HIPAA Compliance for Small Healthcare Providers

Prepared by: Agent 77
Originally created: February 2002
Revised: September 2002

Legislative Background

The intent of the Healthcare Portability and Accountability Act (HIPAA - also known as the Kennedy-Kassebaum Act) was to improve an individual's healthcare portability when changing jobs and to promote administrative simplification of health insurance. In addition, the statute required congress to enact additional medical privacy and security legislation.

Initially, congress had until August 1999 to enact legislation detailing the standardization of electronic transactions and legislation covering the privacy and security of patient health information. Congress missed its deadline and required that the US Department of Health and Human Services complete these tasks. Enforcement of the HIPAA privacy regulations was handed over to the Office of Civil Rights (OCR) as the enforcement structure was already in place.

The current process for each section of HIPAA is that a final regulation becomes law 60 days after it is published in the Federal Register, assuming no further action is taken, and actual implementation is not required for 2 years to allow for a transition period.

Goals of HIPAA

Title I of the law deals with improving health insurance access and portability when changing jobs and became effective in September of 1996.

It is estimated that the Title I section of HIPAA has helped approximately 3 million individuals avoid being impacted by pre-existing conditions when changing jobs. It has also led to many large corporate health plans eliminating pre-existing condition clauses from their plans, therefore benefiting many more individuals.

Title II of HIPAA deals with administrative simplification in healthcare practices. This includes all of the major regulations surrounding changes to your business: standardizing code sets and electronic transactions, establishing privacy and security standards, and standardizing identifiers for healthcare entities (the Standard Unique Employer Identifier has been finalized; the health care provider and individual identifiers have been proposed but not yet finalized as of the latest revision of this manual),.

It is estimated that over 20 cents of every healthcare dollar is spent on administrative overhead. Administrative simplification is intended to improve this situation by creating common standards and data requirements across all segments of the industry.

It is also estimated that 11 cents on every healthcare dollar is attributable to fraud

and abuse. HIPAA tries to address this in Title II through accountability. This is accomplished by defining sanctions for violations of the privacy and security regulations, and further supported by safe harbor provisions. These safe harbor provisions encourage self-reporting of violations and provide protection for whistle blowers.

Transactions

Transactional Compliance For Small Practices

The challenges small providers face in meeting the HIPAA transaction standards are different from those faced by larger providers and health systems. Nevertheless, because all healthcare providers must adhere to the same standards, even small providers must go through the effort of ensuring that they are using the code sets and transaction standards defined by HIPAA. Recent legislation, with few exceptions, requires that all healthcare providers must submit claims to Medicare via compliant electronic transactions no later than October 16, 2003.

Small providers usually fall into one of four categories:

- **Providers not using electronic data interchange (EDI)** have the option of continuing to interact with payers manually, or can automate and have more efficient processing, faster claims turnaround, and improved patient accounts tracking.

- **Providers using a clearinghouse for transactions** must ask their clearinghouse to describe their plans regarding HIPAA transactional compliance. It is critical for providers to not only document their plans, but also to thoroughly test all transactions well before October 2003 to ensure minimal impact of the changeover.

- **Providers currently using systems that cannot be easily made compliant** (usually the result of either in-house development or purchase from a vendor who is no longer in business) should move to a HIPAA compliant automated system. The cost of these systems, even when combined with the switching cost involved, is almost always less than the time and effort involved in making modifications to old or homegrown systems. It is important to assess the cost/benefit analysis of retrofitting their existing systems versus installing a new system.

- **Providers with systems whose vendors will make them compliant** must ask their vendors to describe their plans, to identify costs and to ensure that there will be no interruption of transactions for the provider. Again, it is important to not only verify the vendor's intentions, but also install and thoroughly test all updates.

