AG.601 HIPAA COMPLIANCE OVERVIEW

Approved By:	Board of Directors	Adopted Date:	6/22/20
Distribution:	All Staff	Revision Date(s):	
Category:	Administration & Governance	Reviewed Date(s):	

Printed copies are for reference only. Please refer to the electronic copy of this document for the latest version.

Notice: Under the federal HIPAA laws, those provisions of HIPAA concerning the privacy and confidentiality of a person's health information "give way" to those California state laws provisions, and other federal law provisions, that are more stringent than HIPAA.

ODCHC staff should follow California law or other federal law if it provides greater protection than HIPAA. If you are unsure which law to follow please contact the ODCHC Compliance Officer.

PURPOSE:

To outline how Open Door Community Health Centers (ODCHC) meets the requirements of 45 Code of Federal Regulations (CFR), Part 164, known as the Health Insurance Portability and Accountability Act of 1996 (HIPAA), and current State of California Privacy Laws. This policy references the ODCHC Policies that comprise the ODCHC HIPAA Compliance Program and provides an overview of the guidelines and expectations for the necessary collection, use, and disclosure of protected health information about individuals, while maintaining reasonable safeguards to protect privacy of their protected health information.

DEFINITIONS:

Access: The ability or means necessary to read, write, modify, or communicate data/information or otherwise use any ODCHC system.

Administrative Safeguards: Administrative actions policies and procedures to manage the selection, development, implementation and maintenance of security measures to protect electronic data, protected health information, and to manage the conduct of the ODCHC or business associate staff in relation to the protection of that information.

Breach: The acquisition, access, use, or disclosure of protected health information (PHI) in a manner not permitted under the Privacy Rule.

A breach does not include:

- Any unintentional acquisition, access, or use of PHI by staff or a person acting under the authority of a covered entity if made in good faith and within the scope of the authority, with no further use or disclosure.
- Any inadvertent disclosure by a person authorized to access PHI at the same covered entity or business associate, or organized healthcare arrangement in which the covered entity participates, to any authorized person, and the PHI is not further used or disclosed.
- Any disclosure of PHI where the covered entity or business associate has a good faith belief the unauthorized person would not reasonably have been able to retain such information.

The covered entity or business associate must be able to show that there is a low probability that the information has been compromised based upon a risk assessment of at least the following:

- The nature and extent of the PHI involved, including the identifiers.
- The unauthorized person who used the PHI or to whom the disclosure was made.

Approved By:	Board of Directors	Adopted Date:	6/22/20
Distribution:	All Staff	Revision Date(s):	
Category:	Administration & Governance	Reviewed Date(s):	

- Whether the PHI was actually acquired or viewed.
- The extent to which the risk to the PHI has been mitigated.

Business Associate: A person or organization (or their subcontractor), who is not a member of ODCHC staff, who creates, receives, maintains, or transmits PHI or electronic protected health information (EPHI) on behalf of a HIPAA covered component. Services that a Business Associate (BA) provide may include claims process or administration, data analysis, utilization review, quality assurance, billing, benefit management, document destruction, temporary administrative support, legal, actuarial, accounting, consulting, information processing support, health information organizations, e-prescribing gateways or providers of data transmission services, and certain patient safety activities. A covered entity may be a BA of another covered entity concerning the treatment of the individual.

Client: An individual who requests or receives health services from ODCHC.

Confidentiality: Ensuring that data or information is not made available or disclosed to unauthorized persons or processes.

Covered Entity: A health plan, health care clearing house or health care provider who transmits health information in an electronic form in connection with a transaction to carry out financial or administrative activities related to health care. (A covered entity may also maintain protected health information in paper records).

De-Identified Health Information: Information that does not identify an individual because identifiers have been removed. Identifiers include name, address, geographic subdivisions smaller than a state, dates, phone or fax numbers, email addresses, URLs, IP addresses, biometric identifiers, medical record numbers, social security numbers health plan identification numbers, certificate/license numbers, account numbers, vehicle identification numbers, photographic images, and any other unique identifiers.

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

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

For purposes of this definition, the term record set means any item, collection or grouping of information that includes PHI and is maintained, used, collected, or disseminated by or for the covered entity.

