Appendix 1.1

# Definitions of Key Terms (plain language)

The following simplified definitions are based on the laws and regulations indicated in the number at the end of each definition. Information that is unlikely to apply to dental practices has been omitted from some of the definitions. Refer to Appendix 1.2 (or to the statutes and regulations themselves) for the official definitions. HIPAA definitions change from time to time as new statutes and regulations are adopted. The following definitions are based on laws and regulations that were current as of March 26, 2013.

**Access.** In general, "access" means the ability to obtain, use or disclose patient information. When used in connection with HIPAA Security, "access" means the ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any system resource. **45 CFR § 164.304**

Under the HIPAA Privacy Rule, a patient's right of "access" means the patient's right to see and get copies of his or her patient records. **45 CFR § 164.524**

**Addressable.** When an implementation specification under the HIPAA Security Rule is "addressable," a dental practice must do the following:

1. The dental practice must assess whether the implementation specification is a reasonable and appropriate safeguard in the dental practice's environment (the dental practice must consider whether the implementation specification is likely to contribute to protecting the dental practice's electronic patient information).
2. If the implementation specification ***is*** reasonable and appropriate, the dental practice must implement the implementation specification.
3. If the implementation specification ***is not*** reasonable and appropriate, the dental practice must:
    a. document why it would not be reasonable and appropriate to implement the implementation specification, and
    b. implement an equivalent alternative measure, if the equivalent alternative measure would be reasonable and appropriate.

Business associates and subcontractors must also comply with the HIPAA Security administrative, physical and technical safeguards, so they, too, must go through this process.

**Administrative safeguards.** The HIPAA Security rule requires dental practices to have certain *administrative, physical* and *technical* safeguards in place. Administrative safeguards, such as conducting a written risk assessment and providing workforce training, are administrative actions and policies and procedures that a dental practice uses to manage the selection, development, implementation, and maintenance of security measures to protect electronic patient information and to manage the conduct of the dental practice's workforce in protecting patient information. **45 CFR § 164.304**

**ANSI** stands for the American National Standards Institute. **45 CFR § 160.103**

**Authentication** means corroborating that a person is the person whom he or she claims to be (for example, a person trying to log onto a dental practice's electronic dental record system). **45 CFR § 164.304**

**Availability** means that data or information is accessible and useable upon demand by an authorized person. **45 CFR § 164.304**

**Breach** has two meanings under HIPAA:

1. *Under the Breach Notification Rule*, a "breach" generally means that someone or something acquired, accessed, used or disclosed unsecured patient information in a way that the Privacy Rule does not permit, which compromised the security or privacy of the patient information. Examples of breaches include the loss or theft of a laptop that contains unsecured electronic patient information, disposing of paper patient records in the regular trash without properly shredding them first, and mailing patient information to the wrong address. There are three exceptions to the definition of breach.

   A dental practice must send notification of a breach of unsecured patient information to affected patients, the federal government, and in some cases the media, unless the dental practice can demonstrate that there is a low probability that the information was compromised by conducting a written assessment of the relevant factors, including at least the four required factors.[1] **45 CFR § 164.402**

2. *Breach of the business associate agreement* means violation of a provision in the agreement. For example, a business associate has breached the agreement if the business associate is aware of a "security incident" but does not notify the dental practice. If a business associate breaches the business associate agreement the dental practice may take legal action for breach of contract and HHS can impose civil money penalties directly on the business associate.

**Business associate** generally means an entity, or a person who is not a member of the dental practice's workforce, that performs a service for the dental practice involving patient information. Examples of business associates include a billing service, collection agency, accounting or law firm; consultant, health information organization, e-prescribing gateway, data transmission company that requires access to patient information on a routine basis; and a company that offers patients personal health records on behalf of the dental practice. A dental practice must have a business associate agreement in place with each of the dental practice's business associates. A business associate's subcontractor that has access to patient information is treated as a downstream business associate (see definition of "subcontractor"). A business associate must have a business associate agreement in place with each of the business associate's subcontractors.

A health care provider, such as a dental laboratory, does not become a business associate when a dental practice discloses patient information to the health care provider for treatment purposes. However, a health care provider may be a business associate of a dental practice if the health care provider performs a service for the dental practice rather than providing treatment for a patient. For example, a dental practice would need a business associate agreement with a health care provider that accesses the dental practice's patient information for purposes of providing training to the dental practice's workforce. **45 CFR § 160.103**

[1] (i) The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;
(ii) The unauthorized person who used the protected health information or to whom the disclosure was made;
(iii) Whether the protected health information was actually acquired or viewed; and
(iv) The extent to which the risk to the protected health information has been mitigated.

**Civil money penalty or penalty** means the penalty amount (in dollars) that the federal government may impose for a HIPAA violation. **45 CFR § 160.103**

**CMS** stands for Centers for Medicare & Medicaid Services, an agency within the U.S. Department of Health and Human Services. **45 CFR § 160.103**

**Code set** means any set of codes used to encode data elements, such as tables of terms, medical concepts, medical diagnostic codes, or medical procedure codes. A code set includes the codes and the descriptors of the codes. **45 CFR § 162.103**

**Code set maintaining organization** means an organization that creates and maintains the code sets adopted by the Secretary for use in the transactions for which standards are adopted in this part. **45 CFR § 162.103**

**Common control** exists if an entity has the power, directly or indirectly, to significantly influence or direct the actions or policies of another entity. **45 CFR § 164.103**

**Common ownership** exists if an entity or entities possess an ownership or equity interest of 5 percent or more in another entity. **45 CFR § 164.103**

**Compliance date** means the date by which a dental practice or business associate must comply with a HIPAA provision or a change to a HIPAA provision. **45 CFR § 160.103**

**Confidentiality** means the information is not made available or disclosed to unauthorized persons or processes. **45 CFR § 164.304**

**Contrary.** HIPAA does not preempt "contrary" state law that relates to the privacy of patient information if the state law is more stringent than HIPAA. This means that a dental practice must comply with both HIPAA and any state law (for example, a state medical privacy law or a state data security law) that is contrary to HIPAA and more stringent than HIPAA. "Contrary" means that a dental practice would find it impossible to comply with both the state and the federal requirement, or that the state law would be an obstacle to accomplishing the purpose of the federal law. "More stringent" means that the state law gives more protection to patient information, or gives individuals more rights over patient information. **45 CFR § 160.202**

**Correctional institution** means a jail, reformatory, detention center, work farm, halfway house, residential community program center, or other penal or correctional facility operated for the confinement or rehabilitation of persons charged with or convicted of a crime, or "other persons held in lawful custody." A correctional institution may be operated by or under contract to the U.S., a state, territory, political subdivision of a state or territory, or an Indian tribe. "Other persons held in lawful custody" includes juvenile offenders adjudicated delinquent, aliens detained awaiting deportation, persons committed to mental institutions through the criminal justice system, witnesses, or others awaiting charges or trial. **45 CFR § 164.501**

**Covered Entity** means:

1. A health plan.
2. A health care clearinghouse.
3. A health care provider (such as a dental practice) that transmits any health information in electronic form in connection with a transaction covered by HIPAA. **45 CFR § 160.103**

**Covered functions** means those functions of a dental practice that make the practice a health care provider. **45 CFR § 164.103**

**Data aggregation** means that a business associate will combine a dental practice's patient information with patient information of other covered entities (such as other dental practices) to permit data analyses that relate to the health care operations of the respective covered entities. **45 CFR § 164.501**

**Data element** means the smallest named unit of information in a transaction. **45 CFR § 162.103**

**Data set** means a semantically meaningful unit of information exchanged between two parties to a transaction. **45 CFR § 162.103**

**De-identified.** In general, patient information is "de-identified" if 18 identifiers (name, address, etc.) are removed, and the remaining information cannot be used alone or in combination with other information to identify the patient. HIPAA does not apply to properly de-identified information.

