



eServices Group, Inc.

Health Insurance Portability and Accountability Act (HIPAA) Overview

For more information contact:
eServices Group, Inc.
5301 Buckeystown Pike, Suite 400
Frederick, MD 21704
phone: (301) 698-1900
fax: (301) 698-1909
internet: www.esrv.com and www.medicaidonline.com

Health Insurance Portability and Accountability Act (HIPAA) Overview

This white paper provides an explanation of the Health Insurance Portability and Accountability Act (HIPAA). It is intended to provide a general understanding of each of the regulations/standards required by the statute. It also describes the overall impact of HIPAA to the healthcare industry and the actions healthcare organizations will need to take in order to adapt to the new legislation.

I. General Overview

A. Introduction/Background

The Health Insurance Portability and Accountability Act (HIPAA) was signed by President Clinton on August 21, 1996. The original intent of this act was to provide portability or the continuation of healthcare coverage for workers and their families when they change or lose jobs. However, a number of provisions were added to the bill as it moved through Congress. These provisions are defined under the “Administrative Simplification” title.

B. Administrative Simplification

The purpose of this section is to improve both Federal and private health programs. It aims to increase the effectiveness and efficiency in healthcare delivery by standardizing electronic data interchange. Further, it intends to protect the confidentiality and security of health data through setting and enforcing standards.

The Administrative Simplification section requires the Secretary of the Department of Health and Human Services (“The Secretary”) to adopt:

- Standards for electronic transactions and data elements for those transactions
- Standard code sets to be used in the transactions
- Unique health identifiers
- Security standards and safeguards for electronic information systems involved in those transactions
- Privacy regulations for patient identifiable information

These Administrative Simplification provisions do not require that all health information be transmitted electronically. What they do require, however, is that if electronic media is used to transmit any health information, it must be done in agreement with the regulations.

C. Statutory Processes/Compliance

The Secretary uses the **Federal Register**¹ to distribute proposals for the required standards and regulations. Once a formal proposal is developed, a draft rule (also known as a Notice of Proposed Rulemaking or NPRM) is published in the **Federal Register**. Once the NPRM is released, the public has an opportunity to submit written comments on the proposed action. A response to these comments is then issued in the **Federal Register**. The comment period can be extended or another proposal could be published due to the nature

¹ The Federal Register is a legal newspaper published every business day by the National Archives and Records Administration (NARA). It is the official publication for rules, proposed rules, and notices from Federal agencies and organizations, as well as executive orders and other presidential documents.

Health Insurance Portability and Accountability Act (HIPAA) Overview

of the comments received. However, a Final Rule will ultimately be published which specifies the date the new regulatory requirements or requirements become effective (also called the compliance date).

Most of the HIPAA mandates were supposed to become effective in February 1998, with compliance required by February 2000. However, this did not happen due to recurring delays in the development of the draft rules (also known as the Notices of Proposed Rulemaking or NPRMs) within the Federal government.

The following chart shows the time schedule the Department of Health and Human Services (DHHS) is planning to use to issue HIPAA regulations under the following schedule. As of February 2001, this is the most recent timetable. However, it is subject to change and the following link should be checked for new updates:

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

Regulation	NPRM (Proposed Rule) Published	Final Rule Published
Transaction and Code Sets	May 5, 1998	August 17, 2000
Unique Identifiers		
• National Provider Identifier	May 5, 1998	
• National Employer Identifier	June 16, 1998	
• National Health Plan Identifier		
• National Individual Identifier	on hold	on hold
Security	August 12, 1998	
Electronic Signatures	August 12, 1998	
Privacy	November 4, 1999	December 28, 2000
Claims Attachments		
Enforcement		

Note: Where dates are missing, DHHS has not yet set any specific target dates.

Final Rules for establishing standards for electronic transactions and the code sets used within those transactions (also called the “Transactions Rule”), and for creating standards for privacy of individually identifiable health information (also called the “Privacy Rule”) have been published. The Transactions Rule was published in the **Federal Register** on August 17, 2000 (65 FR 50312) and requires that all Covered Entities² be in compliance with the standards by October 16, 2002 (2003 for small health plans). The Privacy Rule was published in the **Federal Register** on December 28, 2000 (65 FR 82462) and requires that all Covered Entities be in compliance with the standards by February 26, 2003 (2004 for small health plans).

