Unique Identifier for Employers	This rule adopts the IRS Employer Identification Number (EIN) as the standard identifier for employers in standard transactions.	Final rule published on 05/31/2002.
Unique Health Care Provider Identifier	This rule adopts the NPI as the standard identifier.	Estimated publication in fall of 2002.
Unique Health Plan Identifier	This rule proposes the standard health plan identifier.	Estimated publication in fall of 2002.
Identifier for Individual	Work on this identifier was halted due to privacy concerns.	Appropriations language prohibits CMS from expending funds.

Resources

There are many resources and implementation assistance available in the form of documents and guidelines. In addition to resources in your organization, there are consulting services available, and a collaborative effort of health care organizations. A regional effort, the Nebraska Strategic National Implementation Process (NE SNIP) was formed as a collaborative effort to understand the complex regulations and to develop a plan on implementing the requirements. HIPAA compliance information is available at a number of web sites

Nebraska SNIP (www.NESNIP.org)

Nebraska organizations have been working to understand these very complex regulations and planning how to implement the requirements at minimum cost. There is a national task group, the Workgroup for Electronic Data Interchange (WEDI), and a collaborative national implementation effort, the Strategic National Implementation Process (SNIP), organized to assist the health care industry. Nebraska SNIP was formed as a collaborative healthcare industry-wide process that will result in the implementation of HIPAA standards and furthering the development and implementation of future standards.

Nebraska SNIP Task Group Purpose:

- Promote general healthcare industry readiness to implement the HIPAA standards.
- Identify education and general awareness opportunities for the healthcare industry to utilize.
- Recommend an implementation time frame for each component of HIPAA for each stakeholder (Health Plan, Provider, Clearinghouse, Vendor) and identify the best migration paths for trading partners.
- Establish opportunities for collaboration, compile industry input, and document the industry "best practices".
- Identify resolution or next steps where there are interpretation issues or ambiguities within HIPAA Administrative Simplification standards and rules.
- Serve as a resource for the healthcare industry when resolving issues arising from HIPAA implementation.

Nebraska SNIP hosts informational, education and demonstration meetings at various locations in Nebraska. These meetings are generally held each quarter and open to all individuals interested in HIPAA compliance and SNIP activities.

In addition to general oversight, Nebraska SNIP is also coordinating the efforts of four Work Groups involved with HIPAA. Additional information is available at www.nesnip.org on the Work Groups.

- Transactions and Code Sets;
- Privacy;
- Security;
- And Education and Awareness.

In addition to the Work Groups, Nebraska SNIP has formed a Small Provider Interest Group. This group is for providers with limited resources and simpler operations to assist in complying with HIPAA requirements.

HIPAA Web sites

Information on HIPAA Administrative Simplification is available on a number of web sites. The following list is not inclusive, but a good starting point.

www.nesnip.org/	Nebraska Strategic National Implementation Process
www.wedi.org/	WEDI HIPAA and SNIP information
aspe.hhs.gov/admsimp/	HHS Administrative Simplification information Includes regulations, Facts sheets and FAQ's
aspe.hhs.gov/admsimp/pl104191.htm	HIPAA Law
www.nesnip.org	Nebraska Strategic National Implementation Process
www.nhanet.org/hipaa.htm	Nebraska Hospital Association
www.cms.gov/medlearn/hipaa.asp	Medicare Learning Network
www.hhs.gov/ocr/hipaa	HHS Office of Civil Rights
www.disa.org	Data Interchange Standards Association
www.hipaa-dsmo.org	Designated Standard Maintenance Organization (DSMO)
www.ehnac.org	Electronic Healthcare Network Accreditation Commission
www.ncvhs.hhs.gov	National Committee on Vital and Health Statistics
www.wpc-edi.com	HIPAA Implementation Guides published by Washington Publishing Company
www.hipaacomply.com	HIPAA Comply - security and privacy compliance
www.healthprivacy.org	Health Privacy Project.
www.ahima.org/hot.topics/hipaa.html	American Health Information Management Association HIPAA information and model documents.
www.cdc.gov/nchs/otheract/phdsc/phdsc.htm	National Center for Health Statistics Public Health Data Standards Consortium.
pweb.netcom.com/~ottx4/HIPAA.htm	HIPAA Links directory
www.x12.org/	American National Standards Institute (ANSI) X12 Committee.
www.hipaadvisory.com	HIPAA Advisory by Phoenix Health Systems

Implementation Strategies

Even though some HIPAA standards are still being finalized, health care organizations should move to develop and implement compliance plans.

