

Key Terms and Definitions

Business Associate- defined in the Health Insurance Portability and Accountability Act of 1996 (HIPAA):

- Works on behalf of a health plan, provider billing electronically or medical claims clearinghouse to which HIPAA rules apply (a covered entity)
- Uses or discloses protected health information as part of that work
- Not a part of the covered entity workforce

The Privacy Rule lists *typical* business associate activities: Claims processing, administration, data analysis, processing or administration, utilizations review, QA, billing, benefit management, practice management and re-pricing or legal, actuarial accounting, consulting, data aggregation, management, administrative, accreditation or financial services.

CDPHE examples include Vital Statistics doing work for the Wyoming Department of Public Health, Prenatal Plus and Colorado Women's Cancer Control Initiative working for or with Medicaid, and an HCP transcriber hired to do medical reports for UCHSC physicians.

A covered entity may be a business associate of another covered entity.

Confidential. Confidential information or data is that which is sensitive and needs to be protected and carefully controlled. Confidential treatment means that no one outside the immediate data-collecting organization will have access to the information or data without prior approval. See also Sensitive Information, below.

Covered entity- Per the Health Insurance Portability and Accountability Act of 1996 (HIPAA):

- (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 HIPAA.

Data Use Agreement. An agreement signed before a data set containing sensitive record-level information is released. It may stipulate the permitted uses for the data, re-disclosures or follow-back, who may access the data and publication disclaimers, etc. The Data User Agreement may be between CDPHE and an outside entity or be used between two CDPHE units.

Data User. The institution, person or entity signing a **Data Use Agreement**.

Dual (Split) Tunneling or Dual Homing- Split tunneling is a Virtual Private Network (VPN) feature which routes user traffic based on the destination IP address. It is generally used to allow a remote VPN user to connect to the Internet and the intranet at the same time providing a “dual homing” effect. If the user is connected to the Internet at the same time a hacker is, the hacker can come in through the Internet to compromise the home-machine and thus get access to the internal network through the secure VPN connection

Disclosure- the release, transfer, provision of access to, or divulging in any other manner of information outside the entity holding the information. Disclosure may include releasing information to other programs within CDPHE.

Email Relay- The capacity to configure email to be automatically collected and resent to third party email systems not controlled by CDPHE.

Facilities- include all buildings at the CDPHE campus and includes the laboratory building at Lowry. Facilities also include any space rented, leased, owned or shared by CDPHE for use by its workforce, including CDPHE offices statewide.

Firewall-a part of a computer system or network which is designed to block unauthorized access while permitting outward communication (Oxford English Dictionary.)

Health Insurance Portability and Accountability Act of 1996 (HIPAA). Federal legislation that applies to health plans, health providers that bill medical services electronically and medical claims clearinghouses and their business associates. HIPAA mandates privacy and security safeguards for medical information. It also sets standards for electronic billing. HIPAA extends rights to citizens for access to and protection of their own medical information.

Health oversight agency –(per HIPAA) 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.

Identifying information- Refers to any information that could facilitate the identification of any individual. This is not only name and address, but also individual case record data where other demographic items such as age, sex, race and place of residence could possibly be used to identify subjects.

Information system-Includes the servers or computers that store the information, the information itself, any application that is used to store, or make accessible the

information, and other hardware and software that is used to maintain the information, which may include PDAs, desktop or laptop computers, communication devices, and utility and development tools.

ITSR- Information Technology Service Request is a form required by the ITS section when ordering hardware, software, wiring changes, etc. It is located on the Intranet, or call the Help Desk, x2222 for the exact location of the form.

Level 1 and 2 incidents. A Level 1 incident is one which for which standard operational procedures can handle, and that typically, a PC Tech understands how to resolve. A Level 2 incident is one that falls outside of normal operating procedures to correct and which requires more resources to resolve. Most privacy incidents having to do with unauthorized access are Level 2 incidents, while removing a virus from an infected computer would be a typical Level 1 incident. Potential problems that are raised as a threat to maintaining safeguards are most likely Level 2.