² A “Covered Entity” is one of the following: a health plan, a healthcare clearinghouse, or a healthcare provider who transmits any health information in electronic form in connection with a standard transaction.

Health Insurance Portability and Accountability Act (HIPAA) Overview

The following link provides direct access to **Federal Register** publications of the Final Rules for the Administrative Simplification section of HIPAA:

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

Final Rules for establishing unique health identifiers and security standards and safeguards are not yet available.

D. Why use Electronic Media and why Standardize?

Electronic Data Interchange (EDI) is the electronic exchange of information in a standardized format between two entities. EDI allows organizations within the healthcare industry to exchange medical, billing and other information and to process transactions in a fast and cost effective manner. Many entities in the healthcare industry recognize the benefits of EDI and have developed proprietary formats. Currently, about 400 different formats for healthcare claims exist. However, according to the **Federal Register** (65 FR 50312), using many different formats for electronic transactions makes it difficult and expensive to develop and maintain software. Further, the lack of standardization “minimizes the ability of health care providers and health plans to achieve efficiency and savings.”

HIPAA establishes a national standard for electronic claims and other transactions. A national standard means one format for these electronic transactions. And now that these standards are in place, healthcare providers will be able to submit a standard transaction containing standard content to any health plan in the United States and that plan has to accept it. Moreover, health plans are able to send standard electronic transactions (remittance advice and referral authorizations) to healthcare providers. National standards make EDI a practical and preferable alternative to paper processing.

II. A Closer Look at the Provisions

A. Transactions

HIPAA requires The Secretary to adopt standards for the following administrative and financial healthcare transactions:

- Health claims or equivalent encounter information
- Enrollment and 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
- First report of injury

Health Insurance Portability and Accountability Act (HIPAA) Overview

- Coordination of benefits (COB)
- Attachments

The final rule adopts certain ASC X12N³ Version 4010 standards for each of the specified electronic health care transactions (except attachments and first report of injury). It also adopts the National Council for Prescription Drug Programs (NCPDP) electronic formats for retail pharmacy transactions. In the near future, another final rule for attachments transactions will include standards developed by Health Level 7 (HL7).

The Secretary is adopting the following X12N standards:

- ASC X12N **837** for health claims and equivalent encounter information
- ASC X12N **834** for enrollment and disenrollment in a health plan
- ASC X12N **270/271** for eligibility for a health plan
- ASC X12N **835** for healthcare payment and remittance advice
- ASC X12N **820** for health plan premium payments
- ASC X12N **276/277** for health claim status
- ASC X12N **278** for referral certification and authorization
- ASC X12N **835/837** for coordination of benefits

Standards for the first report of injury (ASC X12N **148**) and a separate coordination of benefits (ASC X12N **269**) are being drafted and will be adopted at a later date.

The mandated HIPAA formats are defined in Appendix A. A more detailed explanation of each transaction set is provided in its Implementation Guide (or specifications). These guides provide the standardized data requirements and data content for all users of the transaction sets. They can be downloaded from the following website: http://hipaa.wpc-edi.com/HIPAA_40.asp:

B. Code Sets

HIPAA requires the establishment of standardized Code Sets for appropriate data elements within the transactions described above. According to the **Federal Register** (65 FR 50367), a code set is “any set of codes used for encoding data elements, such as tables of terms, medical concepts, medical diagnosis codes, or procedure codes.” A code set includes the codes and the descriptors of the codes.

According to the **Federal Register** (65 FR 50325), The Secretary has adopted the following code sets as the standard medical data code sets:

³ ASC X12N is a set of standards created by the Accredited Standards Committee (a subcommittee of the American National Standards Institute, ANSI) to facilitate the electronic exchange of business information pertaining to the insurance industry. These standards define the data formats and encoding rules for a multitude of business transactions and set the norm for a more effective exchange of information.