**Descriptor** means the text defining a code. **45 CFR § 162.103**

**Designated record set** means a group of records maintained by or for a dental practice that is:

a. the medical records and billing records about patients maintained by or for the dental practice, or

b. used, in whole or in part, by or for the dental practice to make decisions about patients.

For purposes of this definition, the term "record" means any item, collection, or grouping of information that includes patient information and is maintained, collected, used, or disseminated by or for the dental practice. **45 CFR § 164.501**

**Direct treatment relationship** means a treatment relationship between a patient and a health care provider that is not an indirect treatment relationship. **45 CFR § 164.501**

**Direct data entry** means the direct entry of data (for example, using dumb terminals or web browsers) that is immediately transmitted into a health plan's computer. **45 CFR § 162.103**

**Disclosure** means releasing, transferring, providing access to, or divulging information in any manner outside the dental practice or other entity holding the information. **45 CFR § 160.103**

**Electronic health record (EHR)** means an electronic record of health-related information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff. **HITECH Act, § 13400**

**Electronic media** means:

1. Electronic storage media on which data is or may be recorded electronically, such as computer hard drives and removable/transportable memory medium, such as USB drives, CD-ROMs, digital memory cards, magnetic tape or disks, and optical disks.

2. Transmission media used to exchange information already in electronic storage media, such as the Internet, extranet, or intranet, leased lines, dial-up lines, private networks, and the physical movement of removable or transportable electronic storage media. Certain transmissions, including of paper, via fax, and of voice, via telephone, are not considered to be "transmissions via electronic media" if the information being exchanged did not exist in electronic form before the transmission. **45 CFR § 160.103**

**Electronic protected health information** means protected health information (patient information) that is transmitted by electronic media or maintained in electronic media. Examples include patient information on a desktop or laptop, in an electronic dental record, in an electronic practice management system, in an email, in an electronic document (such as Word or .pdf), or on removable media such as a CD-ROM or a USB drive. **45 CFR § 160.103**

**Employer** is defined as it is in the federal law governing withholding taxes, 26 U.S.C. 3401(d). **45 CFR § 160.103**

**Encryption** means the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key. **45 CFR § 164.304**

**Facility** means the physical premises and the interior and exterior of a building(s). **45 CFR § 164.304**

**Family member** means a person's dependent, which means someone who is or may become eligible for coverage under the terms of a group health plan because of a relationship to a participant, or one of the following relatives by marriage, adoption, or blood (blood relatives include partial blood relatives, such as half-siblings):

- Parents, spouses, siblings, and children.
- Grandparents, grandchildren, aunts, uncles, nephews, and nieces.
- Great-grandparents, great-grandchildren, great aunts, great uncles, and first cousins.
- Great-great grandparents, great-great grandchildren, and children of first cousins. **45 CFR § 160.103**

**Format** refers to those data elements that provide or control the enveloping or hierarchical structure, or assist in identifying data content of, a transaction. **45 CFR § 162.103**

**Genetic information** means information about the following that pertains to (1) a patient, (2) a family member of a patient (see definition of "family member"), (3) a fetus carried by the patient or a family member of a patient, or (4) an embryo legally held by a patient or a patient's family member using an assisted reproductive technology:

- A genetic test (see definition of "genetic test").
- Request for genetic services (see definition of "genetic services").
- Receipt of genetic services (see definition of "genetic services").
- Participation in clinical research which includes genetic services.

Genetic information also includes the manifestation of a disease or disorder in family members of a patient (see definition of "manifested").

Genetic information does not include information about the sex or age of any patient. **45 CFR § 160.103**

**Genetic services** means:

1. A genetic test.
2. Genetic counseling (including obtaining, interpreting, or assessing genetic information).
3. Genetic education. **45 CFR § 160.103**

**Genetic test** means an analysis of human DNA, RNA, chromosomes, proteins, or metabolites, if the analysis detects genotypes, mutations, or chromosomal changes. Genetic test does not include an analysis of proteins or metabolites that is directly related to a manifested disease, disorder, or pathological condition. **45 CFR § 160.103**

**HHS** stands for the U.S. Department of Health and Human Services. **45 CFR § 160.103**

**Health care** means care, services, or supplies related to the health of an individual. Health care includes, but is not limited to, the following:

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. **45 CFR § 160.103**

**Health care clearinghouse** means 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. **45 CFR § 160.103**

**Health care operations.** The definition of health care operations is important because HIPAA generally permits a dental practice to use and disclose patient information for health care operations purposes without having the patient sign a written authorization form. However, there are exceptions, such as subsidized marketing communications and sale of patient information.

"Health care operations" is a broad category of dental practice activities such as business management and general administrative activities of the dental practice (for example, HIPAA compliance, customer service, resolving internal grievances, the sale of the practice to another covered entity (or to an entity that will become a covered entity following the sale) and due diligence related to the sale, and de-identifying PHI). Other examples include business planning and development (such as cost-management and planning related analyses), conducting quality assessment and improvement activities, certain patient safety activities, case management and care coordination, reviewing the competence or qualifications of health care professionals, conducting training programs in which health care students, trainees, or practitioners learn under supervision, training of non-health care professionals, licensing and credentialing activities, arranging for legal services, and auditing (including fraud and abuse detection and compliance programs). To determine whether an activity is a health care operation, consult the full definition in **45 CFR 160.103**.

**Health care provider** means a person or organization that furnishes, bills, or is paid for health care in the normal course of business. Dental practices and dental laboratories providing treatment to patients are examples of health care providers. **45 CFR § 160.103**

**Health information** means any information, including genetic 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. **45 CFR § 160.103**

**Health information technology** means hardware, software, integrated technologies or related licenses, intellectual property, upgrades, or packaged solutions sold as services that are designated for or support the use by health care entities or patients for the electronic creation, maintenance, access, or exchange of health information. **HITECH Act, § 3000**

**Health oversight agency** means an agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, or a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is authorized by law to oversee the health care system (whether public or private) or government programs in which health information is necessary to determine eligibility or compliance, or to enforce civil rights laws for which health information is relevant. **45 CFR § 164.501**

**Health plan** generally means an individual or group plan or combination of plans that provides or pays for the cost of medical care. Examples of health plans include employee welfare benefit plans, HMOs, Medicare, the Medicare Advantage program, an issuer of a Medicare supplemental policy, Medicaid, an approved State child health plan, the veterans health care program, CHAMPUS, the Indian Health Service, and the Federal Employees Health Benefits Program. Health plan also includes the Medicare Voluntary Prescription Drug Program (Medicare Part D), and issuers of certain long-term care policies.