Types Of Transactions Regulated Under HIPAA

HIPAA regulations cover:

- Claims or encounter information
- Eligibility
- Healthcare payment and remittance advice
- Health claims status
- Referral authorization
- Coordination of benefits
- Health claims attachments (anticipated standard)

- First report of injury (anticipated standard)

Code Sets

HIPAA requires that the following code sets be used in conducting electronic transactions:

- ICD-9 CM – Diagnosis and procedure coding for administrative transactions
- ACD-10 CM update - Diagnosis and procedure coding for administrative transactions (anticipated standard)
- CPT-4 – service-level coding for physicians (Level one of HCPCS)
- CPT-5 update - service-level coding for physicians (Level one of HCPCS) (anticipated standard)
- Alphanumeric HCPCS – Coding medical equipment, injectible drugs, transportation services and other services not included in CPT-4. (Level two HCPCS)
- HCPCS local codes termination
- CDT-2 – Dental transactions (HCPCS D-codes)
- NDC – Prescription drug coding in pharmacy transactions and for healthcare professionals

Transaction Compliance Officer

The Transaction Compliance Officer is not an official HIPAA role, but is an important one in making sure that the small healthcare practice becomes and stays compliant with HIPAA's transactional regulations.

Dealing with Software Vendors

The vendor from whom you purchased your practice management software is one of your greatest resources when it comes to complying with HIPAA transactions. You should verify your software vendor's plans regarding each specific transaction and code set required under HIPAA for transactions that you use or plan to use. Verify all costs for the upgrade, install charges, and consulting or other fees. Your cost will depend on the vendor's policies regarding software maintenance. Many vendors will distribute upgrades to maintain Federal regulatory compliance as part of the standard maintenance fee.

Contact your vendor(s) early in your compliance efforts to ensure that there is ample time to obtain releases and documentation, educate yourself on the feature changes in the release, and install and test adequately prior to converting live data to the new formats and code sets.

Note that your software vendor is probably not regulated by HIPAA. Because the Department of Health and Human Services (HHS) has no jurisdiction over non-healthcare entities, it most likely does not have direct jurisdiction over your software vendor. Regardless, <u>you</u> are legally responsible for ensuring that all transactions initiated by your office are compliant.

Dealing with Trading Partners

Trading Partners, or those with whom you exchange electronic patient, encounter, claims and payment information, have a special role in helping you to achieve HIPAA compliance. Unlike software vendors, many trading partners, including payers, clearinghouses and the like are regulated by HHS.

Since transactions by their nature involve multiple parties, those to whom you send and receive data must all operate using the same standard. HIPAA requires that a

single national standard be used. This is a significant difference from the many different file and data formats that were supported in the past, and will result in significant systemic cost savings.

You should work with all existing trading partners to assess their plans regarding HIPAA compliance, testing protocols and any transition or other costs associated with moving to HIPAA-compliant transactions.

Benefits of EDI to Small Practices

Small practices can use the work associated with HIPAA to improve their efficiency and cost structures. Consider the following:

- Using a computer system and EDI typically improves claims turnaround, allowing you to collect on insurance and balance bill faster, improving cash flow and collections.
- Electronic authorizations reduce the cost to determine health insurance coverage and allowed treatments, increasing patient satisfaction and collections.
- Even on lower volumes, electronic claims submission can reduce administrative costs to generate and track bills.

Economical computers are available for under $700 and practice management software can be purchased for under $1000. Virtually no training is required for those already familiar with office procedures.

Compliance Testing

Complete, thorough and accurate testing of all changes to computer and EDI systems is essential for successful migration to HIPAA compliance. Software testing is always good business and, given the penalties that accompany non-compliance with HIPAA, there is a dual incentive to thoroughly test before moving your office to new practices or EDI software.

To test properly, you will need a complete test plan, test data, a safe testing environment that does not interfere with daily operations and trained staff to execute the plan and document its results. Following up and re-testing any discrepancies from your expected results is essential.

Privacy

Why privacy regulations are required

The Hippocratic Oath and the laws of every state provide assurances to patients that their medical data will be held in confidence. However, the patchwork of state laws regulating patient privacy does not adequately provide assurances to patients in today's world in which medical records and patient information are broadly held in electronic form. As a result, HIPAA regulations were developed to ensure consistent treatment of patient's medical data by every healthcare provider in the United States.

