ADMINISTRATIVE REGULATION 3953

SOUTH ORANGE COUNTY COMMUNITY COLLEGE DISTRICT

GENERAL INSTITUTION

HIPAA/CMIA PRIVACY

I. PURPOSE

Medical information regarding an individual is protected by the Confidentiality of Medical Information Act (CMIA), Calif. Civil Code, Section 56 et. seq., is a state law that adds to the federal protection of personal medical records under the Health Information Portability and Accountability Act (HIPAA) of 1996[1] . It is the intent of the District to protect health information in accordance with these laws.

This regulation is intended to do the following:

1. Serve as a foundation for the District's privacy practices;
2. Describe what health or health-related information is considered Protected Health Information (PHI)[2]
3. Designate the HIPAA privacy officer and complaint official; and
4. Require employee training in PHI. PHI can be defined as "individually identifiable information, relating to condition, treatment, or payment and transmitted or stored electronically or otherwise, which is created or received by or on behalf of the District or its health care components."

The colleges and the District Office shall also be responsible for developing additional procedures as necessary to safeguard PHI. Such procedures are subject to approval by the privacy officer and must be consistent with this regulation. This regulation pertains to all District individuals who have access to, use, or disclose PHI. The District's privacy officer develops and implements policies and regulations with respect to HIPAA compliance and receives HIPAA non-compliance allegations.

[1] "Summary of HIPAA Privacy Rule (2022):" U.S. Department of Health and Human Services: https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html

[2] "HIPAA Compliance Terms and Definitions You Should Know (2024)". https://insightassurance.com/hipaa-compliance-terms-and-definitions-you-should-know/

II. DEFINITIONS[3]

A. Authorization

Authorization means the execution of a written document required for the District to use or disclose PHI. Authorization must be obtained in advance of use or disclosure except for purposes of emergency treatment.

B. Breach

Is an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of PHI.

C. Breach Notification

Mandates that covered entities and their business associates notify individuals, the U.S. Department of Health and Human Services (HHS), and, in certain cases, the media of breaches of unsecured PHI.

D. Business Associate

A Business Associate (BA) is a person or an entity not a member of the District's workforce who performs a function and/or activity for a covered entity involving the use, disclosure or creation of PHI. The function and/or activity performed does not have to be a covered function and/or activity but must be a function and/or activity that the covered entity would have had to perform themselves. All entities that perform as a BA of the District will be required to enter into a BA agreement with the District. A BA could be, for example, a copy service that has access to PHI, or a flexible spending account's third party administrator.

E. Compliance

Refers to the adherence to the detailed requirements set forth in the legislation to effectively protect patient data and avoid penalties for non-compliance.

F. Covered Entity

A "covered entity" is a health plan, a health care clearinghouse, or a health care provider that transmits any health information in electronic form in connection with a HIPAA transaction as defined by HIPAA (45 C.F.R. § 160.103).

G. Covered Functions

Covered functions refers to those functions of a covered entity, the performance of which subjects the covered entity to the HIPAA requirements, i.e. use, disclosure, or creation of PHI.

[3] "HIPAA Compliance Terms and Definitions You Should Know (2024)". https://insightassurance.com/hipaa-compliance-terms-and-definitions-you-should-know/

H. Employee Training

Employee training on HIPAA policies and procedures is a crucial element in ensuring that staff understand how to handle PHI in compliance with HIPAA.

I. Enforcement Rule

Outlines the procedures for investigating HIPAA compliance and the penalties for violations.

J. Hybrid Entity

A hybrid entity is a single legal entity, portions of which are covered entities within the meaning of the HIPAA that perform covered functions. The District is such a hybrid entity (45 C.F.R. § 160.103). The District's operations that perform covered functions and, therefore, are designated as health care components, are the District's Student Health and Wellness Center at Saddleback College and the Health and Wellness Center at Irvine Valley College, which engage in standard electronic HIPAA transactions.

K. Limited Data Sets

PHI that excludes the direct identifiers of the individuals, relatives, employers, or household members of the individual, listed below in subsections 1 through 16, constitutes a limited data set. Limited data sets may be used or disclosed, without written authorization, where three criteria are met: (a) the use and/or disclosure is only for purposes of research, public health, or health care operations; (b) the covered entity obtains a data use agreement from the recipient whereby the recipient agrees to limit the use of the limited data set to the purpose allowed by the rules, to limit who can use or receive the data and not to re-identify the data or contact the individuals; and (c) where the covered entity does not have knowledge that the remaining information can be used to identify an individual.

