Live Well. Health Matters.

POLICY TITLE: COMPLIANCE WITH PRIVACY REQUIREMENTS FOR HEALTH INFORMATION
POLICY NUMBER: 4200

COMMITTEE APPROVAL DATE: 12/09/2022 **WRITTEN/REVISED BY**: T. BAKALY
BOARD APPROVAL DATE: 01/25/2023 **SUPERSEDES:** 07/27/2022

POLICY:

4200 It is the policy of the Beach Cities Health District's ("District") to adhere to both Federal and State requirements related to the privacy, security, and confidentiality of health care related information ("health information") that is created, received, used, maintained, or transmitted within the District's relevant operations. It is the intent that this policy shall constitute the security policies and privacy policies mandated by the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

SCOPE:

4200.1 In carrying out its preventative health mission to enhance community health through partnerships, programs and services for people who live and work in Hermosa, Manhattan and Redondo Beach, the District recognizes the applicability of the Health Insurance Portability and Accountability Act of 1996, as amended by the Health Information Technology for Economic and Clinical Health Act (HITECH Act), the Part 2- Confidentiality of Substance Use Disorder Patient Records regulations (Part 2), as well as several California state laws, including the Confidentiality of Medical Information Act (CMIA) and the Patient Access to Health Records Act (PAHRA).

4200.2 Under HIPAA, the District can elect to be a Hybrid Entity with identified Health Care Components which are subject to HIPAA and Non-Covered Components which are not. Hybrid entities must document designations of covered Health Care Components and must include any component that would meet the definition of a covered entity if it were a separate legal entity. **This Policy designates the District as a Hybrid Entity under HIPAA and identifies the Health Care Components subject to HIPAA's privacy, security, breach notification and enforcement provisions and the District's Health Information Privacy Program.**

4200.3 The District's Health Information Privacy Program Policies and Procedures will comply with Title 45 CFR Parts 160-164, including, specifically the Privacy Rule, the Security Rule, and the Breach Notification Rule requirements in 45 CFR §§164.102 – 164.534, Title 42 CFR Part 2, and the requirements in Sections 56 - 56.37 of the California Civil Code and Sections 123100 - 123149.5 of the California Health & Safety Code. The District will ensure that all workforce members will be subject to these regulations and internal policies and procedures.

4200.4 The District will implement a Health Information Privacy Program that is designed to ensure compliance with the various privacy, security and confidentiality requirements that apply to client health information created, received, used, maintained, or transmitted in its daily operations, particularly for its Health Care Components.

RESPONSIBILITY:

4200.5 It is the responsibility of all workforce members involved in creating, receiving, using, maintaining, or transmitting client health information within the District's relevant operations to follow the policies outlined here to comply with the applicable Federal and State privacy, confidentiality, and security requirements.

REQUIREMENTS:

4200.6 The District will meet the following requirements related to its operations involving client health information:

4200.6.1 HIPAA Hybrid Entity Status

4200.6.1.1 The District has elected to be a Hybrid Entity, with identified Health Care Components which are subject to HIPAA and Non-Covered Components which are not. Hybrid entities must document designations of covered Health Care Components and must include any component that would meet the definition of a covered entity if it were a separate legal entity. As a HIPAA Hybrid Entity, the District has identified and designated the following departments and/or operations as Health Care Components, as outlined below. See the mapping diagram in Attachment A to the policy for more information.

4200.6.1.2 As a HIPAA Hybrid Entity, the District has identified and designated the following departments and/or operations as Health Care Components, which means they will comply with the HIPAA requirements, as well as the District Health Information Privacy Program policies and procedures. See the mapping diagram in Attachment A to the policy for more information.

4200.6.1.2.1 Certified Enrollment Entity Services (services performed on behalf of Covered California)
4200.6.1.2.2 Health & Fitness Operations – Centers for Health & Fitness (as a Health Care Provider)
4200.6.1.2.3 Health Fund (as a Health Plan)
4200.6.1.2.4 allcove Beach Cities (as a Health Care Provider)
4200.6.1.2.5 Life Span Areas – Community Services (as a Health Care Provider)

4200.6.1.3 The following departments of the District, to the extent they provide support services to the District Health Care Components in the course of providing health care provider treatment, payment and operations or health plan actions, will also comply with the District Health Information Privacy Program requirements. See the mapping diagram in Attachment A to the policy for more information.

4200.6.1.3.1 Executive Department
4200.6.1.3.2 Finance/Financial Services
4200.6.1.3.3 Information Technology Services
4200.6.1.3.4 Volunteer Services
4200.6.1.3.5 Human Resources

4200.6.1.4 The following departments of the District are not considered Health Care Components under HIPAA and will not be required to comply with the District Health Information Privacy Program policies and procedures. See the mapping diagram in Attachment A to the policy for more information.

4200.6.1.4.1 Administration Services
4200.6.1.4.2 Adventure Plex
4200.6.1.4.3 Well Being Services (including WorkWell)
4200.6.1.4.4 Health Promotions
4200.6.1.4.5 Property Operations
4200.6.1.4.6 Youth Services

4200.6.1.5 The District will ensure that all workforce members carrying out operations within the Health Care Components will be subject to HIPAA and required to comply with the HIPAA Privacy, Security

and Breach Notification Rule, as well as the District Health Information Privacy Program policies and procedures.

4200.6.1.6 The District will develop and implement safeguard procedures to ensure that its Health Care Components do not disclose PHI to another component of the District in circumstances in which the HIPAA Privacy Rule would prohibit such disclosure if the Health Care Component and the other component were separate and district legal entities.

4200.6.1.7 The District will develop and implement safeguard procedures to ensure that its Health Care Components apply protections to its electronic PHI as required under the HIPAA Security Rule, and that these protections apply to other components of the District as if the Health Care Component and the other component were separate and district legal entities.

