Chapter 11 Patient Privacy Policies - GLOSSARY

https://wp.uthscsa.edu/pao/hop/11-toc/

Purpose

UT Health San Antonio Privacy Policies are intended to implement applicable provisions of the Health Insurance Portability and Accountability Act (HIPAA). The HIPAA privacy regulations are complex and include numerous defined terms. This glossary consists of technical terms on which the University's health information policies are based upon. It applies to all Chapter 11 Patient Privacy Policies.

Source

All section references in the definitions are references to Title 45 of the Code of Federal Regulations (CFR) Parts 160, 162, and 164, the HIPAA Administrative Simplification Regulation Text, U.S. Department of Health and Human Services, and the Office of Civil Rights, unless otherwise specified.

Definitions

Access - in connection with HIPAA security standards for the protection of electronic Protected Health Information, the ability, or the means necessary to read, write, modify, or communicate data/information or otherwise use any system resource.

Accounting of Disclosures - a list of certain disclosures of a patient's Protected Health Information, as required by HIPAA regulations.

Administrative Safeguards - the administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic PHI and to manage the conduct of workforce members in relation to the protection of that information.

Audio Monitoring/Recording - for the purpose of this policy, "audio recording" refers to monitoring and/or recording an individual's voice using video cameras, cellular telephones, tape recorders, wearable technology (e.g., Google Glass), or other technologies capable of capturing audio or transmitting it for monitoring purposes.

Authorization - the granting of permission to share specific information with a specific party for a specific purpose.

Breach - the unauthorized acquisition, access, use, or disclosure of unsecured protected health information which compromises the security or privacy of such information, except where an

unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information. Breach does not include the following circumstances:

a. Any unintentional acquisition, access, or use of protected health information by an employee or individual acting under the authority of a covered entity or business associate if (i) such acquisition, access, or use was made in good faith and within the course and scope of the employment or other professional relationship of such employee or individual, respectively, with the covered entity or business associate; and (ii) such information is not further acquired, accessed, used, or disclosed by any person;
b. Any inadvertent disclosure from an individual who is otherwise authorized to access protected health information at a facility operated by a covered entity or business associate to another similarly situated individual at the same facility; and any such information received as a result of such disclosure is not further acquired, accessed, used, or disclosed without authorization by any person; or
c. A situation in which an unauthorized person to whom the information is disclosed would not reasonably be able to retain the information (e.g., protected health information that was sent out by the post office is returned unopened, as undeliverable).

Business Associate (BA) - a person or entity, including their subcontractors, who provide certain services, activities, or functions for or to UT Health San Antonio, involving the use and/or disclosure of protected health information. This includes, but is not limited to, lawyers, auditors, third party administrators, health care clearing houses, data processing firms, billing firms, health information organizations, E-prescribing Gateways, companies providing maintenance to equipment with health information, and others with whom health information is shared. A business associate is not a UT Health San Antonio employee. Disclosures of protected health information by the organization to a healthcare provider for treatment purposes are not considered a business associate function.

Business Associate Agreement (BAA) - a contractual agreement that establishes a legally binding relationship between HIPAA-covered entities and business associates to ensure complete protection of protected health information. This agreement is necessary if business associates can potentially access protected health information during their work.

Business Associate Agreement (BAA) Analysis - a review of the proposed transaction between UT Health San Antonio and another person or company to determine whether the proposed transaction requires the execution of a BAA in accordance with HIPAA requirements.

Care Everywhere - an electronic health information exchange (HIE) application that connects hospitals and organizations using Epic, and that provides access at the point of care to the patient's electronic health records.

Confidentiality - the property that data or information is not made available or disclosed to unauthorized persons or processes. Confidential Information: Information including, but not limited to:

a. Health information relating to patients, research participants, and/or faculty, trainees/students, and other members of UT Health San Antonio's workforce, including, but not limited to, records containing Protected Health Information;
b. Education Records as defined by the Family Educational Rights and Privacy Act (FERPA);
c. Financial information including, but not limited to, account numbers;

d. Personnel and security information including, but not limited to, Social Security numbers, driver's license numbers, or other government-issued identification numbers;
e. Proprietary information related to research, intellectual property, and/or scientific discoveries;
f. All business and litigation information not deemed a Matter of Public Record; and/or,
g. Any other information considered confidential by law.

Confidential Patient - a patient who has been given Confidential Patient status in the electronic health record system.

Consent - for purposes of this policy, "consent" refers to the patient's or patient's personal representative's written acknowledgement and/or agreement of the use and/or disclosure of protected health information for treatment, payment, or health operations purposes or other reasons permitted by the HIPAA Privacy Rule.

