HIPAA INFO

These standards are designed to:

- Improve the efficiency and effectiveness of the healthcare 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 regulations promulgated by DHHS are far-reaching--*all healthcare organizations that maintain or transmit electronic health information must comply*. This includes health plans, healthcare clearinghouses, and healthcare providers, from large integrated delivery networks to individual physician offices. After the final standards are adopted, small health plans have 36 months to comply. Others, including healthcare providers, must comply within 24 months

Electronic Transactions and Code Sets

Currently, there is no common standard for the transfer of information between healthcare providers and payers. Over 400 electronic data information ("EDI") formats are used by various payors. As a result, providers have been required by payers to meet many different requirements. For providers who submit claims to hundreds of payers, programming computer systems to meet these requirements has been a difficult and expensive process.

The new regulations are an effort to reduce paper work and increase efficiency and accuracy 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 for EDI:

- Claims/encounters, eligibility verification, enrollment, and related transactions: *American National Standards Institute ANSI X12N*
- Pharmacy transactions: *National Council for Prescription Drug Programs (NCPDP)*
- Diagnoses 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 3 and *HCFA Common Procedural Coding System* (HCPCS)
- Physician services: *Current Procedural Terminology* (CPT)
- Dental services: *Current Dental Terminology* (CDT)

For more information, you can review the final regulations outlining new standards and code sets for electronic healthcare transactions in their entirety as published in the August 17, 2000, *Federal Register*. The regulations can be downloaded from DHHS's website at http://aspe.os.dhhs.gov/admnsimp/. In addition to providing the regulation text, the preamble to the August, 2000 *Federal Register* publication also discusses several issues and concerns raised in the 17,000 comments received after the May 7, 1998 Notice of Proposed Rule Making ("NPRM").

Privacy

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 DHHS to promulgate final regulations to protect patient privacy. DHHS published a NPRM for individually identifiable health information on November 3, 1999. After reviewing more than 50,000 comments, DHHS published the final regulations on December 28, 2000.

These standards outline specific rights for individuals regarding protected health information and obligations of healthcare providers, health plans, and health care clearinghouses. The privacy regulations grant healthcare consumers a greater level of control over the use and disclosure of personally identifiable health information. In general, healthcare 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 final rule's applicability is expanded to include all personally identifiable health information, irrespective of 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. This expansion eliminates the anticipated confusion of handling various categories of records differently.

Health plans and healthcare providers must inform their patients/beneficiaries of their business practices concerning the use and disclosure of health information. Direct healthcare providers must obtain written consent from a patient for use and disclosure of health information, *even if* the use or disclosure is related such routine purposes as treatment or payment. A separate, specific authorization is required for non-routine disclosures. (Requirements for consent and authorization are forthcoming.) Finally, 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 or payment. Patients also have a right to review and copy their own medical records and have the corresponding right to request amendments or corrections to potentially harmful errors within the record.

Healthcare 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 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-identifiable information whenever possible. Once information is in a de-identifiable form, it is no longer subject to the privacy regulation restrictions.

For more information, you can review the final regulations in their entirety as published by in the December 28, 2000, *Federal Register*. To download them from DHHS's website, go to http://aspe.os.dhhs.gov/admnsimp/. The anticipated compliance date for the privacy regulations is February 26, 2003.

On January 22, 2001, the Bush Administration released a 60 day stay on all regulations passed in the last 60 days of the Clinton Administration to give the new administration time to review the legislation and determine how it will proceed with the recent legislative changes.

Unique Identifiers

HIPAA mandates the use of unique identifiers for providers, health plans, employers, and individuals receiving health care services (patients).

The unique identifier for providers is the National Provider Identifier, which was developed by HCFA 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 DHHS to establish a system to assign the identifiers, and this may be Web-based.

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

The employer identifier is based on the *de facto* standard, the Internal Revenue Service assigned Employer Identification Number (EIN). The EIN has nine numeric positions.

The most controversial of the proposed identifiers, the patient identifier is on hold pending privacy legislation. However, industry experts speculate that the identifier will consist of approximately ten numeric digits with a check digit.

For more information, you can review the proposed regulations in their entirety as published in the *Federal Register*:
National Provider Identifier: May 7, 1998
National Employer Identifier: June 16, 1998

Security

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, DHHS developed a security standard with input from SDO's and business interests. Published in August, 1998, this proposed standard is technology neutral and scaleable for the size and complexity of healthcare organizations.

At a minimum, all health plans, clearinghouses, and healthcare 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.

Up and Coming Standards

DHHS still has to propose the following standards: Unique Identifier for Health Care Plans for electronic transactions (April, 2001 anticipated), Standards for claims attachments (2002 anticipated), Standards for transferring standard data set elements for coordination of benefits between health care plans (placed on hold pending passage of privacy and security regulations).

Implementation Strategy

- Even though HIPAA standards are still being finalized, healthcare organizations must move quickly to develop and implement compliance plans.
- Obtain copies of the proposed rules from the Department of Health and Human Services' comprehensive HIPAA website. Go to http://aspe.os.dhhs.gov/admnsimp/) As you read the proposed rules, identify gaps between your current practices and proposed 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.
- Educate your 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 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. Since most organizations lack the internal resources to efficiently perform an MPI clean-up project, obtain bids from reputable vendors and put this in your budget.
- 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 proposed 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 healthcare 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/revise existing vendor contracts to assure HIPAA compliance. 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 new systems, look for audit trail technologies that can 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 cannot (or does not) follow consistently creates liability for your organization.

Disclaimer: This article is not legal advise and is for informational purposes only.