Health plan generally excludes accident/disability income insurance, liability insurance (including auto) and supplements to liability insurance, worker's comp, auto medical payment insurance, credit-only insurance, coverage for on-site medical clinics, and government-funded programs (except the ones listed above) whose principal purpose is not providing, or paying the cost of, health care, or whose principal activity is directly providing health care to persons or making grants to fund the direct provision of health care to persons. **45 CFR § 160.103**

**Implementation specification** means specific requirements or instructions for implementing a standard. **45 CFR § 160.103**

**Indirect treatment relationship.** An example of an "indirect treatment relationship" is where (1) a health care provider provides health care to patients based on orders of a dental practice, and (2) typically, the health care provider provides services or products, or reports the diagnosis or results, directly to the dental practice, and the dental practice provides the services, products, or reports to the patients. **45 CFR § 164.501**

**Individual** means the person who is the subject of protected health information. For a dental practice, the individual usually means the patient. **45 CFR § 160.103**

**Individually identifiable health information** is health information, including demographic information such as names, addresses, genders, etc., and genetic information, that (1) is created or received by a health care provider, health plan, employer, or health care clearinghouse, and (2) relates to the past, present, or future physical or mental health or condition of a patient; the provision of health care to a patient; or the past, present, or future payment for the provision of health care to a patient, and (3) that identifies the patient or could be used to identify the patient. **45 CFR § 160.103**

**Information system** means an interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people. **45 CFR § 164.304**

**Integrity** means that data or information have not been changed or destroyed in an unauthorized manner. **45 CFR § 164.304**

**Law enforcement official** means an officer or employee of any agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, who is empowered by law to:

1. Investigate or conduct an official inquiry into a potential violation of law; or
2. Prosecute or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law. **45 CFR § 164.103 & 164.501**

**Maintain or maintenance,** when used in the HIPAA Security Rule, refers to activities necessary to support the use of a standard adopted by HHS, including technical corrections to an implementation specification, and enhancements or expansion of a code set. This term excludes the activities related to the adoption of a new standard or implementation specification, or modification to an adopted standard or implementation specification. **45 CFR § 162.103**

**Malicious software** means software, for example, a virus, designed to damage or disrupt a system. **45 CFR § 164.304**

**Manifestation or manifested** means that a person has been, or could reasonably be, diagnosed with a disease or disorder by a health care professional with appropriate training and expertise in appropriate the field of medicine. For HIPAA purposes, a disease, disorder, or pathological condition is not "manifested" if the diagnosis is based principally on genetic information. **45 CFR § 160.103**

**Marketing** means to make a communication about a product or service that encourages recipients of the communication to purchase or use the product or service. However, marketing does not include: (1) certain communications made for treatment, case management, or care coordination purposes *unless* the dental practice receives "financial remuneration" (dollars) in exchange for making the communication, and (2) certain refill reminders. With certain exceptions, if a dental practice will receive financial remuneration for making a marketing communication, the dental practice must have patients sign HIPAA-compliant authorization forms that state that the dental practice will receive financial remuneration for making the communication. **45 CFR § 164.501**

**Maximum defined data set** means all of the required data elements for a particular standard based on a specific implementation specification. **45 CFR § 162.103**

**More stringent.** A state law is more stringent than HIPAA if the state law:

1. prohibits or restricts a use or disclosure that would be permitted under HIPAA (unless the disclosure is to the patient about his or her own information, or to HHS for determining HIPAA compliance).
2. gives patients greater rights than HIPAA to see or get copies of their records, or ask the dental practice to change information in their records.
3. gives patients greater rights to information about a use, disclosure, rights, and remedies than HIPAA.
4. with respect to authorization forms and other legal permissions from patients, has narrower scope or duration, more privacy protections, or less coercive effect of the circumstances surrounding the permission than HIPAA.

5. requires dental practices to retain or report more detailed information, or to retain or report information for a longer period of time, than HIPAA's recordkeeping or accounting of disclosures requirements.

6. With respect to any other matter, provides greater privacy protection for the individual who is the subject of the patient information. **45 CFR § 160.202**

**National Coordinator** means the head of the Office of the National Coordinator for Health Information Technology established under section 3001(a). **HITECH Act, § 3000**

**Payment** generally means the dental practice's activities to obtain reimbursement or compensation for service performed or products provided and a health plan's activities to collect premiums, determine the plan's responsibility to provide coverage and benefits, and provide coverage and benefits. Examples of "payment" activities include things like determinations of eligibility or coverage, coordination of benefits, determination of cost sharing amounts, billing, claims management, collection activities, review of medical necessity, coverage, appropriateness of care or justification of charges, utilization review, including precertification and preauthorization, concurrent and retrospective review of services, and disclosure of limited information to consumer reporting agencies relating to collection of premiums or reimbursement (names and addresses, date of birth, Social Security number, payment history, account number, and name/address of health care provider and/or health plan). **45 CFR § 164.501**

**Physical safeguards.** The HIPAA Security rule requires dental practices to have certain *administrative, physical* and *technical* safeguards in place. Physical safeguards, such as door locks, workstation use and security, and disposal of electronic hardware and software, are physical measures, policies, and procedures to protect a dental practice's electronic information systems and related buildings and equipment from natural and environmental hazards and unauthorized intrusion. **45 CFR § 164.304**

**Privacy Official** means the person the dental practice designates to develop and implement the dental practice's policies and procedures to comply with the Privacy Rule.
**45 CFR § 164.530(a)(1)(i)**

**Privacy Rule** means the HIPAA Privacy Rule. **45 CFR § 164.500 through 45 CFR § 164.532**

**Protected health information ("PHI")** generally means patient information, including demographic information (names, addresses, genders, etc.), genetic information (see definition of "genetic information"), dental records, billing records, and any other information in the dental practice about a patient's health, treatment, or payment for health care. PHI includes information in any form or format, such as electronic, hard copy (paper records, photos, films, etc.) and spoken information. PHI does not include properly de-identified information (Chapter 2, Step 21), or information about a patient who has been deceased for 50 years or more (Chapter 1.H.1) The definition of PHI also excludes certain education records, and employment records held by a dental practice in its role as employer. **45 CFR § 160.103**

**Psychotherapy notes** means notes recorded (in any medium) by a health care provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session and that are separated from the rest of the individual's medical record. Psychotherapy notes excludes medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of the following items: diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date. **45 CFR § 164.501**

**Public health authority** means an agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, or a person or entity acting under a grant of authority from, or contract with, such public agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is responsible for public health matters as part of its official mandate. **45 CFR § 164.501**

**Reasonable cause** means an act or omission in which a dental practice or business associate knew, or by exercising reasonable diligence would have known, that the act or omission violated a HIPAA provision, but in which the dental practice or business associate did not act with willful neglect. **45 CFR § 160.401**

**Reasonable diligence** means the business care and prudence expected from a person seeking to satisfy a legal requirement under similar circumstances. **45 CFR § 164.401**

**Required.** When a HIPAA Security Rule standard includes a "required" implementation specification, a dental practice must implement the implementation specification. Business associates and subcontractors must also comply with the HIPAA Security administrative, physical and technical safeguards, so they, too, must go through this process. **45 CFR § 164.306(d)**

**Required by law** means a mandate contained in law that requires a dental practice to use or disclose patient information and that is enforceable in a court of law. Examples of uses and disclosures required by law includes court orders and court-ordered warrants, subpoenas and summons, Medicare conditions of participation, and statutes or regulations that require patient information if a dental practice seeks payment under a government program providing public benefits. **45 CFR § 164.103**