Health Insurance Portability and Accountability Act (HIPAA) Overview

- **International Classification of Diseases, 9th Edition, Clinical Modification, (ICD-9-CM), Volumes 1 and 2** (including The Official ICD-9-CM Guidelines for Coding and Reporting), as updated and distributed by DHHS, for the following conditions:
 - Diseases
 - Injuries
 - Impairments
 - Other health related problems and their manifestations
 - Causes of injury, disease, impairment, or other health-related problems
- **International Classification of Diseases, 9th Edition, Clinical Modification, (ICD-9-CM), Volume 3 Procedures** (including The Official ICD-9-CM Guidelines for Coding and Reporting), as updated and distributed by DHHS, for the following procedures or other actions taken for diseases, injuries, and impairments on hospital inpatients reported by hospitals:
 - Prevention
 - Diagnosis
 - Treatment
 - Management
- **National Drug Codes (NDC)**, as updated and distributed by DHHS, in collaboration with drug manufacturers, for the following:
 - Drugs
 - Biologics
- **Code on Dental Procedures and Nomenclature**, as updated and distributed by the American Dental Association, for dental services.
- The combination of **Health Care Financing Administration Common Procedure Coding System (HCPCS)**, as updated and distributed by DHHS; and **Current Procedural Terminology, Fourth Edition (CPT-4)**, as updated and distributed by the American Medical Association, for physician services and other health related services.
- The **Health Care Financing Administration Common Procedure Coding System (HCPCS)**, as updated and distributed by HCFA, DHHS, for all other substances, equipment, supplies, or other items used in health care services.

C. Unique Identifiers

HIPAA stipulates the establishment of unique health identifiers for healthcare providers, health plans or payers, employers, and individuals. It also requires that the adopted standards specify for what purposes unique health identifiers may be used.

Health Insurance Portability and Accountability Act (HIPAA) Overview

The Notice of Proposed Rulemaking (NPRM) recommending the National Provider Identifier (NPI) as the standard healthcare provider identifier was published in the **Federal Register** (63 FR 25320). The proposed standard for the NPI is an eight-position alphanumeric identifier that includes a check digit in the last position. The identifier would be implemented through a central electronic enumerating system and would be managed by HCFA (Health Care Financing Administration).

Currently, there is no specific information on the payer ID for payers/health plans.

The proposed standard for employer identifiers would be the employer identification number assigned by the Internal Revenue Service.

Individual health identifiers do not have a standard and will not until legislation is enacted specifically approving the standard. Currently, six alternatives for the identifier are being considered:

- Social Security Number
- Biometric identifiers
- Directory service
- Personal immutable properties
- Patient identification system based upon existing medical record number and practitioner prefix
- Public key/private key cryptography method

Individual identifiers have been controversial because of the perception that “access” to all information on an individual could be obtained through a single identifier. (For more information on individual identifiers, see the following website: <http://www.forhealthfreedom.org/hhswhitepaper>.)

Rules for all unique health identifiers are still being drafted and are not yet available to the public.

D. Security Standards and Privacy Regulations

Although closely related, security and privacy are two separate entities. It is important to differentiate between the two terms because it is possible to secure information without making it private, however it is not possible to protect privacy without having security. In the white paper, **Guide to Understanding and Complying with HIPAA Security and Privacy Regulations** (<http://www.hipaacomply.com/news.htm>), security is defined as “the ability to control access and protect information from accidental or intentional disclosure to unauthorized persons and from alteration, destruction, or loss.” On the other hand, privacy is defined as “controlling who is authorized to access the information (the right of individuals to keep information about themselves from being disclosed).”

Security Standards

The security requirements imposed by HIPAA represent a significant challenge to the exchange of electronic healthcare transactions. HIPAA requires affected entities to

Health Insurance Portability and Accountability Act (HIPAA) Overview

establish and maintain reasonable and appropriate administrative, technical, and physical safeguards to ensure integrity, confidentiality, and availability of the information. Any party transmitting healthcare information must implement the safeguards outlined in HIPAA. Further, HIPAA specifies the need for the standard to ensure that a clearinghouse, if part of a larger organization, has policies and security procedures (for both the data and the physical site) that prevent unauthorized access to the sensitive information by the larger organization.

