PUBLIC HEALTH DATA STANDARDS CONSORTIUM
PHDSC
Promoting Standards Through Partnerships

Public Health Data Standards Consortium
PRISM
A Privacy Toolkit for Public Health Professionals

Glossary

The following is a list of common privacy terminology. These are the working definitions for key terms used through the privacy educational tool.

Accounting of Disclosures: Refers to the right of individuals, with limitations, to a listing of the uses and disclosures of their identifiable health information for a period of time not to exceed six years prior to the date of the request.

Administrative safeguards: Administrative actions, including policies and procedures, that manage the selection, development, implementation, and maintenance of privacy and security measures to protect identifiable health information and to manage the conduct of the workforce in relation to the protection of that information.

Authorization: The HIPAA Privacy Rule requires an individual's permission, known as an authorization, for the use or disclosure of identifiable health information for any activity not specifically allowed without one. Uses and disclosures related to treatment, payment, and health care operations generally do not require an authorization; but some non-health care related activities such as marketing do. Authorization is a new term used in the Privacy rule to denote an activity that has often been called a consent or release. A covered entity would never obtain both an individual's consent and an authorization for a single use or disclosure. An individual's consent cannot be obtained to permit any use or disclosure that requires an authorization, nor can an Authorization be used to obtain consent for uses and disclosures for treatment, payment, and health care operations.

Business Associate: A person or entity who, on behalf of a covered entity, uses or discloses identifiable health information to perform one of the following (1) activities: claims processing or administration; data analysis, processing or administration; utilization review; quality assurance; billing; benefit management; practice management; repricing; or one of the following (2) services that involve identifiable health information: legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation or financial services.

Confidentiality: The obligation of an entity that receives identifiable information about an individual as part of providing a service to that individual to protect that data or information, including not disclosing the identifiable information to unauthorized persons or through unauthorized processes.

Consent: Consent under the Privacy rule refers to a consent by an individual for the covered entity to use or disclose identifiable health information for treatment, payment, and health care operations purposes **only**. This is different from a consent for treatment, which many providers use and which should not be confused with the consent for use or disclosure of identifiable health information. Consent for use and/or disclosure of identifiable health information is

optional under the Privacy rule, although it may be required by state law, and may be combined with a consent for treatment unless prohibited by other law.

Consent, Informed: Refers to the requirement that all researchers explain the purposes, risks, benefits, confidentiality protections, and other relevant aspects of a research study to potential human subjects so that they may make an informed decision regarding their participation in the research. Institutional Review Boards (IRB) review the informed consent process and forms documenting the consent to ensure compliance with research regulations and policies.

Correctional Institution: Any penal or correctional facility, jail, reformatory, detention center, work farm, halfway house, or residential community program center operated by, or under contract to a State, for the confinement or rehabilitation of persons charged with or convicted of a criminal offense or other persons held in lawful custody.

Covered Entity: Entities to which the HIPAA rules apply. These include Health Plans, Health Care Clearinghouses, and Health Care Providers who transmit any health information in electronic form in connection with a standard transaction covered by HIPAA laws and regulations.

De-identified Health Information: Health information that has had all individual identifiers, both direct and indirect, removed. A covered entity may determine that health information is not individually identifiable health information only if: (1) a person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable determines that the risk is very small that the information could be used, alone or in combination with other available information, to identify an individual, and documents the methods and results of the analysis; or (2) the following identifiers of the individual, relatives, employers or household members of the individual are removed:
(1) Name;
(2) Street address, city, county, precinct, zip code and equivalent geocodes;
(3) All elements of dates (except year) for dates directly related to an individual and all ages over 89;
(4) Telephone number;
(5) Fax number;
(6) Electronic mail address;
(7) Social Security Number;
(8) Medical record numbers;
(9) Health plan ID numbers;
(10) Account numbers
(11) Certificate/license numbers;
(12) Vehicle identifiers and serial numbers, including license plate numbers;
(13) Device identifiers and serial numbers
(14) Web addresses (URLs);
(15) Internet IP addresses;
(16) Biometric identifiers, including finger and voice prints;
(17) Full face photographic images and any comparable images; and
(18) Any other unique identifying number, characteristic or code.