**Research** means a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge. **45 CFR § 164.501**

**Secretary** means the Secretary of the U.S. Department of Health and Human Services ("HHS") or any other officer or employee of HHS to whom the authority involved has been delegated. **45 CFR § 160.103**

**Secured.** If patient information is properly "secured," a dental practice does not need to send breach notification if the information is lost or stolen, or used, disclosed, accessed or acquired in violation of the Privacy Rule. Electronic patient information can be secured through appropriate encryption. Hard copy patient information cannot be secured except though appropriate destruction. Encryption and destruction requirements are in the Breach Notification Rule *Guidance*. **45 CFR § 164.402**

**Security or Security measures** encompass all of the administrative, physical, and technical safeguards in an information system. **45 CFR § 164.304**

**Security incident** means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. **45 CFR § 164.304**

**Security Official** means the person a dental practice designates to develop and implement the policies and procedures required by the Security Rule. Business associates and subcontractors must also designate Security Officials. **45 CFR § 164.308(a)(2)**

**Standard** means a rule, condition, or requirement under the HIPAA Security or Privacy Rule. **45 CFR § 160.103**

**Standard transaction** means a transaction that complies with an applicable standard adopted under the Administrative Requirements of the HIPAA regulations. **45 CFR § 162.103**

**State.** Under HIPAA, "state" generally means any of the U.S. states, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, and Guam, American Samoa and the Commonwealth of the Northern Mariana Islands. For a health plan established or regulated by Federal law, "state" has the meaning set forth in the applicable section of the United States Code for such health plan. **45 CFR § 160.103**

**State law** means a constitution, statute, regulation, rule, common law, or other State action having the force and effect of law. **45 CFR § 160.202**

**Subcontractor.** A person or entity is a "subcontractor" of a business associate if a business associate delegates a function, activity, or service to the person or entity; however, the business associate's workforce members are not subcontractors. **45 CFR § 160.103**

**Technical safeguards.** The HIPAA Security rule requires dental practices to have certain *administrative, physical* and *technical* safeguards in place. Technical safeguards, such as unique usernames, automatic logoff, and encryption, means the technology, and the policy and procedures for its use, that protect electronic patient information and control access to it. **45 CFR § 164.304**

**Transaction** means 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. **45 CFR § 160.103**

**Treatment** means providing, coordinating, or managing health care and related services by one or more health care providers, including coordinating or managing health care by a health care provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another. **45 CFR § 164.501**

**Unsecured.** See "Secured."

**Use** means, with respect to patient information, the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information. **45 CFR § 160.103**

**User** means a person or entity with authorized access. **45 CFR § 164.304**

**Violation or violate** means, as the context may require, failure to comply with a HIPAA provision. **45 CFR § 160.103**

**Willful neglect** means conscious, intentional failure or reckless indifference to the obligation to comply with the HIPAA provision that was violated. **45 CFR § 160.401**

**Workforce.** A dental practice's workforce means employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a dental practice, is under the direct control of the dental practice, whether or not they are paid by the dental practice. A business associate's workforce means the business associate's employees, volunteers, trainees, and other persons whose conduct, in the performance of work for the business associate, is under the direct control of the business associate, whether or not they are paid by the business associate. **45 CFR § 160.103**

**Workstation** means an electronic computing device, for example, a laptop or desktop computer, or any other device that performs similar functions, and electronic media stored in its immediate environment. **45 CFR § 164.304**

# Appendix 1.2
# Definitions of Key Terms (regulatory language)

The following HIPAA definitions of key terms are current as of March 26, 2013. The definitions are from the Code of Federal Regulations ("CFR") Title 45, Subtitle A, Subchapter C, Parts 160, 162 and 164. A copy of these regulations can be found online in the *Electronic Code of Federal Regulations* at *http://ecfr.gpoaccess.gov*.

At the end of each definition, in bold, is a number that indicates the statute or regulation where the definition is located. For example, the definition of "administrative safeguards" can be found in **45 CFR § 164.304.**

For simplified versions of definitions, see Appendix 1.1, "Definitions of Key Terms." The definitions in Appendix 1.1 have been simplified and paraphrased, and in some cases information is omitted that is unlikely to apply to most dental practices.

HIPAA definitions change from time to time as new statutes and regulations are adopted.

**Access** means the ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any system resource. (This definition applies to "access" as used in this subpart, not as used in subparts D or E of this part.) **45 CFR § 164.304**

**Act** means the Social Security Act. **45 CFR § 160.103**

**Administrative safeguards** are administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity's or business associate's workforce in relation to the protection of that information. **45 CFR § 164.304**

**Administrative simplification provision** means any requirement or prohibition established by:

(1) 42 U.S.C. 1320d-1320d-4, 1320d-7, 1320d-8, and 1320d-9;

(2) Section 264 of Pub. L. 104-191;

(3) Sections 13400-13424 of Public Law 111-5; or

(4) This subchapter. **45 CFR § 160.103**

**ALJ** means Administrative Law Judge. **45 CFR § 160.103**

**ANSI** stands for the American National Standards Institute. **45 CFR § 160.103**

**Authentication** means the corroboration that a person is the one claimed. **45 CFR § 164.304**

**Availability** means the property that data or information is accessible and useable upon demand by an authorized person. **45 CFR § 164.304**

**Board** means the members of the HHS Departmental Appeals Board, in the Office of the Secretary, who issue decisions in panels of three. **45 CFR § 160.502**

**Breach** means the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part which compromises the security or privacy of the protected health information.

(1) Breach excludes:

(i) Any unintentional acquisition, access, or use of protected health information by a workforce member or person acting under the authority of a covered entity or a business associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under subpart E of this part.

(ii) Any inadvertent disclosure by a person who is authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health information at the same covered entity or business associate, or organized health care arrangement in which the covered entity participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under subpart E of this part.

(iii) A disclosure of protected health information where a covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to
retain such information.

(2.) Except as provided in paragraph (1) of this definition, an acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment of at least the following factors:

(i) The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;

(ii) The unauthorized person who used the protected health information or to whom the disclosure was made;

(iii) Whether the protected health information was actually acquired or viewed; and

(iv) The extent to which the risk to the protected health information has been mitigated.
**45 CFR § 164.402**

**Business associate:**

(1) Except as provided in paragraph (4) of this definition, business associate means, with respect to a covered entity, a person who:

(i) On behalf of such covered entity or of an organized health care arrangement (as defined in this section) in which the covered entity participates, but other than in the capacity of a member of the workforce of such covered entity or arrangement, creates, receives, maintains, or transmits protected health information for a function or activity regulated by this subchapter, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, patient safety activities listed at 42 CFR 3.20, billing, benefit management, practice management, and repricing; or

(ii) Provides, other than in the capacity of a member of the workforce of such covered entity, legal, actuarial, accounting, consulting, data aggregation (as defined in § 164.501 of this subchapter), management, administrative, accreditation, or financial services to or for such covered entity, or to or for an organized health care arrangement in which the covered entity participates, where the provision of the service involves the disclosure of protected health information from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the person.

(2) A covered entity may be a business associate of another covered entity.

(3) Business associate includes:

(i) A Health Information Organization, E-prescribing Gateway, or other person that provides data transmission services with respect to protected health information to a covered entity and that requires access on a routine basis to such protected health information.