On August 12, 1998, HCFA published its proposed standard for the security of health information and the use of electronic signatures in the healthcare industry (also called “The Security Standards”) in the **Federal Register** (43 FR 43242). The Security Standards were created to protect health information against predicted threats or hazards to the security or integrity of the information, and to protect the information against unauthorized use or disclosure. The Security Standards address both organizational and technical practices and procedures and are divided into four categories:

- Administrative Procedures
- Physical Safeguards
- Technical Security Services
- Technical Security mechanisms

The administrative procedures are documented formal procedures designed to manage the selection and execution of security measures to protect data and manage the behavior of personnel in relation to the protection of data. The physical safeguards are designed to protect physical computer systems and related buildings and equipment from natural and environmental hazards (such as fire), as well as from intrusion. The physical safeguards address the use of locks, keys, and administrative measures used to control access to computer systems and facilities. The technical security services are processes designed to protect information and control individual access to information. The technical security mechanisms are processes that guard against unauthorized access to data that is transmitted over a communications network.

The Security Standards were supposed to be finalized after an open comment period that ended October 13, 1998. However, the publication of the final rule has been delayed several times. Currently, the delay is in part to allow the DHHS to align the Security rule with the Privacy rule.

Privacy Regulations

HIPAA calls for standards that protect the privacy of individually identifiable health information. As previously mentioned, the Privacy Rule was published on December 28, 2000 (65 FR 82462). According to the **Federal Register** (65 FR 82463), this regulation has three major purposes:

- To protect and enhance the rights of consumers by providing them access to their health information
- To improve the quality of healthcare in the U.S. by restoring trust in the healthcare system

Health Insurance Portability and Accountability Act (HIPAA) Overview

- To improve the efficiency of health care delivery by creating a national framework for health privacy protection

Until now, there were practically no federal rules to protect the privacy of health information and guarantee the patient access to such information. However, as reported in the **Federal Register** (65 FR 82464), “this final rule establishes, for the first time, a set of basic national privacy standards and fair information practices that provides Americans with a basic level of protection and piece of mind that is essential to their full participation in their care”.

The Privacy Rule is very detailed and it would be a very lengthy discussion to address everything encompassed by this rule. As a result, the main points (from a vendor’s perspective) are highlighted below.

First of all, this rule protects the privacy of Protected Health Information (PHI). PHI refers to all individually identifiable health information that is transmitted or maintained by a covered entity, regardless of form. This includes oral, paper, and electronic information. The rule requires that Protected Health Information may not be used or disclosed unless the disclosure is either permitted by the patient or is specifically allowed under HIPAA regulation.

The rule also allows individuals to control the disclosure of their PHI and the right to access their PHI. With the exception of disclosures made for the purpose of treatment, payment and healthcare operations, the individual has the right to request and receive an accounting for all of the disclosures of their PHI and know to whom their information has been disclosed and the purpose of such disclosures.

The privacy rule also gives specific guidelines on de-identifying health information. PHI is de-identified when:

1. A person with appropriate knowledge applying generally accepted statistical and scientific methods makes a determination that the risk of re-identification of certain information is very small.
2. All the following identifiers of the individual, relatives, employers, and household members have been removed:
 - Names
 - All geographic codes smaller than state, including street, city, county, precinct or zip code
 - All date elements related to an individual
 - Telephone number, fax number, email address, SSN, medical record numbers, health plan beneficiary number, account numbers, certificate/license numbers, any vehicle identifiers (serial number, license plate, etc.), device identifiers & serial numbers, URL’s, IP address, biometric identifiers (fingerprint, voice print, etc.), full face photographic or comparable images, and other unique identifying number, characteristics or code

Health Insurance Portability and Accountability Act (HIPAA) Overview

III. The Effects of HIPAA Implementation

HIPAA will have a significant impact on the healthcare industry, affecting all healthcare organizations, regardless of their size or technical sophistication. This single piece of legislation will dramatically change the way healthcare is administered and delivered over the next few years.

HIPAA presents both benefits and challenges to organizations. HIPAA is very complicated and many industry observers expect healthcare organizations to spend more money on HIPAA compliance than they did to prepare their information systems for Y2K. In addition, HIPAA compliance is mandatory, and noncompliance could result in large fines or threaten the organization's ability to conduct business.

The legislation recognizes that, in the short term, costs will increase as solutions are implemented. However, according to the **Federal Register** (65 FR 50351), "the costs of implementing the standards specified in the statute are primarily one-time or short-term costs related to conversion". The long-term savings can be tremendous as electronic information sharing and processing replace the manual, paper-based, processes of today. The inefficiencies of handling paper documents will ultimately be eliminated, resulting in significantly reduced administrative burden, lowered operating costs, and improved overall data quality. Thus, many of the HIPAA mandated changes save healthcare organizations significant administrative time and money in the long run. Further, many industry leaders believe that HIPAA will accelerate many new forms of e-commerce.