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

EHR: Electronic Health Record (also known as the EMR – Electronic Medical Record) means an electronic record of health-related information on an individual that is created, gathered, managed and consulted by authorized health care clinicians and staff.

Electronic Media:

Approved By:	Board of Directors	Adopted Date:	6/22/20
Distribution:	All Staff	Revision Date(s):	
Category:	Administration & Governance	Reviewed Date(s):	

- Electronic storage material on which data is or may be recorded electronically, including devices in computers (hard drives) or removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card.
- Transmission media used to exchange data already in electronic storage media, such as the internet, intranet, leased lines, dial-up lines, private networks, physical movement of removable/transportable electronic storage media.

Encryption: Scrambling or encoding electronic data to prevent unauthorized access or use. Only individuals with knowledge of a password or key can decrypt the data. Encryption methods use an algorithmic process that transforms the data into a form in which there is a low probability of assigning a meaning to it without the use of a confidential process or key.

ePHI: Protected health information (PHI) that is transmitted by electronic media; maintained in electronic media; or transmitted or maintained in any other form or medium.

E-Prescribing Gateway: An organization providing an electronic network connection for the purpose of transmitting medical prescriptions from a HIPAA covered health care provider to an external pharmacy through standardized electronic messages that both the prescriber's system and the pharmacist's system must implement. An e-prescribing gateway organization is required to be a Business Associate of the covered entity.

Genetic Information: PHI that contains any individual's genetic tests, or those of a family member of the individual; the manifestation of a disease or disorder in family members of such individual, any request for, or receipt of, genetic services or clinical research including genetic services. Genetic information excludes information about the sex or age of the individual

Group Health Plan: An individual or group plan that provides, or pays the cost of, medical care

Health Care Operations: The following are some examples of activities of the covered entity meeting the definition of health care operations:

- Quality assessments and improvement activities, including outcomes evaluation and development of clinical guidelines, population based activities relating to improving health care or reducing health care costs, protocol development, case management, care coordination, contracting of health care providers and patients with information about treatments alternatives, and related functions that do not include treatment;
- Competence or qualifications review of health care professionals, evaluating practitioner and performance, health plan performance, conducting training programs for health care providers with supervision, training of non-health care professionals, accreditation, certification, licensing, or credentialing activities;
- Underwriting, premium rating and other activities relating to creating, renewal or replacement of health insurance contract or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating claims for health care;
- Medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs;
- Business planning and development, such as cost management and planning related analysis related to managing and operating the entity;

Approved By:	Board of Directors	Adopted Date:	6/22/20
Distribution:	All Staff	Revision Date(s):	
Category:	Administration & Governance	Reviewed Date(s):	

- Business management and general administrative activities of the entity, including, but not limited to: customer service, resolution of internal grievances, the sale, transfer, merger, or consolidation of all or part of the covered entity with another covered entity.

Health Information Organization (HIO): Performs activities on behalf of one or more HIPAA covered entities to manage the exchange of PHI through an electronic network. In that role, HIOs are defined by HIPAA as Business Associates of the covered health care providers. Also known as Health Information Exchanges (HIEs), they may be governmental, non-profit or for profit organizations.

HIPAA- 45 CFR: The Health insurance Portability and Accountability Act of 1996 (HIPAA), public Law 104-191, was enacted on August 21, 1996 to ensure that individuals' health information is protected while allowing the flow of health information required to provide high quality health care. It is referred to as 45 CFR (Congressional Federal Register). Part 160 deals with General Administrative Requirements; Part 164 concerns security and privacy. The main sections of Part 164 are: Subpart C: known as the Security Rule (protection of electronic protected health information-EPHI); Subpart D: known as the Notification Rule in case a breach of unsecured protected health information; and Subpart E: known as the Privacy Rule (Standards to ensure the privacy of individually identified health information.

HITECH Act: Health Information Technology for Economic and Clinical Health (HITECH) Act is Title XIII of Division A of the American Recovery and Reinvestment Act of 2009 (ARRA) signed on February 17, 2009. HITECH contains privacy and security enhancements to HIPAA, financial incentives, grants and loans for adopting electronic health records (EHRs) and increased penalties for HIPAA violations.