(ii) A person that offers a personal health record to one or more individuals on behalf of a covered entity.

(iii) A subcontractor that creates, receives, maintains, or transmits protected health information on behalf of the business associate.

4. Business associate does not include:

(i) A health care provider, with respect to disclosures by a covered entity to the health care provider concerning the treatment of the individual.

(ii) A plan sponsor, with respect to disclosures by a group health plan (or by a health insurance issuer or HMO with respect to a group health plan) to the plan sponsor, to the extent that the requirements of § 164.504(f) of this subchapter apply and are met.

(iii) A government agency, with respect to determining eligibility for, or enrollment in, a government health plan that provides public benefits and is administered by another government agency, or collecting protected health information for such purposes, to the extent such activities are authorized by law.

(iv) A covered entity participating in an organized health care arrangement that performs a function or activity as described by paragraph (1)(i) of this definition for or on behalf of such organized health care arrangement, or that provides a service as described in paragraph (1)(ii) of this definition to or for such organized health care arrangement by virtue of such activities or services. **45 CFR § 160.103**

**Civil money penalty or penalty** means the amount determined under **§ 160.404** of this part and includes the plural of these terms. **45 CFR § 160.103**

**CMS** stands for Centers for Medicare & Medicaid Services within the Department of Health and Human Services. **45 CFR § 160.103**

**Code set** means any set of codes used to encode data elements, such as tables of terms, medical concepts, medical diagnostic codes, or medical procedure codes. A code set includes the codes and the descriptors of the codes. **45 CFR § 162.103**

**Code set maintaining organization** means an organization that creates and maintains the code sets adopted by the Secretary for use in the transactions for which standards are adopted in this part. **45 CFR § 162.103**

**Common control** exists if an entity has the power, directly or indirectly, significantly to influence or direct the actions or policies of another entity. **45 CFR § 164.103**

**Common ownership** exists if an entity or entities possess an ownership or equity interest of 5 percent or more in another entity. **45 CFR § 164.103**

**Compliance date** means the date by which a covered entity or business associate must comply with a standard, implementation specification, requirement, or modification adopted under this subchapter. **45 CFR § 160.103**

**Confidentiality** means the property that data or information is not made available or disclosed to unauthorized persons or processes. **45 CFR § 164.304**

**Contrary,** when used to compare a provision of State law to a standard, requirement, or implementation specification adopted under this subchapter, means:

(1) A covered entity or business associate would find it impossible to comply with both the State and Federal requirements; or

(2) The provision of State law stands as an obstacle to the accomplishment and execution of the full purposes and objectives of part C of title XI of the Act, section 264 of Public Law 104-191, or sections 13400-13424 of Public Law 111-5, as applicable. **45 CFR § 160.202**

**Correctional institution** means any penal or correctional facility, jail, reformatory, detention center, work farm, halfway house, or residential community program center operated by, or under contract to, the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, for the confinement or rehabilitation of persons charged with or convicted of a criminal offense or other persons held in lawful custody. *Other persons* held in lawful custody includes juvenile offenders adjudicated delinquent, aliens detained awaiting deportation, persons committed to mental institutions through the criminal justice system, witnesses, or others awaiting charges or trial. **45 CFR § 164.501**

**Covered entity** means:

(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. **45 CFR § 160.103**

**Covered functions** means those functions of a covered entity the performance of which makes the entity a health plan, health care provider, or health care clearinghouse. **45 CFR § 164.103**

**Covered health care provider** means a health care provider that meets the definition at paragraph (3) of the definition of "covered entity" at §160.103 of this subchapter. **45 CFR § 162.103**

**Data aggregation** means, with respect to protected health information created or received by a business associate in its capacity as the business associate of a covered entity, the combining of such protected health information by the business associate with the protected health information received by the business associate in its capacity as a business associate of another covered entity, to permit data analyses that relate to the health care operations of the respective covered entities. **45 CFR § 164.501**

**Data condition** means the rule that describes the circumstances under which a covered entity must use a particular data element or segment. **45 CFR § 162.103**

**Data content** means all the data elements and code sets inherent to a transaction, and not related to the format of the transaction. Data elements that are related to the format are not data content. **45 CFR § 162.103**

**Data element** means the smallest named unit of information in a transaction. **45 CFR § 162.103**

**Data set** means a semantically meaningful unit of information exchanged between two parties to a transaction. **45 CFR § 162.103**

**Descriptor** means the text defining a code. **45 CFR § 162.103**

**Designated record set** means:

(1) A group of records maintained by or for a covered entity that is:

(i) The medical records and billing records about individuals maintained by or for a covered health care provider;

(ii) The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or

(iii) Used, in whole or in part, by or for the covered entity to make decisions about individuals.

(2) For purposes of this paragraph, the term record means any item, collection, or grouping of information that includes protected health information and is maintained, collected, used, or disseminated by or for a covered entity. **45 CFR § 164.501**

**Designated standard maintenance organization (DSMO)** means an organization designated by the Secretary under §162.910(a). **45 CFR § 162.103**

**Direct treatment relationship** means a treatment relationship between an individual and a health care provider that is not an indirect treatment relationship. **45 CFR § 164.501**

**Direct data entry** means the direct entry of data (for example, using dumb terminals or web browsers) that is immediately transmitted into a health plan's computer. **45 CFR § 162.103**

**Disclosure** means the release, transfer, provision of access to, or divulging in any manner of information outside the entity holding the information. **45 CFR § 160.103**

**EIN** stands for the employer identification number assigned by the Internal Revenue Service, U.S. Department of the Treasury. The EIN is the taxpayer identifying number of an individual or other entity (whether or not an employer) assigned under one of the following:

(1) 26 U.S.C. 6011(b), which is the portion of the Internal Revenue Code dealing with identifying the taxpayer in tax returns and statements, or corresponding provisions of prior law.

(2) 26 U.S.C. 6109, which is the portion of the Internal Revenue Code dealing with identifying numbers in tax returns, statements, and other required documents. **45 CFR § 160.103**

**Electronic health record (EHR)** means an electronic record of health-related information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff. **HITECH Act, § 13400**

**Electronic media** means:

(1) Electronic storage material on which data is or may be recorded electronically, including, for example, devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card;

(2) Transmission media used to exchange information already in electronic storage media. Transmission media include, for example, the Internet, extranet or intranet, leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media. Certain transmissions, including of paper, via facsimile, and of voice, via telephone, are not considered to be transmissions via electronic media if the information being exchanged did not exist in electronic form immediately before the transmission. **45 CFR § 160.103**

**Electronic protected health information** means information that comes within paragraphs (1)(i) or (1)(ii) of the definition of protected health information as specified in this section. **45 CFR § 160.103**

**Employer** is defined as it is in 26 U.S.C. 3401(d). **45 CFR § 160.103**

**Encryption** means the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key. **45 CFR § 164.304**

**Facility** means the physical premises and the interior and exterior of a building(s). **45 CFR § 164.304**

**Family member** means, with respect to an individual:

(1) A dependent (as such term is defined in **45 CFR 144.103**), of the individual; or

(2) Any other person who is a first-degree, second-degree, third-degree, or fourth-degree relative of the individual or of a dependent of the individual. Relatives by affinity (such as by marriage or adoption) are treated the same as relatives by consanguinity (that is, relatives who share a common biological ancestor). In determining the degree of the relationship, relatives by less than full consanguinity (such as half-siblings, who share only one parent) are treated the same as relatives by full consanguinity (such as siblings who share both parents).