HIPAA regulations do not automatically override existing state laws. As a general rule the more stringent law is the one to follow. You should follow your state law if it already requires privacy protection for patient information that is more stringent than HIPAA. You should follow HIPAA if your state does not have privacy protection for patient information or if it is less stringent than HIPAA.

Basic Tenets of HIPAA Privacy Rules

HIPAA's Privacy Rules embody 5 fundamental tenets:

1. **Contact** – Each office will have a Privacy Officer who serves as the single contact for patient privacy information
2. **Patient Access** - Increased access and control by patients of their own information
3. **Limited Access** - Limit access to patient information except to those authorized and then only to the minimum information necessary to do the task in question.
4. **Consistent Self-Regulation** - Adopt clear and consistent privacy policies and procedures
5. **Education** - Train employees to understand these rules

Privacy Officer

The law requires that each practice appoint a single person to be responsible for protecting patient data. While this person can – and in smaller offices definitely will – have other duties, responsibilities will always include ensuring that HIPAA privacy rules are followed, and providing patients with a single point of contact for requesting access to their records and for filing grievances. The self-policing nature of designating a Privacy Officer ensures that practices have one person who is aware of the scope of HIPAA and is charged with executing its rules.

Access to Information

Successfully meeting HIPAA's privacy regulations starts with an understanding of the terminology involved. Protected Health Information (PHI) is anything that can be used to identify a patient or encounter including the patient's name, address, social security number or phone numbers, whether or not they are combined with treatment-related information such as dates of service or diagnosis codes. PHI is also known as Individually Identifiable Health Information. Guarding this information from unauthorized or non-essential access is the core of HIPAA's privacy rules.
It is permissible under HIPAA to transmit or share data that has been de-identified. That means that all references to a specific, identifiable patient have been removed from all communications. HIPAA regulations specify 18 identifiers (including one that is all encompassing) that must be removed prior to transmitting data in an otherwise unencrypted form. Examples include name, address, phone number, and social security number. This process is useful for transmitting patient data for research purposes, but is obviously not appropriate for treatment or payment purposes.

Use of a limited data set (data that does not include a certain list of directly identifiable information and namely used for research, public health and health care operation purposes) provided with a signed "data use agreement" by the recipient of the limited data set, is permitted. The data use agreement spells out the permitted uses and disclosures of such information by the recipient, limits who can use or receive the data and requires the recipient to agree to not re-identify the data or contact the individuals.

Privacy Notice

HIPAA requires that healthcare providers give each patient a copy of as well as post a notice of the patient's rights (known as the Notice of Privacy Practices) regarding information privacy in a plainly visible location. The provider must also receive a written acknowledgement from the patient that they received a copy of a notice of your privacy practices. The notice must be provided to the patient at the same time as the delivery of service (if the service delivery was by telephone a notice must be

mailed to the patient the day of the phone call). The provider must make a "good faith" effort to obtain the written acknowledgement from the patient. If the patient refuses, is unwilling or is unable to provide such an acknowledgement, the provider must document the effort made to obtain the acknowledgement and keep that on file. This notice must include information about the patient's rights, and the procedure for filing grievances about breaches of these rights, both to the provider's office and with HHS's Office of Civil Rights. Further, this notice must be in plain language so it can be easily understood by the patient (i.e. not legalese).

It is especially important that this notice match the policies and procedures of the healthcare practice. Enforcement is expected to be especially stringent for those who post a policy and then do not follow it.