Covered Entity (CE) - a health plan, a health care clearinghouse, or a health care provider who transmits any health information in electronic form in connection with furnishing, billing, or receiving payment for health care

Data Use Agreement (DUA) - a contractual agreement that governs the sharing of data between research collaborators who are covered entities under the HIPAA privacy rule. A DUA establishes the ways in which the information in a limited data set may be used by the intended recipient, and how it is protected.

De-identification of Protected Health Information Standard - health information that does not identify an individual and with respect to which there is no reasonable basis to believe the information can be used to identify an individual is not identifiable health information.

a. The following identifiers of the individual or of relatives, employers or household members of the individual must be removed:
    i. Names;
    ii. All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census:
        1) The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and
        2) The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.
    iii. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;
    iv. Telephone numbers;
    v. Fax numbers;
    vi. Electronic mail addresses;
    vii. Social Security numbers;
    viii. Health plan beneficiary numbers;
    ix. Account numbers;

x. Certificate/license numbers;
xi. Vehicle identifies and serial numbers, including license plate numbers;
xii. Device identifiers and serial numbers;
xiii. Web Universal Resource Locators (URLs);
xiv. Internet Protocol (IP) address numbers;
xv. Biometric identifiers, including finger and voice prints;
xvi. Full face photographic images and any comparable images; and
xvii. Any other unique identifying number, characteristic or codes; and
xviii. The covered entity does not have actual knowledge that the Information could be used to alone or in combination with other information to identify an individual who is subject of the information.

Designated Record Set - a group of records maintained by or for a covered entity that is:

a. The medical records and billing records about individuals maintained by or for a covered health care provider;
b. The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or
c. Used, in whole or in part, by or for the covered entity to make decisions about individuals.

For the purpose of this definition, 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.

Disclosure - release, transfer, provisions of, access to, or divulgence in any manner of information outside the entity holding the information.

Electronic Health Record (EHR) System - an integrated system of applications that work together to support patient care processes by integrating data from multiple sources, capturing data at the point of care, supporting caregiver decision-making, enabling appropriate documentation of and reimbursement for the care provided, and facilitating the dissemination of data with patients, referring providers, and other entities with a clinical, research, or business purpose to access patient information.

Electronic Health Information (EHI) - electronic protected health information as defined in 45 CFR 160.103 to the extent that it would be included in a designated record set as defined in 45 CFR 164.501, regardless of whether the group of records are used or maintained by or for a covered entity as defined in 45 CFR 160.103, but EHI should not include: (1) psychotherapy notes as defined in 45 CFR 164.501; or (2) information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding. EHI excludes de-identification.

Note: Starting April 5, 2021, EHI is limited to and will be synonymous with the data elements represented in the United States Core Data for Interoperability (USCDI) v1 standard. On or after October 6, 2022, EHI constitutes the definition above.

EpicCare Link - a Web application that allows non-UT Health San Antonio providers and research study monitors to view a patient's clinical data in UT Health San Antonio's electronic health record system.

Fundraising - the organized activity of raising funds for an institutional cause.

Fundraising Communication - a communication made to an individual by UT Health San Antonio, an institutionally related foundation, or a business associate on behalf of UT Health San Antonio for the purpose of raising funds for UT Health San Antonio. Fundraising communications include, but are not limited to, solicitations for donations or gifts, sponsorship of events, and communications for events or activities held to raise funds for the covered entity.

Genetic Information - information about an individual's genetic tests; the genetic tests of family members of an individual; and the manifestation of a disease or disorder in family members of an individual (i.e., family medical history). It includes the genetic information of a fetus carried by the individual or family member who is a pregnant woman; and any embryo legally held by an individual or family member utilizing an assisted reproductive technology. It excludes information about the sex or age of any individual.

Health Care Operations - certain administrative, financial, legal, and quality improvement activities of a covered entity that are necessary to run its business and to support the core functions of treatment and payment. These activities are limited to the following activities:

a. Conducting quality assessment and improvement activities, population-based activities relating to improving health or reducing health care costs, and case management and care coordination;
b. Reviewing the competence or qualifications of health care professionals, evaluating provider and health plan performance, training health care and non-health care professionals, accreditation, certification, licensing, or credentialing activities;
c. Underwriting and other activities relating 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 health care claims;
d. Conducting or arranging for medical review, legal, and auditing services, including fraud and abuse detection and compliance programs;
e. Business planning and development, such as conducting cost-management and planning analyses related to managing and operating the entity; and
f. Business management and general administrative activities, including those related to implementing and complying with the Privacy Rule and other Administrative Simplification Rules, customer service, resolution of internal grievances, sale or transfer of assets, creating de-identified health information or a limited data set, and fundraising for the benefit of the covered entity. General Provisions at 45 CFR 164.506.