4200.6.1.8 The District will develop and implement safeguard procedures to ensure that where a person performs duties for both the Health Care Component, in the capacity of a member of the workforce of such component, and for another component of the entity, in the same capacity with respect to that component, such workforce member must not use or disclose PHI created or received in the course of or incident to the workforce member's work for the Health Care Component in a way prohibited by the HIPAA Privacy Rule.

4200.6.1.9 The District will maintain a written or electronic record of its hybrid designation (i.e., this policy) and will update the policy when any new Health Care Components are added, or revisions are made to the current listing of Health Care Components for the Hybrid Entity.

4200.6.2 Health Information Privacy Program

4200.6.2.1 The District will designate Privacy Officer and Security Officer responsibilities to an employee(s) who will be tasked with development, implementation, and oversight of the Health Information Privacy Program.

4200.6.2.2 The District will implement policies and procedures with respect to client health information that comply with HIPAA, the Confidentiality of Substance Use Disorder Patient Records regulations (42 CFR part 2), and California state regulations. The District will perform regular, ongoing monitoring, assessment, and revision, as necessary, of the Health Information Privacy Program policies and procedures and documentation in response to environmental, operational, workforce, technical, or legal changes including, but not limited to those aspects of the District's operations affecting the confidentiality, integrity, or availability of its client health information.

4200.6.2.3 The District will implement a training program that informs all workforce members, including management, of the policies and procedures that apply to them in their individual roles, as related to client health information. Health Information Privacy Program training will be provided to new workforce members upon employment and annually thereafter for existing workforce members.

4200.6.2.4 The District will promptly document and process any complaints of alleged HIPAA, Part 2, or state law violations, mitigate any damages, and investigate and address any violations.

4200.6.2.4.1 The District will provide a Compliance Hotline (844-986-1434) as a process for workforce members and clients to submit complaints concerning violations of policies and procedures regarding the use or disclosure of health information or its compliance with its Privacy Program policies and procedures.

4200.6.2.4.2 All District workforce members are responsible for reporting misconduct, including actual or potential violations of law, regulation, policy, and procedures.

4200.6.2.4.3 Any form of retaliation against a workforce member who reports a perceived violation of any HIPAA, Part 2 or California state law related policy or procedure in good faith is strictly prohibited, and any workforce member who commits or condones any form of retaliation will be subject to discipline up to, and including, termination.

4200.6.2.5 The District will develop and implement safeguard procedures to ensure that it does not disclose PHI in circumstances in which the HIPAA Privacy Rule, Part 2 or California state law would prohibit such disclosures.

4200.6.2.6 The Chief Privacy Officer will perform regular, ongoing monitoring, assessment, and revision, as necessary, of business processes and operations to ensure continued compliance and enforcement of Health Information Privacy Program standards.

4200.6.2.7 The District will mitigate to the extent practicable, any harmful effect that is known to the District of a use or disclosure of client health information in violation of its policies and procedures by the District or its business associate.

4200.6.2.8 The District will have and apply appropriate sanctions against workforce members who fail to comply with the Health Information Privacy Program policies and procedures of the District or the requirements of the HIPAA, Part 2 and applicable state law regulations, up to and including termination and any other legal remedies as appropriate, including referral for criminal or civil prosecution.

4200.6.2.9 No client will be required to waive their rights to file a complaint with Department of Health and Human Services (HHS) Office for Civil Rights (OCR) as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits by the District.

4200.6.2.10 The District will enter into a written business associate agreement with every organization or vendor that creates, receives, maintains, or transmits client health information on its behalf and will contractually obligate its business associates to enter into a business associate agreement with any subcontractor used to create, receive, maintain, or transmit the District's client health information on its behalf.

4200.6.2.11 The District will all ensure that all Health Information Privacy related assessments, monitoring activities, mitigation activities, policies and procedures, and business associate agreements are documented and maintained in writing.

4200.6.3 HIPAA Privacy Rule Requirements.

4200.6.3.1 The District will comply with federal HIPAA requirements (except for client information covered by more stringent Part 2 regulations or state privacy requirements) pertaining to the following rights held by the District clients, including:

4200.6.3.1.1 A client's right to request to inspect or copy their own health information records maintained by or for the District, specifically those records that are defined as the Designated Record Set under District procedure. This right is referred to as a "Client Access Request." See 45 CFR §164.524 of the HIPAA regulations for more information.

4200.6.3.1.2 A client's right to request that an amendment be made to their health information records maintained by the District. This right is referred to as a "Client Amendment Request." See 45 CFR §164.526 of the HIPAA regulations for more information.

4200.6.3.1.3 A client's right to request additional restrictions on how their health information may be accessed or disclosed by the District. This right is referred to as a "Client Restriction Request." See 45 CFR §164.522(a) of the HIPAA regulations for more information.

4200.6.3.1.4 A client's right to request to receive communications of their PHI by alternative means or at alternative locations. This right is referred to as a "Client Alternative Communication Request." See 45 CFR §164.522(b) of the HIPAA regulations for more information.

4200.6.3.1.5 A client's right to request an accounting of disclosures made by the District of the client's PHI (with some exceptions). This right is referred to as a "Client Accounting of Disclosure Request." See 45 CFR §164.528 of the HIPAA regulations for more information.

4200.6.3.2 The District will provide a formal notice, in writing, to its clients regarding how the District will use and disclose their health information pursuant to the HIPAA Privacy Rule standard for notice of privacy practices for PHI. See 45 CFR §164.520 of the HIPAA regulations for more information.