1. Names;
2. Postal address information, other than town or city, state, and zip code;
3. Telephone numbers;
4. Fax numbers;
5. Electronic mail addresses;
6. Social security numbers;
7. Medical record numbers;
8. Health plan beneficiary numbers;
9. Account numbers;
10. Certificate/license numbers;
11. Vehicle identifiers and serial numbers, including license plate numbers;
12. Device identifiers and serial numbers;

13. Web Universal Resource Locators (URLs);

14. Internet Protocol (IP) address numbers;

15. Biometric identifiers, including finger and voice prints; and

16. Full face photographic images and any comparable images.

L. Notice of Privacy Practices

The District shall issue a "District Notice of Privacy Practices" for its covered entities. The notice shall specify individual rights under HIPAA as well as the District's contact information and the method of filing a complaint.

M. Omnibus Rule

Integrates provisions of the Health Information Technology for Economic and Clinical Health (HITECH) Act to strengthen patient privacy protections, broaden the scope of privacy and security rules, and increase penalties for non-compliance.

N. Privacy Rule

Establishes national standards for the protection of individuals' medical records and other personal health information.

O. Protected Health Information

For purposes of this regulation, Protected Health Information (PHI) (includes medical and psychological information covered by both HIPAA and the CMIA. PHI is any information that could specifically identify an individual's past, present, or future health condition. For example, medical billing records and a doctor's note. As a precautionary measure, all medical information shall be treated by District employees as PHI unless it can be clearly demonstrated to the privacy officer that said information is outside the scope of HIPAA or the CMIA.

P. Risk Assessment

Involves a comprehensive evaluation of potential risks and vulnerabilities to the confidentiality, integrity, and availability of PHI. It is a core component of achieving and maintaining HIPAA compliance.

Q. Safeguards

Mandates the implementation of three types of safeguards-administrative, physical, and technical- to ensure the confidentiality, integrity, and availability of PHI.

R. Sanctions

Refer to the penalties imposed for non-compliance, which can range from substantial financial fines to criminal charges in cases of severe violations.

S. Security

Security in this regulation is defined as all measures taken by the District and its agents, contractors, officers, and employees to ensure that PHI is protected in a manner that complies with the HIPAA and the CMIA. Security measures include, but are not limited to, policies, regulations, practices, directives, manuals, training, and methods as they relate to compliance with HIPAA and the CMIA. Security measures may also include mechanical and technological protections such as locks, secure access rooms and containers, computer hardware and software with security levels and protocols, secure communication devices and settings, and any other method, device, or practice that limits improper access to PHI.

III. REGULATION

A. Allowable Uses/Disclosures of PHI

PHI shall only be used and/or disclosed on a need-to-know basis or where authorization has been received. The District is responsible for physically protecting access to and modification of PHI whether available in paper, voice, or electronic form and establishment of safeguards and restrictions on access to records for certain public responsibilities, such as public health, research, and law enforcement. In general, PHI may not be used or disclosed by the District without an authorization except in the following circumstances:

1. When the information is provided to the individual whose PHI is released with a signed written consent from the patient. In addition, all students/patients should sign a release when they themselves request access to their records;
2. When the information is required by the United States Secretary of Health and Human Services to investigate compliance with the HIPAA;
3. When the information is requested pursuant to a valid subpoena with legal counsel approval;
4. When the information is part of a limited data set as defined above;
5. When the information is provided to another government agency that is administering a public benefit health plan;
6. When the individual, whose PHI is being disclosed, has been given an opportunity to contest the disclosure of PHI in advance;
7. When the information is used for public health activities authorized by law;
8. When disclosure of the information is necessary to report child abuse or neglect as authorized by law;
9. When the information is provided to a person who may have been exposed to a communicable disease;
10. When the information is disclosed to a government authority, which is authorized by law to receive reports of abuse, neglect, or domestic violence, because there is reasonable belief that the individual is a victim of abuse, neglect, and/or domestic violence;

11. When the information is used for law enforcement purposes;
12. When the District believes that disclosure of the information is necessary to avert a serious threat to health or safety;
13. When the information is used for government programs providing public benefits;
14. When the information is required for workers' compensation purposes;
15. When the information is used or disclosed to a business associate or to an institutionally related foundation for the purpose of raising funds for its own benefit. PHI released can only be in the form of demographic information relating to an individual and dates of health care provided to an individual used for fundraising;
16. When the information is disclosed for underwriting and related purposes.

When a covered entity must obtain an individual's authorization to use or disclose psychotherapy notes with the following exceptions: [4]

a. The covered entity who originated the notes may use them for treatment.

b. A covered entity may use or disclose, without an individual's authorization, the psychotherapy notes, for its own training, and to defend itself in legal proceedings brought by the individual, for HHS to investigate or determine the covered entity's compliance with the Privacy Rules, to avert a serious and imminent threat to public health or safety, to a health oversight agency for lawful oversight of the originator of the psychotherapy notes, for the lawful activities of a coroner or medical examiner, or as required by law.

B. Internal Audit

In order to ensure appropriate use and disclosure of PHI, each college and the District Office shall audit itself on a semi-annual basis. Each college and the District Office shall identify PHI in its possession, then determine whether there are potential HIPAA and CMIA violations and develop a plan for correction. Upon completion of the audit, the information shall be delivered to the District privacy officer. The privacy officer shall work with each college and the District Office to create a remediation plan, if necessary.