Health Care Providers - individuals or other Covered Entities who are responsible for direct patient care or ancillary services provided to the patient. For example, Health Care Providers include the following persons or entities when involved in such direct patient care or ancillary services:

a. Staff Physicians
b. GME Residents and Fellows
c. Dentists, Podiatrists, and Medical Physicists
d. PhDs in the Division of Cancer Prevention
e. Registered Nurses, Advanced Practice Nurses, and Physician Assistants
f. Psychologists, Speech Pathologists, and Physical/Occupational Therapists
g. Pharmacists, Perfusionists, Respiratory Therapists, and Dieticians
h. Technicians, Social Workers, and Chaplains

i. Nursing Assistants
j. Students and trainees under direct supervision
k. Laboratories, clinics, and other health facilities
l. Medical groups and other professional groups providing health care to patients

Health Information Exchange (HIE) - electronic mechanisms for sharing health information about common patients with outside entities.

Health Oversight Agency - a federal, state, or local government agency authorized by law to. oversee the public and private health care system or government programs in which health information. is necessary for determining eligibility or compliance, or to enforce civil rights laws for which health information is relevant.

Health Insurance Portability and Accountability Act (HIPAA): a federal law that requires the creation of national standards to protect sensitive patient health information from being disclosed.

Hybrid Entity - a single legal entity that performs both functions that are subject to the HIPAA Privacy Standards and non-HIPAA covered functions and that segregates its covered functions from its non-covered functions for purposes of compliance with the HIPAA privacy standards.

Information Blocking: an act or omission ("Practice") that:

a. except as required by law or covered by an Information Blocking Exception, is likely to interfere with Access, Exchange, or Use of EHI; and
b. if conducted by:
    i. A Health Care Provider, such provider knows that such Practice is unreasonable and is likely to interfere with Access, Exchange or Use of EHI; or
    ii. A Health IT Developer of Certified Health IT or a HIN/HIE, such developer or HIE/HIN knows, or should know, that such Practice is likely to Interfere with Access, Exchange, or Use of EHI.

Information Blocking Exception - even if a Practice may interfere with access, exchange, or use of EHI, it may still be permissible if it complies with one or more of the following eight exceptions:

a. Preventing Harm Exception
b. Privacy Exception
c. Security Exception
d. Infeasibility Exception
e. Health IT Performance Exception
f. Content and Manner Exception
g. Fees Exception
h. Licensing Exception

Limited Data Set (LDS) - a limited amount of protected health information to be used or disclosed for Research, Public Health, or Health Care Operations that excludes the following direct identifiers of the individual or of relatives, employers, or household members of the individual:

a. Names;
b. Postal address information, other than town or city, state and ZIP code;

c. Telephone
d. Fax numbers;
e. Email address;
f. Social Security numbers;
g. Medical Record Numbers;
h. Health plan beneficiary numbers;
i. Account numbers;
j. Certificate/license numbers;
k. Vehicle identifiers and serial numbers, including license plate numbers;
l. Device identifiers and serial numbers;
m. URLs;
n. IP addresses;
o. Biometrics identifiers, including finger and voice prints; and
p. Full-face photographic images and any comparable images.

A limited data set may include the following information:

a. Dates relating to an individual, including birth date, death date, date of admission, date of discharge, dates of service;
b. City, State, and/or Five-digit ZIP code; and
c. Any other unique identifying number, characteristic, or code, such as study ID numbers and accession numbers.

Marketing - to make a communication about a product or service that encourages recipients of the communication to purchase or use the product or service. Marketing does not include a communication made:

a. 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.
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.

*For the purpose of this definition, 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.

Matter(s) of Public Record - event(s) about which information has been deemed available to the public (e.g., traffic and industrial accidents, crimes, and deaths).

Minimum Necessary - when using or disclosing protected health information or when requesting protected health information from another covered entity, a covered entity must make reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended

purpose of the use, disclosure, or request. This does not apply to disclosures for treatment and other specified purposes.

Organized Health Care Arrangement - includes the following:

a. A clinically integrated care setting in which individuals typically receive health care from more than one health care provider.
b. An organized system of health care in which more than one covered entity participates, and in which the participating entities;
    i. Hold themselves out to the public as participating in a joint arrangement;
    ii. Participate in joint activities that include at least one of the following:
        1) 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.
        2) Quality assessment and improvement activities, in which treatment provided by participating covered entities is assessed by other participating entities or by a third party on their behalf; or
        3) 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 entities or by a third party on their behalf for the purpose of administering the sharing of financial risk.
c. A group health plan and a health insurance issuer of 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.
d. A group health plan and one or more other group health plans each of which are maintained by the same plan sponsor; or
e. The group health plans described in item (d) 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.