Institutional Review Board: A committee formally designated by a covered entity to approve, monitor, and review medical research with the aim to protect the rights and welfare of the research subjects.

Individually Identifiable: Information that is a subset of health information, including demographic information collected from an individual, and either directly identifies that individual or it is reasonable to expect that the information can identify the individual.

Law Enforcement Official: An officer or employee of any agency or authority of the United States, a State, territory, a political subdivision of a State or territory, or an Indian tribe, who is empowered by law to investigate or conduct an official inquiry into potential violation of law, or prosecute or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law.

Limited Data Set: A limited data set is PHI that excludes the following direct identifiers of the individual or of relatives, employers, or household members of the individual: Names; Postal address information, other than city or town, State, and zip code; Telephone numbers; Fax numbers; Electronic mail addresses; Social Security numbers; Medical record numbers; Health plan beneficiary numbers; Account numbers; Certificate/license numbers; Vehicle identifiers and serial numbers, including license plate numbers; Device identifiers and serial numbers; Web Universal Resource Locators (URLs), Internet Protocol (IP) address numbers; Biometric identifiers, including finger and voice prints; Full face photographic images and any comparable images.

Approved By:	Board of Directors	Adopted Date:	6/22/20
Distribution:	All Staff	Revision Date(s):	
Category:	Administration & Governance	Reviewed Date(s):	

Minimum Necessary: Use and disclosure of protected health information (PHI), other than for treatment, payment or health care operations, is limited to the minimum necessary to accomplish the intended purpose of such use, disclosure, or request. The covered entity or Business Associate disclosing the PHI is the one who determines the "minimum necessary".

Omnibus Rule: Modification to the HIPAA, Privacy, Security, Enforcement, and Breach Notification Rules under the HITECH Act and Genetic Information Nondiscrimination Act (GINA), and other modifications to the HIPAA Rules. Effective date March 26, 2013, compliance date September 23, 2013.

Payment:

Payment means the activities undertaken by:

- A health plan to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the health plan; or
- A health care provider or health plan to obtain or provide reimbursement for the provision of health care.

Payment activities include, but are not limited to:

- Determinations of eligibility or coverage (including coordination of benefits or the determination of cost sharing amounts) and adjudication or subrogation of health benefit claims;
- Risk adjusting amounts due based on enrollee health status and demographic characteristics;
- Billing, claims management, collection activities, obtaining payment under a contract for reinsurance (including stop loss insurance and excess of loss insurance, and related healthcare data processing;
- Review of health care services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges;
- Utilization review activities, including precertification and preauthorization of services, concurrent and retrospective review of services; and
- Disclosure to consumer reporting agencies of any of the following PHI relating to collection of premiums or reimbursement: name and address, date of birth, social security number, payment history, account number, and name and address of the health care provider and /or health plan.

Physical Safeguards: Physical measures, policies, and procedures to protect a covered entity's or business associate's electronic information systems and related buildings and equipment, from natural and environmental and unauthorized intrusion.

Plan Administration Functions: Administrative functions performed by group health plan sponsor on behalf of the group health plan, excluding functions performed by the plan sponsor in connection with any other benefit or benefit plan of the sponsor.

Protected Health Information (PHI): PHI is health information that a covered entity creates or receives that identifies an individual, and relates to:

- The individual's past, present, or future physical or mental health or condition.
- The provision of health care to the individual.
- The past, present, or future payment for the provision of health care to the individual.

Approved By:	Board of Directors	Adopted Date:	6/22/20
Distribution:	All Staff	Revision Date(s):	
Category:	Administration & Governance	Reviewed Date(s):	

PHI includes written, spoken and electronic forms. PHI is "individually identifiable information". PHI excludes individually identifiable information in education records, school health records covered by FERPA (Family Educational Rights and Privacy Act), employment records held by a covered entity in its role as employer, or records regarding a person who has been deceased for more than 50 years.

Public Health Authority: An agency or authority of the federal government, State, territory or political subdivision of a State or territory, or a person or entity acting under the grant of authority from such public agency, including the employees or agents of the public agency, that is responsible for public health matters as part of its official mandate.