Types of communication impacted by privacy rules

HIPAA impacts all forms of communication about patient information. It is important to understand that the law is not intended to interfere with patient care or payment, but to protect against unauthorized disclosure of private information. Examples of ways that the law protects each patient's data in each type of communication include:

- **Electronic** – Patient information is protected against hackers through the security provisions
- **Written** – Patient information is protected by requiring adequate security of medical records, and limiting exposure of written information such as patient lists
- **Oral** – Patients are protected against casual conversations about their treatment or payment history between office staff within earshot of other patients
- **Fax** – Patients are protected against providers inadvertently sending a fax to the wrong location, thereby compromising their private information

As important as protecting privacy is, the law does not intend to interfere with providing patients the best care possible, paying providers for their services, or running the normal operations of a provider. HIPAA does not prohibit the communication of treatment or payment-related information. Instead, it insists that such communication be with the appropriate party and only include the minimum necessary information to achieve the specific goal of the communication. For example, HIPAA does not allow sharing of payment history with a provider to whom you are referring a patient for treatment, as that does not further the treatment goal. HIPAA does allow sharing payment information with the payer and treatment information with another covered entity for treatment of a mutual patient for a certain, specific treatment, i.e., it must be for the current treatment of the patient.

Common problems related to privacy

There are several common problems for small healthcare practices that arise from HIPAA's privacy rules.

- "Minimum Necessary" Rule - The "minimum necessary" rule requires thoughtful application of HIPAA rules to everyday communication. Establishing several security classes, and categorizing your relationships into them will make it easier to manage these privacy rules. For example, one security class might be referral providers. For those relationships that fall into this category, you would routinely provide all treatment-related information, including (possibly) the full medical record, but eliminate any payment or other unrelated information. Another category might be

payers, where the billing statement and selected supporting notes might be the limit of routinely shared information.

- Casual conversations – As part of the normal flow of an office, it is common to have casual conversations about those with whom we come in contact. Incidental disclosures of PHI are allowed but only if you make sure that you have taken "reasonable safeguards'" to protect your patients' health information and have followed a minimum necessary approach to the disclosure of PHI. HIPAA recognizes that doctors discuss things with their patients or confer with nurses or assistants at their stations. Conversations should be kept to a reasonable sound level and not easily heard by passers-by and should be held outside of the public's earshot whenever possible.
- Following your own rules – Some of HIPAA's restrictions related to privacy may be redundant at the local level, but HIPAA is largely about consistent application of a set of rules that are the same for all healthcare providers nationwide. HIPAA requires that certain items, like a privacy policy, be outwardly visible. However, the more important aspect is that these rules, once documented and posted, are followed consistently and uniformly. Enforcement is expected to be especially strict for those that post a policy and then do not follow it.

Strategies for HIPAA Privacy compliance

Protecting patient privacy is not an option under HIPAA. As much as HIPAA does to protect patient information privacy and provide them with access to their records, in many cases it does not go as far as the expectations of the public in protecting private information. For example, HIPAA privacy would allow a communication to patients with specific condition or treatment information prominently displayed as long as a few limited conditions are met. Most patient, however, would find such a public display of private information to be unacceptable.

The reason that HIPAA privacy regulations has mandated that you give your patients a copy of a notice of your privacy practices is so that you use them as an opportunity to engage patients fully in decisions related to their care and let them know that you are sensitive to their privacy concerns. It is also why you must prominently post your policies and use appropriate signage to inform patients that privacy precautions are being taken for their protection and their best interests.

Creating a culture which is sensitive to a patient's right to privacy is an important element of complying with HIPAA's privacy regulations.

Security

HIPAA's security regulations are not yet finalized. Final regulations are expected to be issued in Q4 of 2002 (or even possibly into the first quarter of 2003). The effective date of these regulations occurs 60 days after they are published in the Federal Register; enforcement occurs 2 years after their effective date.

Relationship between privacy and security

The security provisions of HIPAA are meant to support and work closely with the privacy provisions. In short, the security provisions are there to ensure that necessary steps are taken to limit unauthorized access to protected health information and to ensure that patients have a reasonable expectation that their information is being managed appropriately.

Security Officer

The Security officer is responsible for making sure that the HIPAA security regulations are followed. HIPAA provides numerous standards and requirements, but little in the way of technical direction. How HIPAA security is implemented will depend on each practice's particular hardware configuration, network capabilities and whether or not your computers are connected to the outside world through a modem or other connection. The Security Officer should be able to provide technical and organizational support to these requirements.