- Obtain copies of and read the rules from the Department of Health and Human Services' comprehensive HIPAA website. (Go to <http://aspe.os.dhhs.gov/admnsimp/>)
- As you read the rules, identify gaps between your current practices and rules.
- Sign up for e-mail notification of publication of documents related to HIPAA standards to keep current on the latest developments.
- Identify key individuals in your organization to spearhead compliance efforts. Be sure to include senior management to assure your efforts have the top-down support you need.
- Generate awareness in your organization. Educate your board, staff, physicians, and other key constituents about HIPAA.
- Make a comprehensive inventory of the individually identifiable electronic health information your organization maintains. Be sure to include information kept on personal computers, PDA's, other electronic devices and in research databases.
- Conduct a risk assessment to evaluate potential risks and vulnerabilities to individually identifiable electronic health information. Include the possibility of outside attacks if your systems have Internet access or dial-up access. Develop a tactical plan to address the identified risks, placing highest priority on the areas of greatest vulnerability.
- Collect existing information security policies and organize them into the four categories outlined in the security standards. Evaluate them to see if they're current, consistent, and provide adequate protections. Develop a checklist to identify policies you need still to develop and assign responsibility to appropriate individuals to draft those policies.
- Educate your staff about your security policies and enforce them. Establish a confidential reporting system, so employees can report security breaches without fear of repercussions. Impose sanctions for violations, and be prepared to deal with system disruptions or data corruption that may result from security violations.
- Assess the accuracy of your master patient index (MPI) to see how many duplicates (patients assigned more than one number) and overlays (more than one patient assigned the same number) you currently have.
- Evaluate your current billing system to see if you are using the standards outlined in the EDI transaction standard. If you're using the designated standards, have they been modified to meet specific payer requirements? If so, you'll need a plan for changing your system back to the approved standard formats.

- Compare your current procedures for disclosure of health information with the final privacy standards. Are individuals allowed to inspect and copy their health information? Are reasonable fees charged for this? Does the organization account for all disclosures of protected health information for purposes other than treatment, payment, or health care operations? Is there a procedure in place to allow individuals to request amendments or corrections to their health information? Is there a mechanism for individuals to complain about possible violations of privacy? Do you have a designated privacy officer?
- Review vendor contracts to assure they will be HIPAA compliant. Your contracts must ensure that your business partners also protect the privacy of identifiable health information.
- Evaluate new information security technologies. Consider adopting biometric identifiers (such as fingerprints, voiceprints, or retinal scans) for secure authentication of users. Investigate single sign-on technology to eliminate the need for users to manage and protect multiple passwords and logons.
- Evaluate the audit trails on your existing information systems. To allow the best protection, audit trails must record every access (including read-only access) to patient information. Many current audit trails record only additions or deletions to electronic information. As you evaluate your systems, look for audit trail technologies that analyze the large amount of information generated and flag suspicious patterns for further evaluation.
- Throughout this process, keep in mind that your approach should be flexible, scaleable, and reasonable. Because technology—especially security technology—is changing so rapidly, the standard will give your organization the flexibility to choose its own technical solutions. You also want to be sure your approach is scaleable to provide an economically feasible solution. Finally, ensure the policies and procedures you outline are reasonable and that your organization can assure compliance. Documenting policies and procedures your staff can not (or does not) follow consistently creates liability for your organization.

Good Luck

The contents of this document are intended for general informational purposes only and should not be considered legal advice. The Nebraska SNIP assumes no liability for intended use or otherwise. Consult your legal counsel as you implement HIPAA strategies or act upon information contained in this document. This material may be reproduced by Nebraska SNIP Task Group members to develop HIPAA Administrative Simplification compliance plans for their organization and others. Use of Nebraska SNIP material should cite Nebraska SNIP as the source.

Copyright Nebraska SNIP, 2002. All rights Reserved.