4200.6.3.3 The District may only use or disclose client health information, that does not meet the definition of a Part 2 program – substance use disorder patient records, subject to Part 2 regulations, without obtaining a client's written authorization for the following purposes: (1) To the client (unless required for access or accounting of disclosures); (2) For treatment, payment, and health care operations; (3) In some circumstances, where the client is given the opportunity to agree or object to the use or disclosure; (4) Incident to an otherwise permitted use and disclosure; (5) For public interest and benefit activities; (6) Where a limited data set is used for the purposes of research, public health or health care operations; and (7) Where necessary to cooperate with an investigation of a covered entity or business associate's compliance with HIPAA by the Secretary of the Department of Health and Human Services. See 45 CFR §164.506, 45 CFR §164.508, 45 CFR §164.510 and 45 CFR §164.512 of the HIPAA regulations for more information.

4200.6.3.4 For all other uses and disclosures of a client's health information, the District will obtain a valid, signed authorization from the client, unless the use or disclosure is required or otherwise permitted without an authorization by HIPAA, Part 2 or relevant California state law. See 45 CFR §164.508 of the HIPAA regulations for more information.

4200.6.3.5 The District workforce members will only access a client's records if the access is necessary to carry out the workforce member's job duties, functions, and/or responsibilities. See 45 CFR §164.502(b) and 45 CFR §164.506 of the HIPAA regulations for more information.

4200.6.3.6 The District workforce members will follow proper procedures to ensure that only the minimum amount of client health information necessary to accomplish the specific purpose of their job is used, disclosed, or requested. See 45 CFR §164.502(b) of the HIPAA regulations for more information.

4200.6.3.7 The District will follow proper procedures addressing when and/or if to treat an individual as the personal representative of a client with respect to using or disclosing their health information. See 45 CFR § 164.502(g) of the HIPAA regulations for more information.

4200.6.3.8 The District will follow proper procedures when determining whether to accept and process a documented authorization from a client requesting that their health information be used or disclosed to an individual other than themselves. See 45 CFR §164.508 of the HIPAA regulations for more information.

4200.6.3.9 The District will allow clients to request and receive an accounting of all instances where their PHI has been used or disclosed by the District within the last six years or since implementation of the Health Information Privacy Program, except for uses and disclosures of PHI made by the District for the following purposes: (a) To carry out treatment, payment, or health care operations; (b) Under the authority of a written authorization given by the subject of PHI; (c) To the client about their own PHI; (d) To persons involved in the client's care or other notification purposes; (e) For national security or intelligence purposes; (f) To correctional institutions or law enforcement custodial situations; and (g) As part of a limited data set. See 45 CFR §164.528 of the HIPAA regulations for more information.

4200.6.4 HIPAA Security Rule Requirements

4200.6.4.1 The District will implement appropriate administrative, technical, and physical safeguards to protect the privacy of client health information.

4200.6.4.2 The District will maintain and comply with security policies that address the following:

4200.6.4.2.1 Administrative security: Formal mechanisms for risk analysis and management, information access controls, information systems review and evaluations, incident reporting and response procedures, security awareness and training, configuration control and management, acceptable and secure use of workstations and portable devices/media, a backup and disaster recovery strategy, appropriate sanctions for failure to comply, and oversight of business associates.

4200.6.4.2.2 Workforce security: Formal mechanisms for ensuring workforce and contractors only have access to health information and other sensitive information for which they have the appropriate authority and clearance, as needed and defined by their roles or job duties, as well as processes for personnel termination and sanctions for violations of HIPAA requirements and/or security procedures.

4200.6.4.2.3 Physical safeguards: Ensure assigned security responsibilities, physical access controls including facility security plan to safeguard areas where electronic health information is housed, such as data centers or areas where digital media and devices are stored, repaired, or disposed of. Implement workstation security measures and procedures for proper disposal, re-use, backup and tracking of device and media containing electronic health information.

4200.6.4.2.4 Technical security: Establish technical access controls including user identification and password management policies, emergency access procedures, authorization controls, encryption and data/entity access and authentication.

4200.6.4.2.5 Transmission security: Establish mechanisms to safeguard against unauthorized access to electronic health information, data alteration or loss during transmission, such as encryption.

4200.6.4.3 The District will maintain and comply with security procedures that include:

4200.6.4.3.1 Regular evaluations of compliance with security measures.

4200.6.4.3.2 Conducting periodic security risk analysis, risk management and risk auditing activities.

4200.6.4.3.3 Contingency plans for emergencies and disaster recovery.

4200.6.4.3.4 Security incident reporting and response mechanisms, processes, and protocols.

4200.6.4.3.5 Testing and revision of security procedures, measures and mechanisms, and continuous improvement.

4200.6.4.3.6 Security awareness and training.

4200.6.4.3.7 Sanction policy.

4200.6.4.4 The District will maintain and comply with appropriate security measures and technical mechanisms to guard against unauthorized access to electronically stored and/or transmitted health information, and protect against reasonably anticipated threats and hazards, for example: (a) Integrity controls; (b) Authentication controls; (c) Access controls; (d) Encryption; and (e) Abnormal condition alarms, audit trails, entity authentication, and event reporting.

4200.6.4.5 The District will oversee and/or perform on-going security monitoring of the District's information systems, including the following activities:

4200.6.4.5.1 Performing periodic information security risk assessments;

4200.6.4.5.2 Conducting gap analyses to determine the extent to which key business areas and infrastructure comply with statutory and regulatory requirements;

4200.6.4.5.3 Evaluating and recommending new information security technologies and countermeasures against threats to information security or privacy; and

4200.6.4.5.4 Ensuring compliance through adequate training programs and periodic security audits.

4200.6.5. HIPAA and California State Law Breach Notification Rule Requirements

4200.6.5.1 The District will comply with the breach identification and notification provisions of HIPAA, as well as relevant California state law (see the *Compliance with California Requirements Regarding Personal Information Policy*), by carrying out the following:

4200.6.5.1.1 All District workforce members will be required to report any potential or actual instances of a breach of client health information immediately to the Privacy Officer/Security Officer.