(i) First-degree relatives include parents, spouses, siblings, and children.

(ii) Second-degree relatives include grandparents, grandchildren, aunts, uncles, nephews, and nieces.

(iii) Third-degree relatives include great-grandparents, great-grandchildren, great aunts, great uncles, and first cousins.

(iv) Fourth-degree relatives include great-great grandparents, great-great grandchildren, and children of first cousins. **45 CFR § 160.103**

**Format** refers to those data elements that provide or control the enveloping or hierarchical structure, or assist in identifying data content of, a transaction. **45 CFR § 162.103**

**Genetic information** means:

(1) Subject to paragraphs (2) and (3) of this definition, with respect to an individual, information about:

(i) The individual's genetic tests;

(ii) The genetic tests of family members of the individual;

(iii) The manifestation of a disease or disorder in family members of such individual; or

(iv) Any request for, or receipt of, genetic services, or participation in clinical research which includes genetic services, by the individual or any family member of the individual.

(2) Any reference in this subchapter to genetic information concerning an individual or family member of an individual shall include the genetic information of:

(i) A fetus carried by the individual or family member who is a pregnant woman; and

(ii) Any embryo legally held by an individual or family member utilizing an assisted reproductive technology.

(3) Genetic information excludes information about the sex or age of any individual. **45 CFR § 160.103**

**Genetic services** means:

(1) A genetic test;

(2) Genetic counseling (including obtaining, interpreting, or assessing genetic information); or

(3) Genetic education. **45 CFR § 160.103**

**Genetic test** means an analysis of human DNA, RNA, chromosomes, proteins, or metabolites, if the analysis detects genotypes, mutations, or chromosomal changes. Genetic test does not include an analysis of proteins or metabolites that is directly related to a manifested disease, disorder, or pathological condition. **45 CFR § 160.103**

**Group health plan** (also see definition of health plan in this section) means an employee welfare benefit plan (as defined in section 3(1) of the Employee Retirement Income and Security Act of 1974 (ERISA), 29 U.S.C. 1002(1)), including insured and self-insured plans, to the extent that the plan provides medical care (as defined in section 2791(a)(2) of the Public Health Service Act (PHS Act), 42 U.S.C. 300gg–91(a)(2)), including items and services paid for as medical care, to employees or their dependents directly or through insurance, reimbursement, or otherwise, that:

(1) Has 50 or more participants (as defined in section 3(7) of ERISA, 29 U.S.C. 1002(7)); or

(2) Is administered by an entity other than the employer that established and maintains the plan. **45 CFR § 160.103**

**HCPCS** stands for the Health [Care Financing Administration] Common Procedure Coding System. **45 CFR § 162.103**

**HHS** stands for the Department of Health and Human Services. **§ 160.103**

**Health care** means care, services, or supplies related to the health of an individual. Health care includes, but is not limited to, the following:

(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. **45 CFR § 160.103**

**Health care clearinghouse** means 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. **45 CFR § 160.103**

**Health care component** means a component or combination of components of a hybrid entity designated by the hybrid entity in accordance with §164.105(a)(2)(iii)(C). **45 CFR § 164.103**

**Health care operations** means any of the following activities of the covered entity to the extent that the activities are related to covered functions:

(1) Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; patient safety activities (as defined in **42 CFR 3.20**); population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of health care providers and patients with information about treatment alternatives; and related functions that do not include treatment;

(2) Reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, health plan performance, conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers, training of non-health care professionals, accreditation, certification, licensing, or credentialing activities;

(3) Except as prohibited under § 164.502(a)(5)(i), underwriting, enrollment, premium rating, and other activities related to the creation, renewal, or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to claims for health care (including stop-loss insurance and excess of loss insurance), provided that the requirements of § 164.514(g) are met, if applicable;

(4) Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs;

(5) Business planning and development, such as conducting cost-management and planning-related analyses related to managing and operating the entity, including formulary development and administration, development or improvement of methods of payment or coverage policies; and

(6) Business management and general administrative activities of the entity, including, but not limited to:

(i) Management activities relating to implementation of and compliance with the requirements of this subchapter;

(ii) Customer service, including the provision of data analyses for policy holders, plan sponsors, or other customers, provided that protected health information is not disclosed to such policy holder, plan sponsor, or customer;

(iii) Resolution of internal grievances;

(iv) The sale, transfer, merger, or consolidation of all or part of the covered entity with another covered entity, or an entity that following such activity will become a covered entity and due diligence related to such activity; and

(v) Consistent with the applicable requirements of §164.514, creating de-identified health information or a limited data set, and fundraising for the benefit of the covered entity. **45 CFR § 164.501**

**Health care provider** means 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. **45 CFR § 160.103**

**Health information** means any information, including genetic 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. **45 CFR § 160.103**

**Health information technology** means hardware, software, integrated technologies or related licenses, intellectual property, upgrades, or packaged solutions sold as services that are designated for or support the use by health care entities or patients for the electronic creation, maintenance, access, or exchange of health information. **HITECH Act, § 3000**

**Health insurance issuer** (as defined in section 2791(b)(2) of the PHS Act, 42 U.S.C. 300gg–91(b)(2) and used in the definition of *health plan* in this section) means an insurance company, insurance service, or insurance organization (including an HMO) that is licensed to engage in the business of insurance in a State and is subject to State law that regulates insurance. Such term does not include a group health plan. **45 CFR § 160.103**

**Health maintenance organization (HMO)** (as defined in section 2791(b)(3) of the PHS Act, 42 U.S.C. 300gg–91(b)(3) and used in the definition of health plan in this section) means a federally qualified HMO, an organization recognized as an HMO under State law, or a similar organization regulated for solvency under State law in the same manner and to the same extent as such an HMO. **45 CFR § 160.103**

**Health oversight agency** means an agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, or a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is authorized by law to oversee the health care system (whether public or private) or government programs in which health information is necessary to determine eligibility or compliance, or to enforce civil rights laws for which health information is relevant. **45 CFR § 164.501**

**Health plan** means an individual or group plan that provides, or pays the cost of, medical care (as defined in section 2791(a)(2) of the PHS Act, 42 U.S.C. 300gg–91(a)(2)).

(1) *Health plan* includes the following, singly or in combination:

(i) A group health plan, as defined in this section.

(ii) A health insurance issuer, as defined in this section.

(iii) An HMO, as defined in this section.

(iv) Part A or Part B of the Medicare program under title XVIII of the Act.

(v) The Medicaid program under title XIX of the Act, 42 U.S.C. 1396, et seq.

(vi) The Voluntary Prescription Drug Benefit Program under Part D of title XVIII of the Act, 42 U.S.C. 1395w-101 through 1395w-152.

(vii) An issuer of a Medicare supplemental policy (as defined in section 1882(g)(1) of the Act, 42 U.S.C. 1395ss(g)(1)).

(viii) An issuer of a long-term care policy, excluding a nursing home fixed indemnity policy.

(ix) An employee welfare benefit plan or any other arrangement that is established or maintained for the purpose of offering or providing health benefits to the employees of two or more employers.

(x) The health care program for uniformed services under title 10 of the United States Code.

(xi) The veterans health care program under 38 U.S.C. chapter 17.