IV. How will Organizations Adapt to the Restrictions Required by HIPAA?

Typically, healthcare organizations have three options as to how to deal with the restrictions imposed by the legislation. First, they can procure or develop an entirely new system for the processing of beneficiary eligibility and encounter data. However, due to Y2K expenditures, it is unlikely that many organizations will have the resources necessary for the procurement of an entirely new Healthcare Management Information System (HMIS), nor the research and development required to "roll their own".

A second alternative for States is to go through an electronic data clearinghouse (such as Envoy or NDC) and have all transactions converted to whatever format is appropriate for their particular HMIS. A clearinghouse or EDI package front-end solution represents only a partial solution to one facet of HIPAA. This presents a challenge for organizations utilizing local codes in that these codes will have to be crosswalked somehow prior to processing. These codes in turn will have to be cleansed from the transaction data prior to transmittal to the consumer. Neither a clearinghouse nor an EDI package front-end solution addresses the privacy or security provisions of the HIPAA regulations.

A third option in implementing HIPAA provisions is to alter current systems to comply with the HIPAA legislation. Although this task may seem daunting, it is an opportunity for States (and other healthcare organizations) to accomplish not only HIPAA-compliance, but to re-engineer their current processing architecture while continuing to capitalize their investment in their current HMIS.

Health Insurance Portability and Accountability Act (HIPAA) Overview

APPENDIX A

The mandated HIPAA formats are defined below:

NCPDP (National Council of Prescription Drug Programs) Telecommunication Claim
This transaction is used for retail drug claims. It is used by providers to submit pharmacy claims and by health care plans to process pharmacy claims.

270 Eligibility and Benefit Inquiry

271 Eligibility and Benefit Response

These transactions are used by providers to request and receive eligibility information from a health care plan prior to providing or billing for a health care service.

276 Health Care Status

277 Health Care Response

These transactions are used by providers to determine the status of submitted claims.

278 Health Care Services and Request for Review and Response

This transaction is used by providers to request and receive approval or certification for a patient to receive health care services (Preauthorization).

820 Payroll Deduction for Group Benefits

This transaction is used for payroll deduction and other group premium payment for insurance product.

834 Benefit and Enrollment Maintenance

This transaction is used for enrollment and disenrollment in a health plan.