4200.6.5.1.2 The District will promptly investigate all reports of potential breaches in accordance with organizational policies and procedures. If the investigation determines that a breach has occurred, the District will take reasonable steps provide the required notifications and to mitigate the breach.

4200.6.5.1.3 In the event of a breach or a use or disclosure of client health information in violation of HIPAA or applicable California state law, the District will have the burden

of demonstrating that all required notifications were made, or that the use or disclosure of client health information did not constitute a breach.

4200.6.5.1.4 Following the discovery of a breach, the District will notify the following parties, as necessary: (a) Clients; (b) Media; (c) Department of Health and Human Services Office for Civil Rights (HHS OCR); (d) Other state authorities (as necessary, for example: California Attorney General or California Office of Information Security within the Department of Technology; and (e) Business associates (as necessary).

4200.6.6 CFR Part 2 Requirements

4200.6.6.1 The District will implement processes to ensure that substance use disorder patient records, subject to Part 2 regulations, are disclosed or used only as permitted by the Part 2 regulations and may not otherwise be disclosed or used in any civil, criminal, administrative, or legislative proceedings conducted by any federal, state, or local authority.

4200.6.6.2 The District will implement processes to ensure that it does not use or disclose substance use disorder patient records, subject to Part 2 regulations, regarding a client without first obtaining a written consent, subject to several exceptions, as outlined in the Part 2 regulations. This includes restrictions on disclosures to third-party payers, administrative entities, and others, as defined by Part 2.

4200.6.6.3 The District will implement processes to ensure compliance with consent to treatment for minor patients, as required by Part 2.

4200.6.6.4. The District will maintain formal policies and procedures to reasonably protect against unauthorized uses and disclosures of patient identifying information and to protect against reasonably anticipated threats or hazards to the security of patient identifying information, which address paper records and electronic records, as required by Part 2.

4200.6.6.5. The District will implement processes for disclosure of substance use disorder patient records, subject to Part 2 regulations, without patient consent for medical emergencies, as defined by Part 2 regulations.

4200.6.6.6. The District will implement processes for disposition of records if it discontinues operations or is taken over or acquired by another program.

4200.6.6.7. The District will communicate to its clients that federal law and regulations protect the confidentiality of substance use disorder patient's records; and provide a formal notice, in writing, to its clients containing a summary of the federal law and regulations, in accordance with Part 2 requirements.

4200.6.6.8 The District will follow proper procedures to provide patients access to their own records, including the opportunity to inspect and copy any records maintained about the patient.

4200.6.6.9. The District will follow proper procedures to disclose patient identifying information for the purposes of the recipient conducting scientific research, in accordance with Part 2 regulations

4200.6.6.10 The District will follow proper procedures to disclose records containing patient identifying information for audits and evaluations, in accordance with Part 2 regulations.

4200.6.6.11 The District will follow proper procedures for disclosing information in response to court orders, in accordance with Part 2 regulations.

4200.6.6.12 The District will direct the report of a violation of the Part 2 regulations to the United States Attorney for the judicial district in which the violation occurs.

4200.6.7 California CMIA Requirements

4200.6.7.1 The District will implement processes to ensure that it does not disclose Medical Information, as defined by CMIA, regarding a client without first obtaining a valid authorization, subject to several exceptions outlined in the CMIA.

4200.6.8 California PAHRA Requirements

4200.6.8.1 The District will implement processes to ensure that it provides access to PAHRA defined Patient Records, including health care records or summaries of those records, for clients and individuals having responsibility for decisions respecting the health care of clients, including the right to inspect and/or receive a copy of their records.

4200.6.8.2 The District will also allow a client who inspects his or her Patient Records the right to provide to the health care provider a written addendum with respect to any item or statement in his or her records that the client believes to be incomplete or incorrect, which shall be attached to the client's records and included if the health care provider makes a disclosure of the allegedly incomplete or incorrect portion of the client's records to any third party.

4200.6.9 Document Retention

4200.6.9.1 This policy, and documentation created to evidence compliance with this policy, will be retained for a period of at least 6 years from the date of its creation or the date when it was last in effect, whichever is later, and as noted within Policy 1040: *Records Retention*.

EXCEPTIONS:

4200.7 The Chief Executive Officer is the only person authorized to make exceptions to this policy.

DEFINITIONS:

4200.8

Breach: Breach is the acquisition, access, use, or disclosure of client health information in a manner not permitted under HIPAA or state law, which compromises the security or privacy of the health information.

Business Associate: A person or entity that creates, receives, maintains, or transmits health information on behalf of a HIPAA Covered Entity or another Business Associate.

Client: Individuals who obtain services from the District.

Covered Entity: (1) A health plan; (2) a health care clearinghouse; and (3) a health care provider who transmits protected health information in electronic form in connection with a HIPAA covered transaction.

Covered Functions: Means those functions of a HIPAA Covered Entity where the performance of the functions makes the entity a health plan, a health care provider or a health care clearinghouse.

Designated Record Set: Under HIPAA, a "designated record set" is defined as a group of records maintained by or for a covered entity that comprises the: (1) Medical records and billing records about individual clients maintained by or for a covered health care provider; (2) Enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or (3) Other records that are used, in whole or in part, by or for the covered entity to make decisions about clients. This last category includes records that are used to make decisions about any clients, whether or not the records have been used to make a decision about the particular client requesting access.

Health Care Component: Any component, or combination of components, of the District which would meet the definition of a HIPAA Covered Entity if it were a separate legal entity and which has been designated as part of the District Hybrid Entity due to its component activities. See Section 4200.6.1 of this Policy for more information regarding the District's designated Health Care Components.

Health Information: Information that meets the definitions of Medical Information (as defined by CMIA), Patient Records (as defined by PAHRA), and/or Protected Health Information (as defined by HIPAA).