Marketing- (HIPAA definition) to make a communication about a product or service a purpose of which is to encourage recipients of the communication to purchase or use the product or service. Marketing *excludes*: 1) communications explaining products or services provided as a benefit of a health plan or program; 2) communicated by a health care provider that are tailored to the circumstances of a particular individual for treatment purposes or 3) communicated by a health care provider for the purpose of directing or recommending to that individual alternative treatments, therapies, health care providers, or settings of care. A communication described is not included in marketing if: (i) The communication is made orally; or (ii) The communication is in writing and no direct or indirect remuneration is received from a third party for making the communication.

PC Tech-see Tech.

Population size. This is used in determining whether information can be released and still protect the privacy of any individuals referenced in the information. The size could be the entire population of the state, a region of the state, a county, a zip code, or census tract. Thus, defining the geographic region is the first step in defining the population size. The population size may be restricted to births in a geographic region. When the data are restricted to births defects or developmental disabilities, the population size is the number at risk for the given time period. For example, county X might have 6,000 births per year, but the surveillance data are for births in a six month period; the population size, therefore, is 3,000; similarly, if the time period were 24 months, the population size would be 12,000.

Privacy-1) Privacy is a key value which underpins human dignity and other key values such as freedom of association and freedom of speech...Privacy is a basic human right and the reasonable expectation of every person." ("The Australian Privacy Charter," published by the Australian Privacy Charter Group, Law School, University of New South Wales, Sydney, 1994; 2) The right of the individual to be protected against intrusion into his personal life or affairs, or those of his family, by direct physical means

or by publication of information (Report of the Committee on Privacy and Related Matters, Chairman David Calcutt QC, 1990, Cmnd. 1102, London: HMSO); 3) “Privacy is what you protect-security is how you protect it.” (Bob O’Doherty, CIO CDPHE, 2004.)

Program Manager-A CDPHE staff member who is responsible for the mission, strategies, policies and procedures of a unit. The program manager may also oversee an information system that supports the activities of the program. Each division may have a different name (unit, section, etc.) for the same type of position, and each CDPHE division must designate the individuals who qualify as program managers.

Personal Health Information. This includes all information from a medical record or file that can be used to identify a person either on its own or in conjunction with other information that may be available for outside sources. HIPAA uses the term “Protected Health Information (see below). “Personal Health Information” is used at CDPHE to designate information needing to be kept confidential regardless of status under HIPAA.

Protected Health Information (PHI)-defined in HIPAA to include individually identified information, 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 *except* health information in: (i) Education records covered by the Family Educational Right and Privacy Act, as amended, 20 U.S.C. 1232g; and (ii) Records described at 20 U.S.C. 1232g(a)(4)(B)(iv).

Psychotherapy Notes- (per HIPAA) 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.

Public Health Authority- (per HIPAA) 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.

Remote Access- Remote access is access to a CDPHE server or network from a remote location. Remote access may be used by a network administrator to monitor servers while at home, or for a developer to support an application remotely. Remote access does not include normal sign-on to a CDPHE web application. Special care must be taken to ensure that the security of CDPHE internal network is not compromised by remote access due to outdated security patches, virus checking software or lack of strong firewalls on the remote access computer.

Research-Research means a systematic investigation, including research development, testing, and evaluations, designed to develop or contribute to generalizable knowledge.

Research is designed to *test a hypothesis* through the collection and analysis of data. The resulting conclusions are used to develop or contribute to generalizable knowledge. A hypothesis is a tentative assumption that is empirically tested. If the conclusions resulting from data analysis do not support the hypothesis, it must be rejected or modified. A research study is usually described in a formal protocol that sets forth an objective and a set of procedures designed to reach that objective.

Research may be distinguished from public health practices. The majority of **public health practices** (e.g., public health surveillance, and the implementation and evaluation of disease prevention and control projects) are based on scientific evidence, data collection and analytic methods similar to those used in research. They are not, however, *designed to contribute to generalizable knowledge*. Their primary purpose is to protect the health of the population through such activities as disease surveillance, prevention, or control.

For the most part, the term “public health practice” refers to interventions that are designed solely to enhance the well-being of the community with a reasonable expectation of success. The purpose of these interventions is to provide identification, prevention, and treatment to either an individual or the community at-large.