Designated Record Set: Medical and billing records and any other information that is used to make decisions about an individual's care, treatment, or payment maintained by or for a covered entity. It also means the enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a Health Plan. The term "record" means any item, collection, or grouping of information that includes identifiable health information and is maintained, collected, used, or disseminated by or for a covered entity.

Disclosure: The release, transfer, provision of access to, or divulging in any other manner of information outside the entity holding the information.

Electronic protected health information (EPHI): Individually identifiable health information that is transmitted or maintained in electronic form.

Encryption: 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.

Group Health Plan: An employee welfare benefit plan (as defined by ERISA) or insured and self-insured plans that provides medical care (as defined by the Public Health Service Act; *see definition below*) to employees or their dependents directly or through insurance that:
(1) Has 50 or more participants (as defined by ERISA); or
(2) (2) Is administered by an entity other than the employer that established and maintains the plan. See related definition for Health Plan.

The Public Health Service Act definition of a "group health plan" means an employee welfare benefit plan (as defined in section 3(1) of the Employee Retirement Income Security Act of 1974 [29 U.S.C. 1002 (1)]) to the extent that the plan provides medical care (as defined in paragraph (2)) and including items and services paid for as medical care) to employees or their dependents (as defined under the terms of the plan) directly or through insurance, reimbursement, or otherwise.

In the public sector, the health coverage that is available to public sector employees qualifies as a group health plan. However, most non-employee public sector payers and plans, including Medicaid and Medicare, are not governed by ERISA and therefore do not qualify as group health plans under this definition.

Health Care: Care, services, or supplies related to the health of an individual and 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.

Health Care Clearinghouse: A public or private entity, including a billing service, repricing company, community health management information system or community health information system 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, or
(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.

Healthcare Operations: Any of the following activities of the covered entity to the extent that the activities are related to covered functions:

- conducting quality assessment and improvement activities, population-based activities, and related functions that do not include treatment;
- reviewing the competence or qualifications of health care professionals, evaluating practitioner, provider, and health plan performance, conducting training programs where students learn to practice or improve their skills as health-care providers, training of non-health-care professionals, accreditation, certification, licensing, or credentialing activities;
- underwriting, premium rating, and other activities relating to the creation, renewal or replacement of a contract of health insurance or benefits;
- conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs;
- 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
- business management and general administrative activities of the entity.

Health Care Provider: A provider of medical or health services and any other person or organization that furnishes, bills for, or is paid for health care in the normal course of business. Under HIPAA, entities that have not previously been considered health care providers may now meet the criteria for a covered health care provider, such as social service programs, school health programs, and public health prevention and screening programs.

Health Oversight Agency: An agency or other governmental authority, including employees, agents or contractors of such agency or authority, authorized by law to oversee the health care system (whether public or private) or government programs in which public health information is necessary to determine eligibility or compliance or to enforce civil rights law. Under the HIPAA Privacy Rule, a covered entity may disclose identifiable health information to a health oversight agency for oversight activities authorized by law. For example, a covered entity could disclose public health information in the course of reporting suspected health care fraud to a health oversight agency. Health oversight activities include audits, inspections, licensure, disciplinary action, government monitoring, and other mandated or specified regulatory activities.