Hybrid Entity: Per HIPAA, the term "Hybrid Entity" means a single legal entity: (1) That is a covered entity; (2) Whose business activities include both covered and non-covered functions; and (3) That designates Health Care Components in accordance with 45 CFR §164.105(a)(2)(iii)(D) of the HIPAA regulations. The District has designated itself as a Hybrid Entity, as outlined in Section 4200.6.1 of this Policy.

Medical Information: Under the California Confidentiality of Medical Information Act (CMIA), Medical Information means any individually identifiable information, in electronic or physical form, in possession of or derived from a provider of health care, health care service plan, pharmaceutical company, or contractor regarding a client's medical history, mental or physical condition, or treatment. Individually identifiable means that the Medical Information includes or contains any element of personal identifying information sufficient to allow identification of the individual client, such as the client's name, address, electronic mail address, telephone number, or social security number, or other information that, alone or in combination with other publicly available information, reveals the individual's identity.

Minor: Under the Part 2 regulations, means an individual who has not attained the age of majority specified in the applicable state law, or if no age of majority is specified in the applicable state law, the age of 18 years.

Part 2 Program: Under the Part regulations, means a federally assisted program (federally assisted as defined in § 2.12(b) and program as defined in this section). See § 2.12(e)(1) for examples.

Particularly Sensitive Health Information: Health information that is generally considered highly confidential including, but not limited to, mental health, drug and alcohol abuse, and communicable disease information.

Patient: Under the Part 2 regulations, means any individual who has applied for or been given diagnosis, treatment, or referral for treatment for a substance use disorder at a part 2 program. *Patient* includes any individual who, after arrest on a criminal charge, is identified as an individual with a substance use disorder in order to determine that individual's eligibility to participate in a part 2 program. This definition includes both current and former patients.

Patient Identifying Information: Under the Part 2 regulations, means the name, address, social security number, fingerprints, photograph, or similar information by which the identity of a patient, as defined in this section, can be determined with reasonable accuracy either directly or by reference to other information.

The term does not include a number assigned to a patient by a part 2 program, for internal use only by the part 2 program, if that number does not consist of or contain numbers (such as a social security, or driver's license number) that could be used to identify a patient with reasonable accuracy from sources external to the part 2 program.

Patient Records: Under the California Patient Access to Health Records Act (PAHRA), a Patient Record is defined to mean records in any form or medium maintained by, or in the custody or control of, a health care provider relating to the health history, diagnosis, or condition of a client, or relating to treatment provided or proposed to be provided to the client. A Patient Record includes only records pertaining to the client requesting the records or whose representative requests the records. Patient Records does not include information given in confidence to a health care provider by a person other than another health care provider or the client, and that material may be removed from any records prior to inspection or copying under Section 123110 or 123115 of PAHRA. A Patient Record does not include information contained in aggregate form, such as indices, registers, or logs.

Program: Under the Part 2 regulations, means:

(1) An individual or entity (other than a general medical facility) who holds itself out as providing, and provides, substance use disorder diagnosis, treatment, or referral for treatment; or

(2) An identified unit within a general medical facility that holds itself out as providing, and provides, substance use disorder diagnosis, treatment, or referral for treatment; or

(3) Medical personnel or other staff in a general medical facility whose primary function is the provision of substance use disorder diagnosis, treatment, or referral for treatment and who are identified as such providers.

Protected Health Information (PHI): Under HIPAA, PHI is defined as information, including genetic information, created, or received by a Covered Entity which relates to: (1) an individual client's past, present, or future physical or mental health or condition; or (2) the provision of health care to a client; or (3) the past, present, or future payment for the provision of health care to a client. And as to any such information, the information identifies the client or there is a reasonable basis to believe it can be used to identify the client.

Qualified service organization: Under the Part 2 regulations, means an individual or entity who:

(1) Provides services to a part 2 program, such as data processing, bill collecting, dosage preparation, laboratory analyses, or legal, accounting, population health management, medical staffing, or other professional services, or services to prevent or treat child abuse or neglect, including training on nutrition and child care and individual and group therapy, and

(2) Has entered into a written agreement with a part 2 program under which that individual or entity:

(i) Acknowledges that in receiving, storing, processing, or otherwise dealing with any patient records from the part 2 program, it is fully bound by the regulations in this part; and

(ii) If necessary, will resist in judicial proceedings any efforts to obtain access to patient identifying information related to substance use disorder diagnosis, treatment, or referral for treatment except as permitted by the regulations in this part.

Records: Under the Part 2 regulations, means any information, whether recorded or not, created by, received, or acquired by a part 2 program relating to a patient (*e.g.,* diagnosis, treatment and referral for treatment information, billing information, emails, voice mails, and texts), provided, however, that information conveyed orally by a part 2 program to a non-part 2 provider for treatment purposes with the consent of the patient does not become a record subject to this Part in the possession of the non-part 2 provider merely because that information is reduced to writing by that non-part 2 provider. Records

otherwise transmitted by a part 2 program to a non-part 2 provider retain their characteristic as records in the hands of the non-part 2 provider, but may be segregated by that provider. For the purpose of the regulations in this part, records include both paper and electronic records

Substance Use Disorder: Under the Part 2 regulations, means a cluster of cognitive, behavioral, and physiological symptoms indicating that the individual continues using the substance despite significant substance-related problems such as impaired control, social impairment, risky use, and pharmacological tolerance and withdrawal. For the purposes of the regulations in this part, this definition does not include tobacco or caffeine use.

Third-party payer*:* Under the Part 2 regulations, means an individual or entity who pays and/or agrees to pay for diagnosis or treatment furnished to a patient on the basis of a contractual relationship with the patient or a member of the patient's family or on the basis of the patient's eligibility for federal, state, or local governmental benefits.