Physical security

HIPAA requires that reasonable steps be taken to secure your data and computer systems (although realistically you should include paper-based data as well) from physical tampering. This may include using/putting appropriate locks on doors, alarm systems and locking file cabinets where needed. Though you aren't mandated to use locked filing cabinets or rooms to house your records, you ARE responsible for safeguarding your patients PHI and a locked filing cabinet or putting a lock on a door to segregate your patients records may be the least costly solution you can implement.

Technical security – data

The data on your computers must be secured from viruses that would alter it, hackers that would disrupt or steal it, and any other unauthorized use through the use of passwords, anti-virus software, and other network security safeguards.

Technical security – transactions

Encryption, transmission validation and other means of verifying that what was sent was what was received are the subject of the section of the security regulations dealing with transaction security.

Disaster preparedness

The items required under the Disaster Preparedness section simply make good business sense regardless of the HIPAA requirements. These activities include making backups, having contingency and disaster recovery plans, and keeping adequate maintenance records.

Common problems related to security

The biggest challenges at this point with the HIPAA security regulations are two-fold: (1) the regulations are not yet final, and (2) the regulations require a significant upgrading of computer skills for many small providers. The fact that the regulations are only in draft form at this time should not impede providers from starting to implement them; we don't expect sweeping changes, and we don't expect the final regulations to be less restrictive than the proposed regulations, though that is possible. The issue of necessitating an upgrading of computer skills among healthcare provider staffs is a fact of the world in which we live. Because we all rely so completely on technology to conduct our businesses, we must also do the "hard part" of knowing how to safeguard it, because doing so also means safeguarding our businesses. Bottom line: even if the final HIPAA security regulations wouldn't require that you implement significant changes to your system security or upgrade your computer system you should be examining those aspects of your business anyway. Business improvements created by installing upgraded technology and securing your businesses data is something that will pay you pack multi-fold.

What Kind Of Providers Are Affected By HIPAA?

The easiest answer to this question is that all healthcare providers in the United States, regardless of size, are impacted by HIPAA regulations. Technically, you are only required to comply with HIPAA regulations if you are a covered entity (see definition included in the Glossary at the end of this document).

But, recent surveys and legislation enacted around privacy in the financial arena indicate that privacy (or loss of it) is one of, if not, the biggest concern(s) of the American public. Surveys suggest that at least 1/3 of all Americans are concerned more about the loss of their privacy than anything else. That means that 1 of every 3 patients that walk through your office door is concerned that you are employing privacy conscious practices, especially with regard to their health information. HIPAA is the way that this concern is being levied on the American health community but it is the public that is speaking. So, even if you aren't a covered entity, compliance with HIPAA is good for your practice and your patients. And, eventually, if you decide to perform electronic transactions or use a clearinghouse or data aggregator to submit information on your behalf you become a covered entity and are required to comply with the HIPAA regulations.

HIPAA reflects the prevailing standard of care for privacy and security of patient data. Special rules for mental health providers exist, reflecting the historically more stringent privacy regulations under which they have operated.

HIPAA Timeline

Transactions Deadline

The original deadline for compliance with electronic transaction standards is October 16, 2002. In early 2002, Congress granted an extension of this enforcement date to October 16, 2003 only for those covered entities who request it by October 15, 2002. For more information about filing for an extension see section 3.2.1.

Privacy

The enforcement date for privacy regulations is April 14, 2003. There is no delay or extension expected regarding this date.

Security

Final security rules have not yet been issued. They are expected to be substantially similar to the draft rules and are expected to be issued in final form in late 2002 (currently estimated to be Q4 of 2002). The enforcement date will be 2 years after the effective date of the final rules (the effective date is usually 60 days after the rules are published).