Health Plan: An individual or group plan that provides or pays the cost of medical care and includes the following, singly or in combination:
(1) A Group Health Plan, as defined herein
(2) A Health Insurance Issuer, as defined herein

(3) An HMO, as defined herein
(4) Part A or Part B of the Medicare program under Title XVIII
(5) The Medicaid program under Title XIX
(6) An issuer or a Medicare supplemental policy
(7) An issuer or a long-term care policy, excluding a nursing home fixed-indemnity policy
(8) 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
(9) The health care program for active military personnel under title 10 of the United States Code
(10) The veterans health care program under 38 U.S.C. chapter 17.
(11) The Civilian Health and Medical Program of the Uniformed Services (CHAMPUS)
(12) The Indian Health Service program under the Indian Health Care Improvement Act
(13) The Federal Employees Health Benefits Program
(14) An approved State child health plan under Title XXI providing benefits for child health assistance
(15) The Medicare + Choice program under Part C of Title XVIII
(16) A high risk pool that is a mechanism established under State law to provide health insurance coverage or
comparable coverage to eligible individuals
(17) Any other individual or group plan, or combination of individual or group plans, that provides or pays for the cost of medical care

Many non-employee public sector programs and services that pay for health care services, including through contracts with providers, may qualify under this definition of health plan, even though the programs and services do not operate like commercial health plans or consider themselves primarily health service providers. If the public program functions primarily as a payer or primarily contracts for services rather than provides services directly, this program is very likely to meet the health plan definition.

Individual: The person who is the subject of identifiable or protected health information.

Individually Identifiable Health Information: Information that is a subset of all health information, that contains identifiable elements including demographic information collected from an individual, and:
(I) 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
(A) Identifies the individual; or
(B) reasonably could be used to identify the individual.

Information system: An interconnected set of electronic information resources and/or applications under the same direct management control. A system normally includes hardware, software, information, data, applications, communications, and people. It is made up of databases, application programs and manual and machine procedures. It also encompasses the

computer systems that do the processing as well as intermediary systems that route or perform some action as part of the processing.

Integrity: The property that data or information have not been altered or destroyed in an unauthorized manner.

Limited Data Set: Identifiable health information that excludes the following identifiers of the individual, or of relatives, employers or household members of the individual: names, postal address information other than town or city, state and zip code, telephone numbers, fax numbers, electronic mail address, social security number, health plan beneficiary number, account number, certificate/license number, vehicle identifiers and serial numbers, including license plate numbers, device identifiers and serial numbers, web universal resource locators (URLs), Internet Protocol (IP) address numbers, biometric identifiers, including finger and voice prints and full face photographic images and any comparable images. The exclusions are the same as for de-identified information except that a limited data set can include dates, geographic identifiers other than the street address, and an identifying code that allows the user to know which records belong to the same and which belong to different individuals. A limited data set can only be used for research, public health, or health care operations purposes, and requires a data use agreement prior to disclosure.

Medical Care: Care that relates to
(A) the diagnosis, cure, mitigation, treatment, or prevention of disease, or amounts paid for the purpose of affecting any structure or function of the body,
(B) amounts paid for transportation primarily for and essential to medical care referred to in subparagraph (A), and
(C) amounts paid for insurance covering medical care referred to in subparagraphs (A) and (B).

Minimum Necessary: Sharing only the minimum amount necessary to accomplish the specific purpose of the use or disclosure, whether shared internally or with external parties. The minimum necessary is based on the recipient's need to know as related to their job function or legal mandates. For internal use, the amount of information necessary to accomplish the purpose varies by job title, classification, and/or function. Uses and disclosures for treatment purposes are not subject to the minimum necessary requirement under HIPAA.

Notice of Privacy Practices: A notice to the individual of the uses and disclosures of identifiable health information and the individual's rights and the covered entity's legal duties with respect to that identifiable health information.

Payment: 1) The activities undertaken by
- (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 when 2) the activities relate to the individual to whom health care is provided and include, but are not limited to
- (i) determinations of eligibility or coverage 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 related health-care services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges;
(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 identifiable 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 or health plan.

Personal Representative: A individual's personal representative is the person who has the legal authority according to state law to act on the behalf of the individual in making decisions related to health care provided to the individual. It should not be assumed that a family member or caregiver is the personal representative of an individual.

Physical safeguards: Physical measures, policies, and procedures to protect a covered entity's electronic data and information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.