C. Individual Rights

An individual has the following rights as to their PHI protected under HIPAA. Individuals covered by HIPAA have the following rights:

1. The right to request restrictions on certain uses and disclosures of protected health information as provided by 45 C.F.R. § 164.522(a);
2. The right to receive their PHI confidentially as provided by 45 C.F.R. § 164.522(b), as applicable;

[4] "OCR Privacy Brief: Summary of the HIPAA Privacy Rule (2003): United States Department of Health and Human Services. https://www.hhs.gov/sites/default/files/privacysummary.pdf.

3. The right to inspect and copy their PHI held in the covered entity's designated record set as provided by 45 C.F.R. § 164.524;
4. The right to request amendments to their PHI held in the covered entity's designated record set as provided by 45 C.F.R. § 164.526; and
5. The right to receive an accounting of disclosures of PHI as provided by 45 C.F.R. § 164.528.

For individually identifiable medical information protected by the CMIA, but not HIPAA, an employee shall have the right to review and copy their medical information.

D. District Privacy Official and Contact Person

The District privacy official is the Vice Chancellor of Human Resources. The privacy official is responsible for resolving complaints under HIPAA and/or the CMIA, as well as questions regarding the Notice of Privacy Practices. This official shall be identified as the person to receive complaints of alleged HIPAA and/or CMIA violations. Specific duties include, but are not limited to:

1. Develop privacy policies and regulations pursuant to HIPAA and the Notice of Privacy Practice;
2. Develop training documents for the workforce on policies and regulations regarding PHI;
3. Set up a complaint process and sanctions;
4. Track all PHI;
5. Ensure policies are implemented for determining when an individual can inspect, copy, amend, or request restrictions on their PHI disclosures;
6. Receive complaints from individuals concerning violations of HIPAA and/or CMIA and requirements;
7. Log all complaints received and tracking the disposition of the complaints;
8. Review complaints for allowable uses and disclosures and disposing of complaints that identify allowable uses and disclosures;
9. Review complaints for non-HIPAA and/or non-CMIA related issues and refer individuals to the appropriate organization, if any;
10. Identify and investigate all HIPAA and/or CMIA-related complaints including allegations of: inappropriate use or disclosure of PHI; inappropriate disposal of PHI; denial of access to PHI; and denial of amendments to PHI;
11. Coordinate and collaborate with members of the workforce to investigate and develop actions to resolve the complaints;
12. Resolve complaints, seeking approval of the resolution (from the complainants), and oversee implementation of the resolution. Resolutions may include changes in business

practices or information technology changes, personnel actions, contract changes, or terminations, etc.;

13. Serve as the District's liaison with the federal and/or state government with respect to any inquiries into HIPAA and/or CMIA privacy violation complaints.

E. Sanctions and Penalties

Employees may be subject to discipline, up to and including termination for violations of this regulation, which includes the inappropriate use or disclosure of PHI, in accordance with existing provisions of law, policies of the Board, or applicable collective bargaining agreements.

In addition, federal authorities may sanction employees and the District for violations of the HIPAA Privacy Rule as follows:

1. Civil Money Penalties (CMP):[5]

Penalties will vary significantly depending on factors such as the date of the violation, whether the covered entity knew or should have known of the failure to comply, or whether the covered entity's failure to comply was due to willful neglect. Penalties may not exceed a calendar year cap for multiple violations of the same requirement.

2. Criminal penalties for violations of the Privacy Rule:

a. A person who knowingly and in violation of the Privacy Rule either (a) obtains individually identifiable health information relating to an individual; or (b) discloses individually identifiable information to another person may have a criminal penalty assessed against them. Any violator may be fined up to $50,000 or imprisoned for up to one (1) year, or both;

b. Where a known violation is committed under false pretenses, the person may be fined up to $100,000 or imprisoned for up to five (5) years, or both;

c. Where a known violation is committed with the intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm, a person can be fined up to $250,000, and/or incarcerated for not more than ten (10) years.

Any violation of CMIA that results in economic loss or personal injury to a patient is punishable as a misdemeanor. Any person and/or entity that negligently, knowingly, or willfully discloses medical information, in violation of CMIA, may be assessed fines or civil penalties.

F. Training

The District shall train employees so that they understand their obligations under this regulation. The training requirement may be satisfied by providing new employees with a copy of this privacy regulation and documenting that new members have reviewed the

[5] "Health Information Privacy-Summary of HIPAA Privacy Rule (2022):" U.S. Department of Health and Human Services, www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html.

regulation. From time to time, the District may provide training through live instruction, video presentations, or interactive software programs.

G. Audit and Compliance

Each college and the District Office are responsible for compliance with this regulation. The privacy officer may, in their discretion, audit and examine the procedures and practices of any college and the District Office to ascertain compliance with the requirements of this regulation.