Patient Representative - a surrogate decision maker who has decision-making capacity and is authorized by law and UT Health San Antonio policy to provide informed consent and participate in medical decision making on behalf of a patient when the patient lacks decision-making capacity. In the case of a deceased individual, the Patient Representative is the person with legal authority to act on behalf of the deceased individual or the deceased individual's estate.

Payment - encompasses the various activities of health care providers to obtain payment or be reimbursed for their services and of a health plan to obtain premiums, to fulfill their coverage responsibilities and provide benefits under the plan, and to obtain or provide reimbursement for the provision of health care. In addition to the general definition, the Privacy Rule provides examples of common payment activities which include, but are not limited to:

a. Determining eligibility or coverage under a plan and adjudicating claims;
b. Risk adjustments;
c. Billing and collection activities;

d. Reviewing health care services for medical necessity, coverage, justification of charges and the like;
e. Utilization review activities; and
f. Disclosures to consumer reporting agencies (limited to specified identifying information about the individual, his or her payment history, and identifying information about the covered entity).

Physical Safeguards - physical measures, policies, and procedures to protect a covered entity's electronic information systems and related buildings and equipment from natural and environmental hazards, and unauthorized intrusion. The standards under physical safeguards include facility access controls, workstation use, workstation security, and device and media controls.

Private Note - a type of Sensitive Note that is only viewable by certain users (e.g., mental health professionals, Health Information Management (HIM) staff, and other select users). Private Notes are not released without consulting with the physician or practitioner who created them, are not released without the patient's authorization, and are not available in UT Health San Antonio's MyChart.

Protected Health Information (PHI) - any information transmitted or maintained in any form or medium (including orally), that: a) is created or received by a health care provider, health plan, employer, or health care clearinghouse; b) relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual; and c) either identifies the individual or with respect to which there is a reasonable basis to believe the information can be used to identify the individual; provided that the term "PHI" does not include: a) education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. § 1232g, b) student treatment records described at 20 U.S.C. § 1232g(a)(4)(B)(iv), and c) employment records held by a Covered Entity in its role as employer, or d) records of a person who has been deceased for more than 50 years.

Psychotherapy Notes - 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 Activities - activities including, but not limited to, the reporting or disease, injury, vital events, and for the conducting of public health surveillance, investigation, and/or intervention.

Qualified Protective Order - an order of the court or administrative tribunal or stipulation that prohibits the parties from using or disclosing the protected health information for any purpose other than litigation or proceeding for which such information was requested and requires the return to the facility or destruction of the protected health information at the end of the litigation or proceeding.

Required by Law - a mandate contained in law that compels a covered entity to use or disclose protected health information which 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 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 such information if payment is sought under a government program providing public benefits.

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

Restriction Request - a written request from a patient or the patient's representative asking UT Health San Antonio to restrict or alter the manner in which UT Health San Antonio generally uses or discloses the patient's PHI, including requests to receive communications from UT Health San Antonio in an alternative format or at an alternative location.

Self-Pay Restriction Request - a type of Restriction Request in which a patient pays for a particular item or service in full and asks that no information about that item or service be disclosed to their health insurer.

Sensitive Information - information maintained by the institution that, while not Confidential Information, requires special precautions to prevent any disclosure that might harm or embarrass the subject of such information, including a patient or research participant; a faulty member, trainee/student, or other member of UT Health San Antonio's workforce; or the institution.

Technical Safeguards - the technology and the policy and procedures for its use that protect electronic protected health information and control access to it.

Texas Medical Records Privacy Act (TMRPA) - prohibits any release of protected health information for marketing purposes without consent or authorization from the individual.

Treatment - the provision, coordination, or management of health care and related services among health care providers or by a health care provider with a third party, consultation between health care providers regarding a patient, or the referral of a patient from one health care provider to another.

United States Core Data for Interoperability (USCDI) - the standardized set of health data classes and constituent data elements set forth at www.healthit.gov/USCDI.

Use - 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.

Video Monitoring - for the purposes of these policies, "video monitoring" refers to monitoring an individual or transmitting protected health information or the patient's likeness using technologies capable of transmitting a video (e.g., video cameras, cellular telephones, web cameras, wearable technology) regardless of whether the transmission is recorded.

Violation - failure to comply with an administrative simplification provision.

Workforce Member - employees, volunteers, trainees, or other persons whose conduct, in the performance of work for a covered entity or business associate, is under the direct control of UT Health San Antonio or its business associates, whether or not they are paid by UT Health San Antonio or the business associate.

Questions regarding this policy glossary should be directed to the Institutional Compliance and Privacy Office at 210-567-2014 or compliance@uthscsa.edu.