835 Health Care Claim Payment/Advice

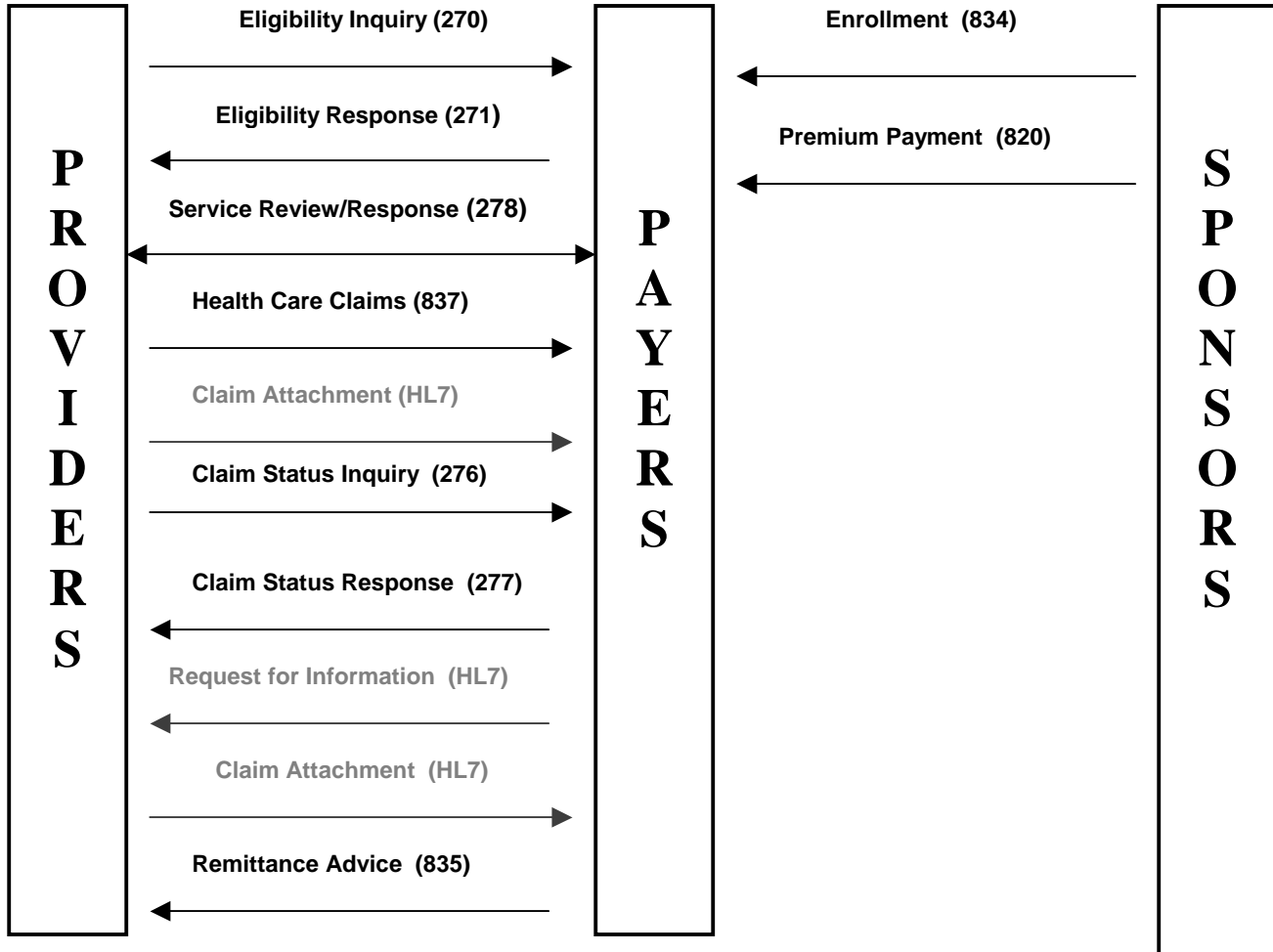
This transaction is used to send payment and/or an EOB (Explanation of Benefits) remittance advice directly to the provider or through a DFI (Depository Financial Institution). It is also used in conjunction with the 837 for the COB (Coordination of Benefits).

837 Health Care Claims

This transaction is used for the submission of Institutional Health Care Claims (UB92), Professional Health Care Claims (HCFA), and Dental Claims. It is also used in conjunction with the 835 for the COB (Coordination of Benefits).

Health Insurance Portability and Accountability Act (HIPAA) Overview

The following diagram presents an overview of the above mandated HIPAA transactions (except the NCPDP):



Note: Grey Transactions are not currently part of HIPAA

Information flows back and forth between Providers, Health Plans and Sponsors. Each of these entities is defined as follows.⁴

Providers

Under the **Federal Register** (65 FR 50366), “a provider means a provider of services as defined in section 1861(u) of the Social Security Act, a provider of medical or other health services as defined in section 1861(s) of the Social Security Act, and any other person who furnishes or bills and is paid for health care services or supplies in the normal course of business.” Providers as defined by X12N “may include entities such as physicians,

⁴All information taken from the Healthcare Transactions presentation presented by ANSI ASC X12N Task Group 3, Work 2. For more information, contact a Co-Chair listed on <http://www.disa.org>.

Health Insurance Portability and Accountability Act (HIPAA) Overview

hospitals and other medical facilities or suppliers, dentists, and pharmacies, and entities providing medical information to meet regulatory requirements”.

Health Plan

Under the **Federal Register** (65 FR 50366), “a health plan means an individual or group plan that provides, or pays the cost of, medical care”. Health Plans, as defined by X12N, refers to “a third party entity that pays claims or administers the insurance product or benefit or both”. For example, a health plan may be an insurance company, health maintenance organization (HMO), preferred provider organization (PPO), government agency (Medicare, Medicaid, etc.) or an entity that may be contracted by one of those groups {e.g. a third party administrator (TPA) or a third party organization (TPO)}.

Sponsor

A sponsor, as defined by X12N, is “the party or entity that ultimately pays for the coverage, benefit or product. A sponsor can be an employer, union, government agency, association or insurance agency”.