Public benefits plan: A government program providing health or other public benefits. Government agencies administering public benefits plans are also allowed to share eligibility or enrollment information with other government agencies administering public benefits programs, as required or expressly authorized by law. An example is that a Medicaid agency and an agency administering Temporary Assistance to Needy Families (TANF) benefits may maintain combined data system or share eligibility information.

Privacy: For purposes of the HIPAA Privacy Rule, privacy means an individual's right to control access to his/her personal health care information.

Protected Health Information: Information that is a subset of individually identifiable health information that is held by, transmitted or maintained in any form or medium by a covered entity. Protected health information excludes individually identifiable health information in education records covered by the Family Educational Right and Privacy Act (FERPA), and employment records maintained by a covered entity in its capacity as an employer.

Psychotherapy notes: The handwritten notes by 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 exclude 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. Psychotherapy notes are not to be

confused with progress notes, which are part of the medical record and are often required for payment.

Public Health Activities: Covered entities may disclose identifiable health information to:
(1) public health authorities authorized by law to collect or receive such information for preventing or controlling disease, injury, or disability and to public health or other government authorities authorized to receive reports of child abuse and neglect;
(2) entities subject to FDA regulation regarding FDA regulated products or activities for purposes such as adverse event reporting, tracking of products, product recalls, and post marketing surveillance;
(3) individuals who may have contracted or been exposed to a communicable disease when notification is authorized by law; and
(4) employers, regarding employees, when requested by employers, for information concerning a work-related illness or injury or workplace related medical surveillance, because such information is needed by the employer to comply with the Occupational Safety and Health Administration (OHSA), the Mine Safety and Health Administration (MHSA), or similar state law.

Public Health Authority: An agency or authority of the United States, a State, territory, political subdivision of a State or territory, Indian tribe, 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, its contractors or delegated persons that is responsible for public health matters as part of its official mandate.

Research: A systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge. The term research is used widely in the public sector but often for activities that do not meet this definition of research. While it is difficult to define exactly what is research, it is NOT:

(i) Quality improvement or assurance activities
(ii) Public health or health services activities designed to protect the public's health or for normal program functions
(iii) Any study or activity specific to or for a program's normal operations
(iv) Health care operations activities, such as activities for case management and care coordination, business planning and development, management and administration, or program evaluation or assessment
(v) Health oversight activities, including Federal program or grant oversight, audits, or investigations related to law enforcement, fraud and abuse, licensing and professional discipline

An activity may fall both in and out of the research definition depending on purpose, who conducts it, funding, and whether the activity is required by law.

Safeguards: Encompasses all of the administrative, physical, and technical actions used or taken to protect identifiable health information regardless of the medium or format.

Security or Security measures: Encompasses all of the administrative, physical, and technical safeguards related to electronic information and information systems. It refers to techniques for

ensuring that data stored in a computer cannot be accessed, read or compromised by any individuals without authorization.

Technical safeguards: The technology and the policy and procedures for its use that protect electronic identifiable health information and control access to it.

Transaction: The transmission of information between two parties to carry out financial or administrative activities related to health care. It includes the following types of information transmissions:
(1) Health care claims or equivalent encounter information
(2) Health care payment and remittance advice
(3) Coordination of benefits
(4) Health care claim status
(5) Enrollment and disenrollment in a health plan
(6) Eligibility for a health plan
(7) Health Plan premium payments
(8) Referral certification and authorization
(9) First report of injury
(10) Health claims attachments
(11) Other transactions that the Secretary of the Department of Health and Human Services may prescribe by regulation

Treatment: 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 individual; or the referral of an individual for health care from one health care provider to another.

Use: The internal sharing, employment, application, utilization, examination, or analysis of identifiable health information maintained by an organization. Just because identifiable health information is used internally, however, does not mean that there are no restrictions on its use.

User: A person or entity with authorized access.

Workforce: Under HIPAA, the employees, volunteers, trainees, and other persons under the direct control of a covered entity, whether or not they are paid by the covered entity.