Reasonable Cause: An act or admission in which a covered entity or business associate knew, or by exercising reasonable diligence would have known, the act or omission violated an administrative simplification provision (under HIPAA), but in which the covered entity or business associate did not act in willful neglect.

Required by Law: A mandate contained in law that compels a HIPAA covered entity to make use or disclosure of protected health information (PHI) and that it is enforceable by law

Risk Assessment: A process of assessing those factors that could affect confidentiality, availability, and integrity of key information assets and systems. HIPAA covered components are responsible for ensuring the integrity, confidentiality, and availability of PHI, electronic PHI and equipment that contains it, while minimizing the impact of security procedures and policies upon business productivity.

Security or Security Measures: All of the administrative, physical and technical safeguards in an information system.

Security Incident: The attempted or successful unauthorized access, use, disclosure, modification or destruction of protected health information, or interference with system operations in an information system containing protected health information.

Technical Safeguards: The technology and policy and procedures that protect and control access to electronic PHI.

Treatment: The provision, coordination, or management of health care and related services, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another.

Unsecured PHI: Protected health information(PHI) that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of technology or methodology such as encryption, or otherwise specified by the Secretary of DHHS in the guidance issued under section 13402 (h) (2) of Public Law 111-5.

Workstation: An electronic computing device, for example a laptop or desktop computer, or any other device that performs similar functions and any electronic media stored in its immediate environment.

POLICY:

ODCHC may collect, maintain, use, transmit, share and/or disclose confidential information about individuals to the extent needed to provide treatment and services.

Approved By:	Board of Directors	Adopted Date:	6/22/20
Distribution:	All Staff	Revision Date(s):	
Category:	Administration & Governance	Reviewed Date(s):	

The three types of individuals on whom ODCHC is most likely to obtain, collect, maintain or transmit information are ODCHC patients, providers, and employees.

ODCHC will safeguard protected health information about individuals, inform individuals about the ODCHC privacy practices, and respect individual privacy rights.

ODCHC shall provide Privacy and Security training to all staff, and shall require all staff to sign the ODCHC Security and Privacy Checklist outlining their role and responsibilities relating to protecting the privacy of ODCHC clients.

Safeguarding Confidential Information about Clients

ODCHC has adopted policies and procedures to reasonably safeguard all client protected health information.

ODCHC staff and business associates shall respect and protect the privacy of records and protected health information about clients who request or receive services from ODCHC. This includes but is not limited to:

- Applicants or enrollees in ODCHC health insurance plans
- Minors and adults receiving alcohol and drug, mental health, primary health services from ODCHC

ODCHC shall not use or disclose protected health information unless either:

- The client has authorized the use or disclosure in accordance with ODCHC Policy AG_Use and Disclosures of Protected Health Information
- The use or disclosure is specifically permitted under ODCHC Policy AG_Use and Disclosure of Protected Health Information

Safeguarding Confidential Information about Health Plan Enrollees

ODCHC has adopted policies and procedures to reasonably safeguard the protected health information of any Covered Person enrolled in one or more of the group health plans sponsored by ODCHC.

When ODCHC obtains protected health information about health plan enrollees, ODCHC may use and disclose such protected health information consistent with federal and state law.

Conflict with other Requirements regarding Privacy and Safeguarding

ODCHC has adopted reasonable policies and procedures for administration of its programs, services, and activities. If any State or federal law or regulation, or order of a court having appropriate jurisdiction, imposes a stricter requirement upon any ODCHC policy regarding the privacy or safeguarding of protected health information, ODCHC shall act in accordance with the stricter standard.

Approved By:	Board of Directors	Adopted Date:	6/22/20
Distribution:	All Staff	Revision Date(s):	
Category:	Administration & Governance	Reviewed Date(s):	

In the event that more than one policy applies but compliance with such policies cannot reasonably be achieved the ODCHC staff will seek guidance according to established ODCHC policy and procedure. ODCHC staff should first consult with their site leadership and then the ODCHC Compliance Officer.

Open Door Community Health Centers Notice of Privacy Practices

ODCHC will make available a copy of the ODCHC Notice of Privacy Practices to any client covered by HIPAA applying for or receiving covered services from ODCHC or enrolled in an ODCHC health plan.