Treatment Under the Part 2 regulations, means the care of a patient suffering from a substance use disorder, a condition which is identified as having been caused by the substance use disorder, or both, in order to reduce or eliminate the adverse effects upon the patient.

Treating provider relationship Under the Part 2 regulations, means that, regardless of whether there has been an actual in-person encounter:

(1) A patient is, agrees to, or is legally required to be diagnosed, evaluated, and/or treated, or agrees to accept consultation, for any condition by an individual or entity, and;

(2) The individual or entity undertakes or agrees to undertake diagnosis, evaluation, and/or treatment of the patient, or consultation with the patient, for any condition.

Workforce or Workforce Member: Employees, contractors, volunteers, interns, trainees, and other persons whose conduct, in the performance of work for the District, is under its direct control, regardless of whether they are paid by the District.

REFERENCES:

4200.9

The HIPAA Privacy Rule can be found at 42 CFR. Part 164 Subpart A:
http://www.ecfr.gov/cgi-bin/text-idx?SID=0483960b0a53d93800f7c95d70ebe75c&mc=true&node=sp45.1.164.a&rgn=div6

and 42 CFR Part 164 Subpart E:
http://www.ecfr.gov/cgi-bin/text-idx?SID=0483960b0a53d93800f7c95d70ebe75c&mc=true&node=sp45.1.164.e&rgn=div6

The HIPAA Security Rule can be found at 42 CFR Part 164, Subpart C:
http://www.ecfr.gov/cgi-bin/text-idx?SID=0483960b0a53d93800f7c95d70ebe75c&mc=true&node=sp45.1.164.c&rgn=div6

The Breach Notification Rule can be found at 42 CFR Part 164, Subpart D:
http://www.ecfr.gov/cgi-bin/text-idx?SID=0483960b0a53d93800f7c95d70ebe75c&mc=true&node=sp45.1.164.d&rgn=div6

Part 2 - Confidentiality of Substance Use Disorder Patient Records:
https://www.ecfr.gov/current/title-42/chapter-I/subchapter-A/part-2

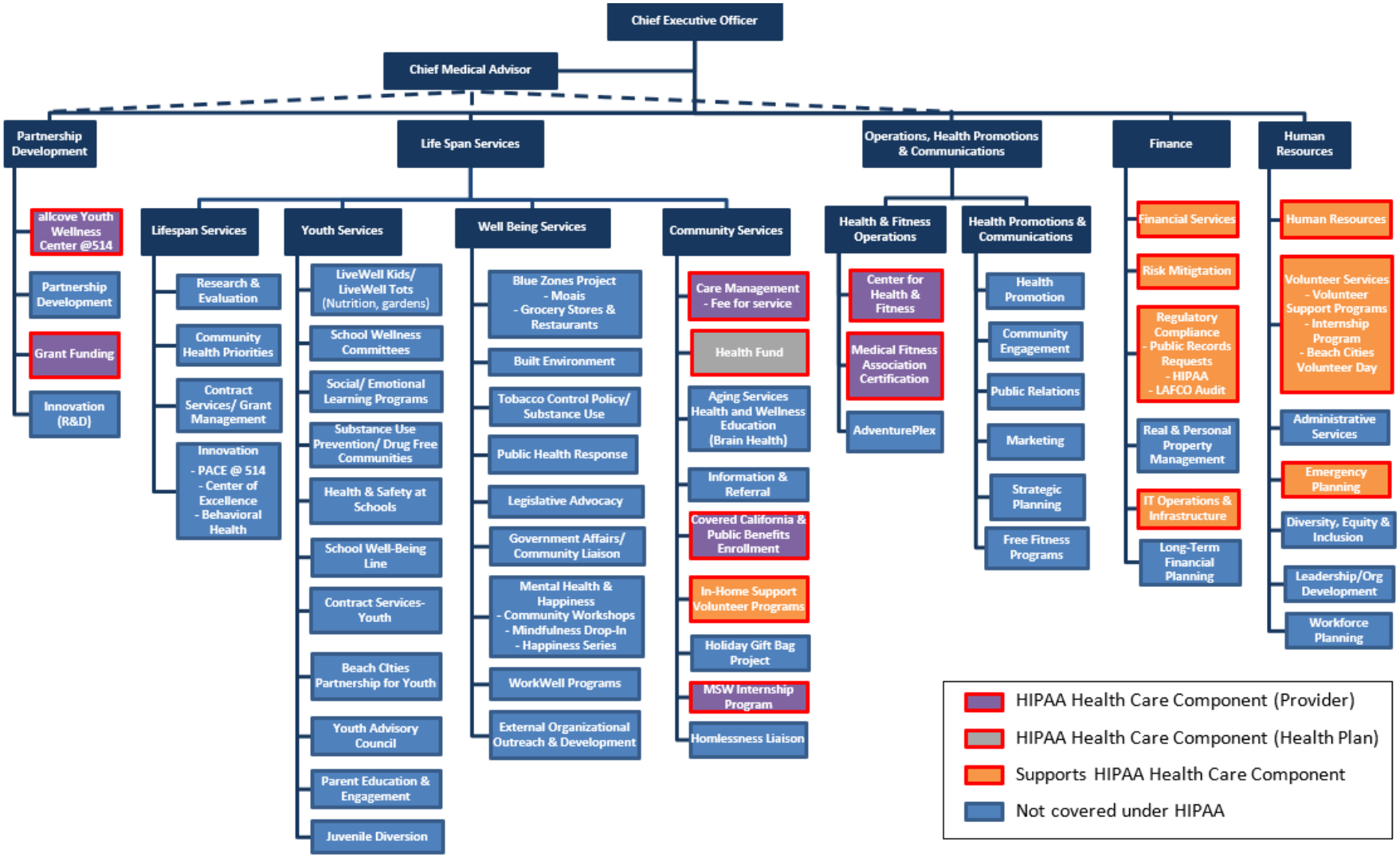
California Confidentiality of Medical Information Act and implementing regulations found in Sections 56 - 56.37 of the California Civil Code:
https://leginfo.legislature.ca.gov/faces/codes_displayexpandedbranch.xhtml?lawCode=CIV&division=1.&title=&part=2.6.&chapter=1.&article=&goUp=Y

