

DOCUMENT:
Section:
REVISION DATE:
PAGE:
Prepared by:
APPROVED BY:

Patient Access Definitions Protocol

Objective: To provide definitions to terms found in the Patient Access and Security Rules under HIPAA and the HITECH Act.

Responsibility: The **Medical Records Supervisors** is responsible for the maintenance of this protocol. All (Facility Name) Staff have a responsibility to assist in the maintenance of this protocol.

Definitions:

Access – refers to: the ability or the means necessary to read, write, modify or communicate patient data/information.

Administrative Safeguards – refers to: administrative actions, policy and protocols to manage the selection, development, implementation and maintenance of security measures to protect PHI in any format and to manage the conduct of the health centers workforce in relation to the protection of that PHI.

Patient – refers to:

- a. The person whose record is requested.
- b. Either current or former patient.

Patient Representative – refers to:

- a. Conservator/guardian of an adult.
- b. Attorney - in- Fact – a person authorized to make health care decisions under a patients Advanced Healthcare Directive.
- c. Parent or guardian of a minor patient (unless minor is entitled to consent).
- d. Beneficiary or personal representative of a deceased patient.

Patient Records – defined as: “in any form or medium maintained by, or in the custody or control of, health care provider, relating to the health history, diagnosis, or condition of a patient, or relating to treatment either provided or proposed.”

DOCUMENT:
Section:
REVISION DATE:
PAGE:
Prepared by:
APPROVED BY:

Patient Access Definitions Protocol

COIMA - California Confidentiality of Medical Information Act this is a State law that was passed and became effective 1/1/1982. It provides rules and regulations for the security, use and release of patient medical information in California. *(Please note that each state has specific regulations regarding Patient Health Information. If you need help in finding these regulations, additional resources and documentation contact your State Health Information Association or American Health Information Management Association, www.ahima.org)*

Confidentiality – defined as: ensuring that information is accessible only to those authorized to have access to PHI.

Designated Record Set (DRS) – defined as: “a group of medical/dental and billing records about individuals maintained by or for a covered health care provider and used to make health care decisions about the patient.”

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

Health Oversight Agency – defined as: 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 law for which health information is relevant.

HIPAA – Health Insurance Portability Accountability Act is a federal Law that as passed in 1996 and became effective in 2001.

1. The purpose of this law is to protect the privacy of a patient’s personal and health information.
2. Provides for the physical and electronic security of personal health information.

Health Care Provider/Covered Entity - refers to:

DOCUMENT:
Section:
REVISION DATE:
PAGE:
Prepared by:
APPROVED BY:

Patient Access Definitions Protocol

- a. All licensed Health Care Facilities, Clinics, Home Health Agencies, and certain licensed health care professionals (i.e., physicians, dentists, podiatrists, psychologists, optometrists, chiropractors, social workers).
- b. Health care provider who furnishes, bills, or is paid for health care and transmits health information electronically in connection with HIPAA covered transactions, health plans or health care clearinghouses.

Protected Health Information (PHI) – refers to: individually identifiable health information that is transmitted or maintained in any medium, written, oral or electronic.

Physical Safeguards – refers to: the physical measures, policies and procedures to protect a health centers paper and electronic health information systems and related buildings and equipment, from natural and environmental hazards and unauthorized intrusions.

Minimum Necessary – refers to: individual access to PHI granted by health center to perform required job duties.

Required by Law – defined as: A mandate contained in the law that compels a covered entity to make 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 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

DOCUMENT:
Section:
REVISION DATE:
PAGE:
Prepared by:
APPROVED BY:

Patient Access Definitions Protocol

TPO – defined as: “for treatment, payment and health care operations.”

Use – defined as: individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information.

Business Associate (BA) – defined as: a person whom a health center discloses PHI so that they can perform a function or activity on the health centers behalf.

Breach – defined as: “the inappropriate acquisition access to, and use or disclosure of unsecured patients medical information in a manner not permitted under the HIPAA regulations.”

Mandatory – defined as: disclosure of PHI under a legal process: court order, subpoenas criminal and civil, depositions, and parole hearing.

Discretionary – defines as: disclosure of PHI by a provider to prevent to lessen immediate serious threat to health and safety of identified person.

Subpoena – define as: an order to present self or to take or send patient health records in a legal proceeding.

Technical safeguards – refers to: technology and the policy and protocols for its use that protect electronic and paper health information and control access to it.

Red Flag – defined as: a pattern, practice or specific activity that could indicate identity theft. The Red Flag Rules are to go into effect 11/1/2010 but have been delayed 5 times.

Reference:

45 Code of Federal Regulation §§160 -164.524 (HIPAA)

California Confidentiality of Medical Information Act - Civil Code § 56 – 56.16

California Health and Safety Code §§ 123110, 123130;

Title 22 C.C.R.; California Code Regulation §§ 70751(b) and 71551(b)

DOCUMENT:
Section:
REVISION DATE:
PAGE:
Prepared by:
APPROVED BY:

Patient Access Definitions Protocol

Sections 13101-13402 of Title XIII (Health Information Technology for Economic and Clinical Health Act) of the American Recovery and Reinvestment Act of 2009;

Please note that each state has specific regulations regarding Patient Health Information. If you need help in finding these regulations, additional resources and documentation contact your State Health Information Association or American Health Information Management Association, www.ahima.org