A discussion of public health practice versus research is also included in HIPAA Privacy Rule and Public Health Guidance from CDC and the U.S. Department of Health and Human Services. The guidance was first released online in *MMWR*, Volume 52, Early Release:<http://www.cdc.gov/privacyrule/privacy-HIPAAfacts.htm>

Role- A defined function or task in an information system. A role requires defined access (screens, tables, files) and privileges (read, write, edit, delete) in order to accomplish the task. Data entry clerks may have write access to one set of screens, supervisors who do not enter into a system may only require read access, whereas system administrators may need write/delete access to all screens.

Security- 1) the safety of a state or organization against criminal activity such as terrorism or espionage (Compact Oxford Dictionary); 2) “Privacy is what you protect-security is how you protect it.” (Bob O’Doherty, CIO CDPHE, 2004.); 3) security

encompasses all the administrative, physical and technical safeguards in an information system (HIPAA Security Rule §164.304.)

Security Breach- A security incident is defined as an adverse event caused by a failure of a security mechanism or an attempted or threatened breach of those mechanisms, (i.e., computer hacker system penetrations, shared user IDs, computer viruses, stolen papers, stolen equipment or disks, etc). Incidents are categorized according to their seriousness. A Level 1 incident may include mitigation for known problems for which the cause and the remedy are well understood by PC Technicians and no sensitive information has been compromised. Removing a known virus from an infected machine would be a Level 1 incident. A Level 2 incident is one in which there is any one of the following: 1) real or potential compromise of a server, PC, laptop or database or papers containing sensitive information; 2) uncertainty as to best way to mitigate the potential damage; 3) suspicion of internal malfeasance; 4) system reports or logs that indicate an unusual occurrence or possible intrusion.

Sensitive Information – This broad designation includes public health information that identifies an individual, personal information for employees or social security numbers for vendors and licensees. Tax numbers are not considered to be sensitive information. Other sensitive information may include cell phone numbers that are not generally available. Information may be designated as sensitive on a program-by-program basis at the discretion of the program manager. Examples of sensitive information include:

- a. KRONOS
- b. Disease tracking or case-management information that identifies individuals
- c. Human Resources information that includes staff social security numbers or information about any type of staff leave
- d. Budgeting and accounting software with social security numbers, including Colorado Financial Reporting System (COFRS)
- e. Facility databases with patient information
- f. Registries
- g. Call lists that may include non-published phone numbers or addresses
- h. Word files, Excel spreadsheets or any other files type with individually identifiable sensitive information.
- i. Medical records reviews or audits that include individual medical information
- j. CDPHE computer network diagrams
- k. Personnel exposure reports on radioactive materials licensees
- l. Confidential commercial data on licensees and permittees

Strong Password- Strong passwords reduce the likelihood of a password being deciphered and sensitive information compromised. They require more time to “break” and increasing the time required is a major part of password security. Strong passwords are also a protection against those with some personal knowledge of a user who might be able to guess obvious passwords. See *Strong Password Guidelines* for specifics about creating strong passwords.

Tech or PC Tech- This refers to the staff members who support personal computers. Some PC Techs work for the ITS section, while other divisions provide their own PC

Techs. They typically set up new computers, trouble-shoot hardware and some software problems, remove viruses from infected computers, and are the first line support for computer issues.

Treatment- (HIPAA definition) 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.

Use- (HIPAA definition) 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.

VPN-Virtual Private Network. This is a special communications arrangement that allows a user to securely access information systems. Commonly used by system administrators when performing system support activities from a remote location or for some wireless access.

Workforce - (HIPAA definition) employees, volunteers, trainees, and other persons whose conduct, in the performance of work is under the direct control of an entity, whether or not they are paid. Only workforce members that are employees are subject to the State of Colorado personnel policies and procedures, and may be sanctioned accordingly if found to be in violation of CDPHE policies and procedures. All workforce members are expected to understand and abide by CDPHE security policies and procedures and may have their contract, internship, etc. terminated as appropriate if found in violation of the security policies and procedures.