California Patient Access to Health Records Act (PAHRA) and implementing regulations found in Sections 123100 - 123149.5 of the California Health & Safety Code:
https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=HSC&division=106.&title=&part=1.&chapter=1.&article=

ATTACHMENTS

4200.10
4200.10.1 Attachment A – HIPAA Hybrid Covered Entity Organization Chart
4200.10.2 Attachment B – HIPAA Overview

Attachment A – HIPAA Hybrid Covered Entity Organization Chart



Attachment B – HIPAA Overview

Health Insurance Portability and Accountability Act Overview

The Health Insurance Portability and Accountability Act ("HIPAA") of 1996 (Public Law 104-191) was enacted on August 21, 1996 to combat fraud, waste and abuse, improve the portability of health insurance coverage, and simplify the administration of health care. The initial core elements under the Administrative Simplification portion of the Act were designed to improve the efficiency and effectiveness of health care management by standardizing the interchange of electronic data for specified administrative and financial transactions and protecting the security and confidentiality of client identifiable health information. HIPAA laws have been strengthened since the law was initially introduced. The Health Information Technology for Economic and Clinical Health Act ("HITECH Act"), enacted as part of the American Recovery and Reinvestment Act of 2009, addressed the privacy and security concerns associated with the electronic transmission of health information. Notably, the HITECH Act extended liability for compliance with the complete Security provisions and certain Privacy provisions to business associates of covered entities, as well as mandated notification requirements for incidents involving the breach of protected health information ("PHI"). A portion of the regulations implementing the HITECH Act changes were released as part of the HIPAA Omnibus Final Rule, published on January 25, 2013. The HIPAA Omnibus Final Rule, which has a compliance date of September 23, 2013, made significant modification to various areas of HIPAA compliance, including business associates, business associate agreements, breach notification, enforcement, marketing, fundraising, research, genetic information, and notice of privacy practices.

Three categories of individuals/entities are covered under HIPAA: (1) covered entities; (2) business associates; and (3) subcontractors. **Covered entities** are health care providers, health plans and health care clearinghouses that provide, bill for, or receive payment for health care and electronically submit covered transactions that include PHI. Covered entities are required to comply with all applicable provisions under the HIPAA Privacy, Security, and Breach Notification Rules. A covered entity that qualifies as a **hybrid entity**, meaning that the entity is a single legal entity that performs both covered and non-covered functions, may choose whether it wants to be a hybrid entity. If such a covered entity decides not to be a hybrid entity then it, and all of its components, are subject to the HIPAA Rules in its entirety. If a covered entity decides to be a hybrid entity, it must define and designate its health care component(s), including those components that function as health care providers, health plans or health care clearinghouses and engage in standard electronic transactions. All health care component(s) must be included in the hybrid entity's health care component(s) and are subject to the HIPAA Rules.[1]

Business associates are individuals and organizations that create, receive, maintain, or transmit PHI on behalf of a covered entity. Examples of business associates include: claims auditors,

[1] For example, per OCR guidance, a hybrid entity, such as a university, has the option to include or exclude a research laboratory, that functions as a health care provider but does not engage in electronic transactions, as part of the hybrid entity's health care component. If such a research laboratory is included in the hybrid entity's health care component, then the employees or workforce members of the laboratory must comply with the HIPAA Rules. But if the research laboratory is excluded from the hybrid entity's health care component, the employees or workforce members of the laboratory are not subject to the HIPAA Rules.

attorneys, third party billing entities, storage companies, cloud service vendors, IT auditors, and transcription services. Business associates are required to comply with all requirements under the HIPAA Security Rule, as well as certain provisions of the HIPAA Privacy and Breach Notification Rules.

Subcontractors are individuals or organizations that create, receive, maintain, or transmit PHI on behalf of a business associates, other than as a member of the business associate's workforce. HIPAA treats subcontractors as business associates under the regulations and requires them to comply with the same requirements.

Under HIPAA, a covered entity must execute a business associate agreement ("BAA") with each of its business associates to ensure that the privacy and security of its PHI is protected when it is handled by third parties. A covered entity may not contractually authorize its business associate to make any use or disclosure of PHI that would violate the HIPAA Rule. Similarly, a business associate must execute a subcontractor BAA with each of its subcontractors and a subcontractor must execute a subcontractor BAA with each of its downstream contractors.

The Department of Health and Human Services ("HHS") Office for Civil Rights ("OCR") is responsible for implementing and enforcing the HIPAA rules. A covered entity or business associate that fails to comply with the HIPAA rules may be subject to multiple violations of up to a $1.5 million cap for each violation. Historically, OCR has investigated and resolved over 25,695 cases by requiring changes in privacy practices and corrective actions by, or providing technical assistance to, HIPAA covered entities and their business associates. Further, from November of 2011 through December of 2012, OCR conducted a pilot audit program to evaluate HIPAA compliance of all types of covered entities. The purpose of the pilot program was to identify entities' weaknesses and vulnerabilities related to HIPAA compliance. Based on that experience and the results of the evaluation, OCR implemented Phase 2 of the audit program in 2016. OCR is in the process of implementing a permanent audit program that will evaluate both covered entities' and business associates' compliance with specific high-risk areas of the HIPAA Privacy, Security and Breach Notification Rules.