(xii) The Indian Health Service program under the Indian Health Care Improvement Act, 25 U.S.C. 1601, et seq.

(xiii) The Federal Employees Health Benefits Program under 5 U.S.C. 8902, et seq.

(xiv) An approved State child health plan under title XXI of the Act, providing benefits for child health assistance that meet the requirements of section 2103 of the Act, 42 U.S.C. 1397, et seq.

(xv) The Medicare Advantage program under Part C of title XVIII of the Act, 42 U.S.C. 1395w-21 through 1395w-28.

(xvi) A high risk pool that is a mechanism established under State law to provide health insurance coverage or comparable coverage to eligible individuals.

(xvii) Any other individual or group plan, or combination of individual or group plans, that provides or pays for the cost of medical care (as defined in section 2791(a)(2) of the PHS Act, 42 U.S.C. 300gg–91(a)(2)).

(2) *Health plan* excludes:

(i) Any policy, plan, or program to the extent that it provides, or pays for the cost of, excepted benefits that are listed in section 2791(c)(1) of the PHS Act, 42 U.S.C. 300gg–91(c)(1); and

(ii) A government-funded program (other than one listed in paragraph (1)(i)–(xvi) of this definition):

(A) Whose principal purpose is other than providing, or paying the cost of, health care; or

(B) Whose principal activity is:

(1) The direct provision of health care to persons; or

(2) The making of grants to fund the direct provision of health care to persons. **45 CFR § 160.103**

**Hybrid entity** means a single legal entity:

(1) That is a covered entity;

(2) Whose business activities include both covered and non-covered functions; and

(3) That designates health care components in accordance with paragraph §164.105(a)(2)(iii)(C). **45 CFR § 164.103**

**Implementation specification** means specific requirements or instructions for implementing a standard. **45 CFR § 160.103**

**Indirect treatment relationship** means a relationship between an individual and a health care provider in which:

(1) The health care provider delivers health care to the individual based on the orders of another health care provider; and

(2) The health care provider typically provides services or products, or reports the diagnosis or results associated with the health care, directly to another health care provider, who provides the services or products or reports to the individual. **45 CFR § 164.501**

**Individual** means the person who is the subject of protected health information. **45 CFR § 160.103**

**Individually identifiable health information** is information that is a subset of health information, including demographic information collected from an individual, and:

(1) Is created or received by a health care provider, health plan, employer, 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; and

(i) That identifies the individual; or

(ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual. **45 CFR § 160.103**

**Information system** means an interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people. **45 CFR § 164.304**

**Inmate** means a person incarcerated in or otherwise confined to a correctional institution. **45 CFR § 164.501**

**Integrity** means the property that data or information have not been altered or destroyed in an unauthorized manner. **45 CFR § 164.304**

**Law enforcement official** means an officer or employee of any agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, who is empowered by law to:

(1) Investigate or conduct an official inquiry into a potential violation of law; or

(2) Prosecute or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law. **45 CFR § 164.103**

**Maintain or maintenance** refers to activities necessary to support the use of a standard adopted by the Secretary, including technical corrections to an implementation specification, and enhancements or expansion of a code set. This term excludes the activities related to the adoption of a new standard or implementation specification, or modification to an adopted standard or implementation specification. **45 CFR § 162.103**

**Malicious software** means software, for example, a virus, designed to damage or disrupt a system. **45 CFR § 164.304**

**Manifestation or manifested** means, with respect to a disease, disorder, or pathological condition, that an individual has been or could reasonably be diagnosed with the disease, disorder, or pathological condition by a health care professional with appropriate training and expertise in the field of medicine involved. For purposes of this subchapter, a disease, disorder, or pathological condition is not manifested if the diagnosis is based principally on genetic information. **45 CFR § 160.103**

**Marketing:**

(1) Except as provided in paragraph (2) of this definition, marketing means to make a communication about a product or service that encourages recipients of the communication to purchase or use the product or service.

(2) Marketing does not include a communication made:

(i) To provide refill reminders or otherwise communicate about a drug or biologic that is currently being prescribed for the individual, only if any financial remuneration received by the covered entity in exchange for making the communication is reasonably related to the covered entity's cost of making the communication.

(ii) For the following treatment and health care operations purposes, except where the covered entity receives financial remuneration in exchange for making the communication:

(A) For treatment of an individual by a health care provider, including case management or care coordination for the individual, or to direct or recommend alternative treatments, therapies, health care providers, or settings of care to the individual;

(B) To describe a health-related product or service (or payment for such product or service) that is provided by, or included in a plan of benefits of, the covered entity making the communication, including communications about: the entities participating in a health care provider network or health plan network; replacement of, or enhancements to, a health plan; and health-related products or services available only to a health plan enrollee that add value to, but are not part of, a plan of benefits; or

(C) For case management or care coordination, contacting of individuals with information about treatment alternatives, and related functions to the extent these activities do not fall within the definition of treatment.

(3) Financial remuneration means direct or indirect payment from or on behalf of a third party whose product or service is being described. Direct or indirect payment does not include any payment for treatment of an individual. 45 CFR § 164.501

**Maximum defined data set** means all of the required data elements for a particular standard based on a specific implementation specification. **45 CFR § 162.103**

**Modify or modification** refers to a change adopted by the Secretary, through regulation, to a standard or an implementation specification. **45 CFR § 160.103**

**More stringent** means, in the context of a comparison of a provision of State law and a standard, requirement, or implementation specification adopted under subpart E of part 164 of this subchapter, a State law that meets one or more of the following criteria:

(1) With respect to a use or disclosure, the law prohibits or restricts a use or disclosure in circumstances under which such use or disclosure otherwise would be permitted under this subchapter, except if the disclosure is:

(i) Required by the Secretary in connection with determining whether a covered entity or business associate is in compliance with this subchapter; or

(ii) To the individual who is the subject of the individually identifiable health information.

(2) With respect to the rights of an individual, who is the subject of the individually identifiable health information, regarding access to or amendment of individually identifiable health information, permits greater rights of access or amendment, as applicable.

(3) With respect to information to be provided to an individual who is the subject of the individually identifiable health information about a use, a disclosure, rights, and remedies, provides the greater amount of information.

(4) With respect to the form, substance, or the need for express legal permission from an individual, who is the subject of the individually identifiable health information, for use or disclosure of individually identifiable health information, provides requirements that narrow the scope or duration, increase the privacy protections afforded (such as by expanding the criteria for), or reduce the coercive effect of the circumstances surrounding the express legal permission, as applicable.

(5) With respect to recordkeeping or requirements relating to accounting of disclosures, provides for the retention or reporting of more detailed information or for a longer duration.

(6) With respect to any other matter, provides greater privacy protection for the individual who is the subject of the individually identifiable health information. **45 CFR § 160.202**

**Organized health care arrangement** means:

(1) A clinically integrated care setting in which individuals typically receive health care from more than one health care provider;

(2) An organized system of health care in which more than one covered entity participates and in which the participating covered entities:

(i) Hold themselves out to the public as participating in a joint arrangement; and

(ii) Participate in joint activities that include at least one of the following:

(A) Utilization review, in which health care decisions by participating covered entities are reviewed by other participating covered entities or by a third party on their behalf;

(B) Quality assessment and improvement activities, in which treatment provided by participating covered entities is assessed by other participating covered entities or by a third party on their behalf; or

(C) Payment activities, if the financial risk for delivering health care is shared, in part or in whole, by participating covered entities through the joint arrangement and if protected health information created or received by a covered entity is reviewed by other participating covered entities or by a third party on their behalf for the purpose of administering the sharing of financial risk.