The ODCHC Notice of Privacy Practices shall contain all information required under federal and state regulations regarding the Notice of Privacy Practices for protected health information under HIPAA.

Where ODCHC is a health care provider the Notice of Privacy Practices will be posted in the clinic, on the ODCHC website, and made available to clients in hardcopy as they desire.

ODCHC policies and procedures, as well as other federal and state laws and regulations, outline the HIPAA covered client's rights to access their own protected health information, with some exception. These policies also describe specific actions that a client can take to request restrictions or amendments to their protected health information and the method for filing complaints. These specific actions are outlined in the ODCHC Notice of Privacy Practices.

AG_Use and Disclosure of Protected Health Information

ODCHC shall not use or disclose any protected health information about a HIPAA covered client of ODCHC programs or services without a signed authorization for release of that protected health information from the individual, or the individual's personal representative, unless authorized by this policy, or as otherwise allowed or required by state, or federal law, as outlined in ODCHC policy AG_Use and Disclosure of Protected Health Information.

AG_MINIMUM NECESSARY STANDARD

ODCHC will use or disclose only the minimum amount of protected health information necessary to provide services and benefits to HIPAA covered clients, and only to the extent provided in ODCHC policy AG_Minimum Necessary Standard.

AG_ADMINISTRATIVE, TECHNICAL AND PHYSICAL SAFEGUARDS

ODCHC staff must take reasonable steps to safeguard protected health information from intentional or unintentional use or disclosure, as outlined in ODCHC Policies OPS.008 Security, IT 1.1.01.2.0, and ISP 1.0.0 through 1.20.0.

AG_DE-IDENTIFICATION OF PROTECTED HEALTH INFORMATION AND USE OF LIMITED DATA SETS

ODCHC staff will follow standards under which client protected health information can be used and disclosed if information that can identify a person has been removed (de-identified) or restricted to a limited data set. Unless otherwise restricted or prohibited by other federal or state law, ODCHC can use and share information as appropriate for the work of ODCHC, without further restriction, if ODCHC or

Approved By:	Board of Directors	Adopted Date:	6/22/20
Distribution:	All Staff	Revision Date(s):	
Category:	Administration & Governance	Reviewed Date(s):	

another entity has taken steps to de-identify the protected health information as outlined in the ODCHC policy AG_De-Identification of Protected Health Information and Use of Limited Data Sets.

AG_BUSINESS ASSOCIATES

ODCHC may disclose protected health information to business associates with whom there is a written contract or memorandum of understanding as outlined in the ODCHC Policy AG_Business Associates. Business Associates and their subcontractors have responsibilities under HIPAA to protect and safeguard client's confidential information.

Enforcement, Sanctions and Penalties for Violations of Individual Privacy

All ODCHC staff, contract staff, volunteers, and interns must guard against improper uses or disclosures of ODCHC client information. ODCHC shall apply appropriate sanctions against members of its staff as outlined in ODCHC Policies HR.110 Ethics and Compliance, sections 110.1 Patient Relationships and 110.2 Patient Information, as well as, HR.380 Disciplinary Actions.

References;

United States 45 CFR Parts 160 and 164
California Health Information, Privacy Manual, California Hospital Association, 2017
County of Sacramento HIPAA Privacy Rule Policies and Procedures, September 23, 2013

Associated Documents:

ODCHC Form #568 Notice of Privacy Practices
OPS.008 Security
OPS.041 Equipment & System Access Controls
OPS.061 Clinical Records Storage Handling
ITEP 1.1.0 Mobile Device and Remote Access Appropriate Use
ITEP 1.2.0 Computer, Email and Internet Usage
ISP 0.0.0 Information Security Policy Summary and Descriptions
HR.110 Ethics and Compliance
HR.380 Disciplinary Actions
AG_Electronic Communication of Protected Health Information
AG_Use and Disclosure of Protected Health Information
AG_De-Identification of PHI and Use of Limited Data Sets
AG_Administrative, Technical, and Physical Safeguards
AG_Business Associates
AG_Minimum Necessary Standard

Keyword Tags:

Privacy, security, HIPAA, confidential, protected, health, information