The HIPAA law is generally divided into three Rules: The Privacy Rule, Security Rule, and Breach Notification Rule. As a general note, federal compliance guidance for each of the HIPAA Rules recognizes each health care institution as a unique entity, and therefore acknowledges that no "best standard" for HIPAA compliance exists. As such, the implementation of HIPAA requirements should be individually tailored for each institution according to what is "reasonable and appropriate."

The **HIPAA Privacy Rule** outlines regulations addressing the authorized uses and disclosures of PHI and the rights of clients with regard to their health information. PHI is generally defined as any information about health status, the provision of health care, or payment for health care that can be linked to an individual. PHI includes medical records and any other individually identifiable health information in any form (written, verbal, or electronic). Individually identifiable information is information, including demographic data, which is explicitly linked to an individual or reasonably expected to permit individual identification. Individually identifiable information includes many common identifiers, such as name, address, birth date, and Social Security Number.

A covered entity is permitted to use and disclose PHI, without an individual's written authorization, for the following purposes:

1. To the individual (unless required for access or accounting of disclosures);
2. For treatment, payment, and health care operations;
3. Where the individual is given the opportunity to agree or object;
4. Incident to an otherwise permitted use and disclosure;
5. For public interest and benefit activities; and
6. Where a limited data set is used for the purposes of research, public health or health care operations.

A covered entity is required to obtain the individual's written authorization for any use or disclosure of PHI that is not for treatment, payment, or health care operations or otherwise permitted or required by the Privacy Rule.

The Privacy Rule requires covered entities to develop and implement policies and procedures, and make reasonable efforts to use, disclose, and request only the minimum amount of PHI needed to limit uses and disclosures to the minimum necessary. Organization policies and procedures that address the access, use and disclosure of PHI must identify the individuals, or classes of individuals in the workforce, who need access to PHI to carry out their duties, the categories of PHI to which access is needed, and any conditions under which they need the information to do their jobs. Under the Privacy Rule, each covered entity must also provide a notice of its privacy practices, which contain required elements under the Privacy Rule. The Notice of Privacy Practices contains information on uses of PHI, explanation of privacy rights, responsibilities of covered entities, and the complaint process.

The Privacy Rule also provides individuals with several rights with respect to their own PHI, including the right to access their information and request amendments where they disagree with content included in their medical record. Individuals may also request restrictions on how the covered entity uses or discloses their information and may ask that their information be communicated in a means that is confidential. Additionally, individuals have the right to request an accounting of the disclosures of their PHI made by a covered entity or business associate. Covered entities must develop and implement policies to ensure that individual's rights to PHI are properly respected and followed by its workforce.

The **HIPAA Security Rule** is intended to complement the Privacy Rule. The Security Rule deals specifically with "electronic protected health information" ("ePHI") and establishes three main types of security safeguards required for compliance: administrative, physical, and technical. Prior to the enactment of HIPAA, no generally accepted set of security standards or general requirements for PHI existed in the health care industry. A main goal of the Security Rule is to protect the privacy of ePHI while permitting covered entities, business associates, and subcontractors to adopt new technologies to improve the quality and efficiency of client care. Specifically, under the Security Rule, covered entities, business associates, and subcontractors must:

1. Ensure the confidentiality, integrity, and availability of all ePHI they create, receive, maintain or transmit;
2. Identify and protect against reasonably anticipated threats to the security or integrity of the information;
3. Protect against reasonably anticipated, impermissible uses or disclosures; and
4. Ensure compliance by all relevant workforce members.

The Security Rule covers PHI transmitted or maintained in electronic form and does not apply to PHI transmitted orally or in writing. Examples of ePHI that are considered "in motion" or "at rest" include: emails, information stored on network drives and electronic systems, information shared between applications, and information stored on laptops, PDAs, mobile phones, CDs, thumb drives, and other portable media. Under the administrative safeguard provisions in the Security Rule, covered entities, business associates, and subcontractors are required to perform a risk analysis as part of their security management processes. The risk analysis process includes assessing the likelihood and impact of potential risks to ePHI and implementing appropriate security measures to address those risks. Covered entities, business associates, and subcontractors must also document their security measures and maintain continuous, reasonable, and appropriate security protections. Physical safeguards of the Security Rule require covered entities, business associates, and subcontractors to limit physical access to its facilities while ensuring that authorized access is allowed. Technical Safeguards of the Security Rule require covered entities, business associates, and subcontractors to implement access controls, audit controls, integrity controls, and transmission security controls.

The **HIPAA Breach Notification Rule** sets forth regulations that require covered entities and their business associates to provide notification following a breach of unsecured PHI. A breach is defined as the impermissible acquisition, access, use, or disclosure of PHI which comprises the security and privacy of such information. An impermissible use or disclosure of PHI is presumed to be a breach unless the covered entity or business associate demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment using four main criteria. The three exceptions to the definition of breach include: (1) unintentional acquisition, access or use of PHI by a workforce member or individual acting under the authority of the covered entity or business associate; (2) inadvertent disclosures between authorized persons at the covered entity or business associate; and (3) unauthorized disclosures in which the unauthorized person would not have been able to retain the information.

Upon a breach of unsecured PHI, covered entities are required to provide notification to the affected individuals within 60 days following the discovery of the breach. For a breach that involves the PHI of 500 or more individuals, covered entities must also notify individuals via the media and notify HHS within 60 days following the breach. For breaches that involve fewer than 500 people, the covered entity must report the breach to HHS no later than 60 days after the end of the calendar year in which the breaches are discovered. Business associates are required to notify covered entities that a breach has occurred without reasonable delay and no later than 60 days from the discovery of the breach, and in accordance with the terms of a Business Associate Agreement between the business associate and the covered entity. A covered entity or business associate should maintain documentation that all required notifications were made or documentation that demonstrates that notification was not required.