The HIPAA Project

HIPAA Coordinator

The HIPAA Coordinator is responsible for coordinating and integrating all of the activities surrounding HIPAA compliance. This may include assistance from others serving in the roles of Privacy Officer or Security Officer. The HIPAA Coordinator is supported by and leads the Task Force.

Project Plan

Coordinating and integrating compliance with HIPAA is a lengthy and complex project likely to last several months of total calendar time. While not a full time job, it does require significant coordination to ensure that all the appropriate elements are covered.

The HIPAA*Now!* toolkit provides step-by-step instructions to ensure that all necessary actions are taken. To that end, it is important that the HIPAA Coordinator review the entire toolkit to understand the complete scope of the HIPAA compliance process.

Penalties For Non-Compliance

HIPAA provides for numerous serious penalties, including:

- The penalty for non-compliance with transactions and code sets is $100 per occurrence up to a maximum of $25,000 per standard per year.
- The civil penalties for health plans, providers and clearinghouses that violate the privacy standards are $100 per incident, up to $25,000 per year, per standard.
- The federal criminal penalties for health plans, providers and clearinghouses include:
    - Up to $50,000 and/or one year in prison for obtaining or disclosing protected health information
    - Up to $100,000 and/or up to five years in prison for obtaining protected health information under "false pretenses"
    - Up to $250,000 and/or up to 10 years in prison for obtaining or disclosing protected health information with the intent to sell, transfer or use it for commercial advantage, personal gain or malicious harm.

Glossary of Terms

HIPAA has its own language; special terms that you need to understand in order to accomplish your compliance efforts. This glossary provides these specific definitions. Please note that these are working definitions (and not the exact legal definitions) that are easier to read and understand.

Business Associate	A person or organization that performs a function or activity on behalf of a *covered entity*, but is not part of the *covered entity's workforce*. A *business associate* can also be a *covered entity* in its own right.
Compliance date	The date by which a covered entity must comply with a standard, *implementation specification*, requirement, or *modification.* Usually 24 months after the effective date of a standard.
Chain of Trust	A term used in the HIPAA Security regulations for a pattern of agreements that extend protection of health care data by requiring that each *covered entity* that shares health care data with another entity require that that entity provide protections comparable to those provided by the *covered entity*, and that that entity, in turn, require that any other entities with which it shares the data satisfy the same requirements.
Code Set	Any set of codes used to encode *data elements*, such as tables of terms, medical concepts, medical diagnostic codes, or medical procedure codes. This includes both the codes and their descriptions.
Covered entity	(1) A health plan. (2) A health care clearinghouse. (3) A health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter.
Electronic Data Interchange (EDI)	Electronic exchange of formatted data using defined and accepted industry standards.
Effective Date	The date that a final rule is effective, usually 60 days after it is published in the Federal Register.
FAQ(s)	Frequently Asked Question(s).
HHS	The Department of Health and Human Services, the administrative body responsible for determining the HIPAA regulations and ensuring their enforcement.
Health care	Care, services, or supplies related to the health of an individual. *Health care* includes, but is not limited to: (1) Preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status, of an individual or that affects the structure or function of the body; and (2) Sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription.
Health care Clearinghouse	A public or private entity, including a billing service, repricing company, community health management information system or community health information system, and "value-added" networks and switches, that does either of the following functions: (1) Processes or facilitates the processing of health information received

