



I. OVERVIEW

The Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191), also known as HIPAA, was enacted as part of a broad Congressional attempt at incremental healthcare reform. The "Administrative Simplification" aspect of that law requires the United States Department of Health and Human Services (DHHS) to develop standards and requirements for maintenance and transmission of health information that identifies individual patients.

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.

The provisions cover the following areas:

1. Electronic Transactions and Code Sets Rule
2. Privacy Rule
3. Security Rule*
4. Unique Identifiers (Providers, Employers, and Health Plans)*

* Has not been finalized

A. Enforcement

Under the Privacy regulations, the DHHS Secretary has delegated enforcement responsibilities to the DHHS Office for Civil Rights (OCR). The OCR will be responsible for (1) assisting with voluntary compliance efforts, (2) responding to questions on regulations, interpretation and guidance, (3) responding to state requests for exception

determinations, (4) investigating complaints, (5) conducting compliance surveys, and (6) when a covered entity does not voluntarily comply, and referring criminal prosecution.

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

The law provides for *significant* financial penalties for violations:

General Penalty for Failure to Comply:

- Each violation: \$100.
- Maximum penalty for all violations of an identical requirement: May not exceed \$25,000.

Wrongful Disclosure of Individually Identifiable Health Information:

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

B. Impact

HIPAA is an enterprise-wide issue—not an information technology issue. There are legal, regulatory, process, security, and technology aspects to each proposed rule that must be carefully evaluated before an organization can begin its implementation plan. HIPAA is rapidly becoming a major issue in healthcare because:

- Senior management is responsible for the security and confidentiality of patient health 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.

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. (The government estimated the five-year "conservative" cost of the privacy regulation alone to be \$3.8 billion.)

HIPAA will have a major, ongoing impact on healthcare providers in several areas:

- Significant resources will be required.

- Some degree of IT retooling will be required, as well as major operational and procedural changes.
- Transactions will become more standardized, resulting in eventual savings for electronic data interchange.
- For transaction standards, code sets, and identifiers, implementation will be the most expensive. Ongoing costs will involve obtaining and implementing updates to the standards.
- Security and privacy regulations will be the most difficult and costly to implement and maintain because they are broad in scope, less definitive, and require constant vigilance for ongoing compliance.

II. ELECTRONIC TRANSACTIONS AND CODE SETS

Currently, there is no common standard for the transfer of information between healthcare providers and payors. Over 400 electronic data information (“EDI”) formats are used by various payors. As a result, providers have been required by payors to meet many different requirements. For providers who submit claims to hundreds of payors, 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 payors 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)

Revised HIPAA Code Sets

- **ICD-9-CM** (Diagnosis and Procedures)
- **CPT-4** (Physician Procedures)
- **HCPCS** (Ancillary Services/Procedures)
- **CDT-2** (Dental Terminology)
- **NDC** (National Drug Codes)
- Other supporting code sets

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 14, 2002, 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 May 7, 1998.

The main change for your organization will be that the HCFA 1500 form will no longer be used for electronic transactions. Once the new rules are in effect, your organization must submit claims in the ANSI ASC X12N 2761277 format. Electronic health payments, EOB transactions and remittance advice must be processed using the ANSI ASC X12N 835 format.



GET HIP WITH HIPAA TIP:

Organizations should note that after the compliance deadline, their claims may be denied if they do not collect all the new required data. Any organization that works with a billing service or has a billing software vendor should determine what data needs to be collected in order to get paid.

A. Electronic Transaction Checklist:

1. Identify and document the current status of your organization's electronic billing systems and their degree of HIPAA readiness.
2. Identify the risks to the organization if your vendor fails to make your billing systems compliant by the October 16, 2003 deadline (assuming the extension form has been filed).
3. Locate the contracts and service agreements you have with your software vendors.
4. Locate and document all communications you may have or are planning to initiate with the responsible systems vendor regarding their HIPAA compliance and testing plans and due dates. See your legal counsel for assistance in writing these communications.
5. Locate and document your contracts and service agreements with the vendors who maintain or troubleshoot your information systems.

See Electronic Healthcare Transactions and Code Sets Extension Form in Appendix.

Questions To Ask Your Vendors:

- When will you be ready to upgrade my system?

- Will I require any new hardware?
- Will you send me a schedule of upgrades and testing?
- Can I upgrade incrementally?
- What are the costs?
- When will you be ready to accept a HIPAA compliant claim?
- Will you be providing any billing software?
- When will you be able to handle the additional transactions?

B. Unique Identifiers

HIPAA proposes to mandate 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 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 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 CMS did for a Medicare Payor ID 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 rules and regulations.

C. HIPAA Electronic Transaction Extension Form Issued By CMS

On March 28, 2002, CMS issued an application form for requesting a one year extension to comply with the HIPAA electronic transactions rule. To take advantage of the one-year extension, organizations must electronically submit the application form by October 15, 2002 or have the form postmarked for hard copy submissions by October 15, 2002. CMS has published an electronic version of the form that can be submitted via the internet.

An organization that fails to submit a form to CMS and is not compliant by October 16, 2002 can be excluded from the Medicare program. The extension form contains sections including a requirement that organizations set forth their implementation strategy for meeting the October 2003 deadline.

When completing the extension form an organization must provide information regarding the following:

- The organization will acquire information regarding electronic transactions and code set rules; and will conduct staff training.
- The organization will inventory gaps, identify implementation issues and develop a plan.
- The organization will finalize applicable software, complete staff training, and start and finish testing issues.

It is highly recommended that even if an organization believes they will be compliant with the transaction code sets by October 15, 2002, the organization should still file the extension form. Therefore, we recommend that all organizations file the extension form by October 15, 2002. Also, those organizations utilizing the services of a clearinghouse or billing service should communicate with these companies to make certain that they also complete an extension form.



GET HIP WITH HIPAA TIP:

An organization should review the electronic transactions and code sets extension form which identifies formats and code sets that must be used in connection with electronic transactions commonly conducted by a healthcare organization.

III. 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 Notice for Proposed Rule Making (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 through

the Notice of Privacy. A separate, specific authorization is required for non-routine disclosures. As a component of privacy rights, 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 regulations in their entirety in the Federal Register. To download them from DHHS website, go to <http://aspe.os.dhhs.gov/admsimp/>. The compliance date for the privacy regulations is April 14, 2003.

IV. 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. Standards for claims attachments. Standards for transferring standard data set elements for coordination of benefits between health care plans.

A. Important Dates

Current HIPAA Rule compliance dates:

October 15, 2002 – The date by which an Electronic Transactions and Code Set extension must be filed.

October 16, 2002 – The compliance date for the new Electronic Transactions and Code Set for organizations, except small health plans as defined by HHS, that did not file for an extension.

April 14, 2003 – The compliance date for the Privacy Rule and Regulations. The rules were finalized on August 14, 2002.

April 16, 2003 – Deadline to begin testing for compliance with the electronic transactions rule if an organization has applied for the one-year extension.

October 16, 2003 – The compliance date for the Electronic Transactions and Code Set for all organizations that applied for an extension. Note: the regulations require testing to begin no later than April 16, 2003.

October 16, 2003 – The date that Medicare will no longer accept claims from Medicare providers that did not qualify for the following waivers:

- § You are an exempted “small health plan”.
- § You are a small provider of services or supplies.
- § You do not have the ability to submit claims in an electronic form.
- § You are a beneficiary that is submitting a claim(s) on your own behalf.

2004 – Potential deadline for compliance with security rule. The current proposed security rule is not yet final.

I. What's Next?



Although there are now definitive timelines, additional changes to the rules are possible. However, the timing of any such changes are not known nor can they be projected. Therefore, each organization should begin making every effort to meet HIPAA's known rule requirements without delay. The HIPAA clock is now ticking.

B. Privacy Officer

The information privacy officer is responsible for developing, implementing, and maintaining adherence to the healthcare organization's policies and procedures governing HIPAA.

This person should be responsible for maintaining a good understanding of the HIPAA privacy rule as well as any Michigan privacy rules that continue to apply to the organization's activities.

Examples of Information privacy officer are:

- Office Manager
- Organization Administrator
- Billing Manager
- Physician, etc.

The HIPAA privacy rule requires that the designation of the Information Privacy Officer be documented and retained by the respective organization.

See Privacy Officer Job Description in Appendix.



GET HIP WITH HIPAA TIP:

All privacy officers should be aware that Michigan also has specific privacy rules and should have knowledge of both the federal and state rules.

C. Privacy Contact Person Or Office

The HIPAA privacy rule also requires that a physician organization designate a “contact person or office” who is in charge for receiving privacy complaints. The privacy rule does not require that the contact person be a different person than the privacy officer. If the same person holds both the role of the privacy officer and the privacy contact, that person’s name can be listed on both designations.

V. REASONS TO ESTABLISH A HIPAA PROJECT PLAN

All members of a healthcare organization’s workforce play key roles in ensuring information security and privacy. Consider the following scenarios:

- The housekeeper called upon to clean an isolation room who may be curious about its last occupant.
- The individual who takes the trash from locked shredder bins to the designated service collection point, but leaves the trash unattended while returning for the forgotten key.
- The friendly volunteer who believes in making people feel comfortable by inquiring about the nature of their illness.
- The physician who spends hours of clinic time day trading, thereby slowing down system access time.
- The clergyman who recognizes a member of the congregation and seeks to provide solace when perhaps the individual is not yet ready.
- The medical student who is so intent on diagnosing a patient that personal details are shared with a fellow student in the local tavern.
- The nurse who grieves for a neighbor’s stillborn and, in a friendly gesture, orders a pie to be delivered to the family.

All the above scenarios have actually occurred. Many of them resulted in termination or dismissal. Most healthcare organizations are aware of the need for improved security and privacy. In addition, many organizations have installed privacy partitions, adopted shredder bins, turned monitors away from public view, and removed patient names from whiteboards. Every member of the workforce is key to having effective safeguards and protections. One more reason to establish a HIPAA implementation plan.