(3) A group health plan and a health insurance issuer or HMO with respect to such group health plan, but only with respect to protected health information created or received by such health insurance issuer or HMO that relates to individuals who are or who have been participants or beneficiaries in such group health plan;

(4) A group health plan and one or more other group health plans each of which are maintained by the same plan sponsor; or

(5) The group health plans described in paragraph (4) of this definition and health insurance issuers or HMOs with respect to such group health plans, but only with respect to protected health information created or received by such health insurance issuers or HMOs that relates to individuals who are or have been participants or beneficiaries in any of such group health plans. **45 CFR § 160.103**

**Password** means confidential authentication information composed of a string of characters. **45 CFR § 164.304**

**Payment** means:

(1) The activities undertaken by:

(i) Except as prohibited under § 164.502(a)(5)(i), a health plan to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the health plan; or

(ii) A health care provider or health plan to obtain or provide reimbursement for the provision of health care; and

(2) The activities in paragraph (1) of this definition relate to the individual to whom health care is provided and include, but are not limited to:

(i) Determinations of eligibility or coverage (including coordination of benefits or the determination of cost sharing amounts), and adjudication or subrogation of health benefit claims;

(ii) Risk adjusting amounts due based on enrollee health status and demographic characteristics;

(iii) Billing, claims management, collection activities, obtaining payment under a contract for reinsurance (including stop-loss insurance and excess of loss insurance), and related health care data processing;

(iv) Review of health care services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges;

(v) Utilization review activities, including precertification and preauthorization of services, concurrent and retrospective review of services; and

(vi) Disclosure to consumer reporting agencies of any of the following protected health information relating to collection of premiums or reimbursement:

(A) Name and address;

(B) Date of birth;

(C) Social Security number;

(D) Payment history;

(E) Account number; and

(F) Name and address of the health care provider and/or health plan. **§ 164.501**

**Person** means a natural person, trust or estate, partnership, corporation, professional association or corporation, or other entity, public or private. **45 CFR § 160.103**

**Physical safeguards** are physical measures, policies, and procedures to protect a covered entity's or business associate's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion. **45 CFR § 164.304**

**Plan sponsor** is defined as defined at section 3(16)(B) of ERISA, 29 U.S.C. 1002(16)(B). **45 CFR § 164.103**

**Protected health information** means individually identifiable health information:

(1) Except as provided in paragraph (2) of this definition, that is:

(i) Transmitted by electronic media;

(ii) Maintained in electronic media; or

(iii) Transmitted or maintained in any other form or medium.

(2) Protected health information excludes individually identifiable health information:

(i) In education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g;

(ii) In records described at 20 U.S.C. 1232g(a)(4)(B)(iv);

(iii) In employment records held by a covered entity in its role as employer; and

(iv) Regarding a person who has been deceased for more than 50 years.
**45 CFR § 160.103**

**Psychotherapy notes** means notes recorded (in any medium) by a health care provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session and that are separated from the rest of the individual's medical record. *Psychotherapy* notes excludes medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of the following items: diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date. **45 CFR § 164.501**

**Public health authority** means an agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, or a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is responsible for public health matters as part of its official mandate. **45 CFR § 164.501**

**Reasonable cause** means an act or omission in which a covered entity or business associate knew, or by exercising reasonable diligence would have known, that the act or omission violated an administrative simplification provision, but in which the covered entity or business associate did not act with willful neglect. **45 CFR § 160.401**

**Reasonable diligence** means the business care and prudence expected from a person seeking to satisfy a legal requirement under similar circumstances. **45 CFR § 164.401**

**Relates to the privacy of individually identifiable health information** means, with respect to a State law, that the State law has the specific purpose of protecting the privacy of health information or affects the privacy of health information in a direct, clear, and substantial way. **45 CFR § 160.202**

**Required by law** means a mandate contained in law that compels an entity to make a use or disclosure of protected health information and that is enforceable in a court of law. Required by law includes, but is not limited to, court orders and court-ordered warrants; subpoenas or summons issued by a court, grand jury, a governmental or tribal inspector general, or an administrative body authorized to require the production of information; a civil or an authorized investigative demand; Medicare conditions of participation with respect to health care providers participating in the program; and statutes or regulations that require the production of information, including statutes or regulations that require such information if payment is sought under a government program providing public benefits. **45 CFR § 164.103**

**Research** means a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge. **45 CFR § 164.501**

**Respondent** means a covered entity or business associate upon which the Secretary has imposed, or proposes to impose, a civil money penalty. **45 CFR § 160.103**

**Secretary** means the Secretary of Health and Human Services or any other officer or employee of HHS to whom the authority involved has been delegated. **45 CFR § 160.103**

**Security or Security measures** encompass all of the administrative, physical, and technical safeguards in an information system. **45 CFR § 164.304**

**Security incident** means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. **45 CFR § 164.304**

**Segment** means a group of related data elements in a transaction. **45 CFR § 162.103**

**Small health plan** means a health plan with annual receipts of $5 million or less. **45 CFR § 160.103**

**Standard** means 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 protected health information. **45 CFR § 160.103**

**Standard setting organization (SSO)** means 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, this part. **45 CFR § 160.103**

**Standard transaction** means a transaction that complies with an applicable standard adopted under this part. **45 CFR § 162.103**

**State** refers to one of the following:

(1) For a health plan established or regulated by Federal law, State has the meaning set forth in the applicable section of the United States Code for such health plan.

(2) For all other purposes, State means any of the several States, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, Guam, American Samoa, and the Commonwealth of the Northern Mariana Islands.
**45 CFR § 160.103**

**State law** means a constitution, statute, regulation, rule, common law, or other State action having the force and effect of law. **45 CFR § 160.202**

**Subcontractor** means a person to whom a business associate delegates a function, activity, or service, other than in the capacity of a member of the workforce of such business associate.
**45 CFR § 160.103**

**Technical safeguards** means the technology and the policy and procedures for its use that protect electronic protected health information and control access to it. **45 CFR § 164.304**

**Trading partner agreement** means 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.) **45 CFR § 160.103**

**Transaction** means 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. **45 CFR § 160.103**

**Treatment** means the provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another. **45 CFR § 164.501**

**Unsecured protected health information** means protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary in the guidance issued under section 13402(h)(2) of Public Law 111-5. **45 CFR § 164.402**

**Use** means, with respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information. **45 CFR § 160.103**

**User** means a person or entity with authorized access. **45 CFR § 164.304**

**Violation or violate** means, as the context may require, failure to comply with an administrative simplification provision. **45 CFR § 160.103**

**Willful neglect** means conscious, intentional failure or reckless indifference to the obligation to comply with the administrative simplification provision violated. **45 CFR § 160.401**

**Workforce** means employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity or business associate, is under the direct control of such covered entity or business associate, whether or not they are paid by the covered entity or business associate. **45 CFR § 160.103**

**Workstation** means an electronic computing device, for example, a laptop or desktop computer, or any other device that performs similar functions, and electronic media stored in its immediate environment. **45 CFR § 164.304**