	from another entity in a nonstandard format or containing nonstandard data content into standard *data elements* or a standard transaction. (2) Receives a standard transaction from another entity and processes or facilitates the processing of health information into nonstandard format or nonstandard data content for the receiving entity.
Health care provider	A provider of services (as defined in section 1861(u) of the Act, 42 U.S.C. 1395x(u)), a provider of medical or health services (as defined in section 1861(s) of the Act, 42 U.S.C. 1395x(s)), and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business.
Health information	Any information, whether oral or recorded in any form or medium, that: (1) Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and (2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.
Health Care Operations	The use of PHI is restricted by the privacy rule, except for treatment, payment and Health Care Operation activities. Health care operations, as defined by the statute, include: (1) conducting quality assessment and improvement activities (2) accrediting/licensing of health care professionals (3) evaluating health care professional performance (4) training future health care professionals (5) activities relating to the renewal of a contract for insurance (6) conducting or arranging for medical review and auditing services (7) compiling and analyzing information for use in a civil or criminal legal proceeding
Implementation specification	Specific requirements or instructions for implementing a standard.
Incidental Use & Disclosure	Unintended uses and disclosures of PHI that occur as a byproduct of a use or disclosure otherwise permitted under the Privacy Rule. An incidental use or disclosure is permissible only to the extent that the covered entity has applied reasonable safeguards as required by the regulations and has implemented the minimum necessary standard, where applicable, as required by the regulations.
Individually identifiable data	Data that can be readily associated with a specific individual. Examples would be a name, a personal identifier, or a full street address. Includes data that alone could not identify an individual, could collectively identify an individual.
Limited Data Set and Data Use Agreement	A set of limited data which has been de-identified of all of the facially identifying information and a few other direct identifiers. For a covered entity to disclose a limited data set to a recipient they must first obtain a "data use agreement" from the recipient of the data. The data use agreement spells out the terms under which the recipient agrees to use or receive the data. It also includes similar language to the Business Associate agreement to ensure that the recipient uses appropriate

Limited Data Set and Data Use Agreement (continued)	Associate agreement to ensure that the recipient uses appropriate safeguards to prevent use or disclosure of the limited data set other than as permitted by the HIPAA regulations.
Marketing communications	Marketing is defined as follows: To make a communication about a product or service that encourages the recipients of the communication to purchase or use the product or service. There are three categories of communications that are excluded from the definition of marketing (which means that the covered entity is not engaged in marketing when it communicates to individuals about: (1) The participating providers and health plans in a network, the services offered by a provider, or the benefits covered by a health plan; (2) the individual's treatment; or (3) case management or care coordination for that individual, or directions or recommendations for alternative treatments, therapies, health care providers, or settings of care to that individual. For example, a doctor that writes a prescription or refers an individual to a specialist for follow-up tests is engaged in a treatment communication and is not marketing a product or service.
"Minimum Necessary" Rule or Minimum Scope of Disclosure	The principle that, to the extent practical, individually identifiable health information should only be disclosed to the extent needed to support the purpose of the disclosure.
Office for Civil Rights (OCR)	The entity within the Department of Health and Human Services (HHS) responsible for enforcing the HIPAA privacy rules.
Payer	An entity that assumes the risk of paying for medical treatments. This can be an uninsured patient, a self-insured employer, a health plan, or an HMO.
Protected Health Information (PHI)	Individually identifiable health information that is transmitted or maintained in any form or medium, including electronic, written, oral or other.
Standard	A rule, condition, or requirement: (1) Describing the following information for products, systems, services or practices: (i) Classification of components. (ii) Specification of materials, performance, or operations; or (iii) Delineation of procedures; or (2) With respect to the privacy of individually identifiable health information.
Standard setting organization (SSO)	An organization accredited by the American National Standards Institute that develops and maintains standards for information transactions or data elements, or any other standard that is necessary for, or will facilitate the implementation of, these regulations.
Trading partner agreement	An agreement related to the exchange of information in electronic transactions, whether the agreement is distinct or part of a larger agreement, between each party to the agreement. (For example, a trading partner agreement may specify, among other things, the duties and responsibilities of each party to the agreement in conducting a standard transaction.)
Transaction	The transmission of information between two parties to carry out financial or administrative activities related to health care. It includes the

	following types of information transmissions: (1) Health care claims or equivalent encounter information. (2) Health care payment and remittance advice. (3) Coordination of benefits. (4) Health care claim status. (5) Enrollment and disenrollment in a health plan. (6) Eligibility for a health plan. (7) Health plan premium payments. (8) Referral certification and authorization. (9) First report of injury. (10) Health claims attachments. (11) Other transactions that the Secretary may prescribe by regulation.
Workforce	Employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity.