AG.604 ADMINISTRATIVE, TECHNICAL AND PHYSICAL SAFEGUARDS

Approved By:	Board of Directors	Adopted Date:	6/22/20
Distribution:	All Staff	Revision Date(s):	
Category:	Administration and 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 Health Insurance Portability and Accountability Act (HIPAA), provisions of HIPAA concerning the privacy and confidentiality of a person's confidential health information "give way" to California state law provisions and other federal provisions that are more stringent than HIPAA.

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

PURPOSE:
To outline reasonable and appropriate safeguards to reduce the risk of unauthorized access, use, and disclosure of protected health information as required under HIPAA Section 164.312.

DEFINITIONS:
See HIPAA Compliance Overview policy for all definitions.

POLICY:
ODCHC and its business associates, as covered entities, shall protect all patient and staff protected health information. This includes accidental or deliberate access, use, or disclosure through the use of administrative, technical, or physical safeguards.

- **Administrative Safeguards:**
  - **Policies and Procedures:**
    ODCHC has written policies and procedures in Human Resources, Information Technology, Operations, and Administration to prevent accidental or deliberate violations of the HIPAA regulations.
  - **Risk Analysis:**
    ODCHC shall conduct a risk analysis every two years to evaluate the safeguards. The analysis will be conducted by an outside agency. When completed, the deficiencies will be addressed internally.
  - **Training:**
    ODCHC conducts regular training on HIPAA rules and regulations to newly hired staff and existing staff. The training includes security requirements as well as use and disclosure practices for electronic, oral, and hardcopy protected health information (PHI).
  - **Business Associates:**
    Business associate agreements may be required, depending on the level of risk ODCHC perceives with the vendor. A business associate may create, receive, maintain, or transmit electronic protected health information (ePHI) on behalf of ODCHC only if satisfactory assurances are made that they will appropriately safeguard the information.

- **Sanctions:**
  ODCHC's policies and procedures outline disciplinary actions, up to and including termination, for violations regarding protected health information.
  Note: Exceptions to Disciplinary Actions:

- **Whistleblower:**
  When a staff member or business associate acting as a whistleblower (someone who notifies authorities of the unlawful or unethical actions of ODCHC) releases PHI. This disclosure could be sent to a health oversight agency, a public health authority to investigate the conduct of ODCHC, or a health care accreditation agency to report alleged failure to meet professional standards or misconduct. An attorney will be acquired by or on behalf of the staff member to determine legal options.
- **Staff Member is a Victim of a Crime:**
  When a staff member discloses protected health information is the victim of a crime, a disclosure is made about the suspected perpetrator of the criminal act, and only certain limited protected health information is disclosed.
- **Privacy Complaint:**
  When the staff member exercises any right under the Privacy Rule, including filing a complaint.

- **Workforce Security:**
  ODCHC has implemented role-based and need to know access for protected health information to promote administrative safeguards.
  - **Authorized Access:**
    Only staff members or business associates will be authorized to have access to specified PHI, in accordance with the requirements set forth in the ODCHC Policy ISP Information Access Management. ODCHC staff are assigned a unique name and/or number for identifying and tracking user identity.
    - Users are obligated to use their assigned unique user ID and authenticator to access the information system. Usage of another user's identifier and/or authentication data to access an information system is strictly prohibited.
    - Users are obligated to change their authenticator (excepting biometric authenticators) on a regular basis. ODCHC's IT Department will determine the frequency for authenticator changes based on risks associated with the information system.
    - Users are obligated to change their authenticator whenever there is a reason to suspect the authenticator may have become known to another person or otherwise compromised.
    - Upon staff member termination or modification of job duties, ODCHC HR will notify Corporate Services to disable physical access and IT to disable electronic information system access.
- **Disaster Plan:**
  ODCHC has developed and implemented an Emergency Operations Plan that addresses the most likely risks faced by ODCHC. The plan has also developed contingency plans if the emergency occurs.

- **Physical Safeguards:**

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

- **Policies and Procedures:**
  ODCHC has written policies and procedures in Human Resources, Information Technology, Operations, and Administration to promote physical safeguards to protect staff, patients, and PHI.
- **Workplace Security:**
  Workplace security ensures that persons who are not authorized to access PHI, but who work in or visit locations where PHI might be accessible, will be supervised or otherwise procedurally denied access. Staff members will safeguard PHI when persons who are not authorized access to the information are present, in accordance with the ODCHC Policy OPS.008 Security.

- **Technical Safeguards:**
  - **Policies and Procedures:**
    ODCHC has written policies and procedures in IT, Operations, and Administration to promote technical safeguards to limit access to authorized individuals only.
  - **Automatic Log off Process:**
    ODCHC has developed an automatic log off process that terminates an electronic session after a predetermined time of inactivity.
  - **Monitoring and Tracking:**
    ODCHC has the capability to monitor and track access to electronic protected health information.

REFERENCES:

California Hospital Association, California Health Information Privacy Manual, 2017
HIPAA rules and regulations, 45 CFR 164
County of Sacramento, HIPAA Privacy Rules Policies and Procedures, September 23, 2013
Stanford University, HIPAA Security: Information Access Controls Policy, 12-07-2015

ASSOCIATED DOCUMENTS:

OPS.008 Security
ITEP 1.1.0 Mobile Devise and Remote Access Appropriate Use Policy
ITEP 1.2.0 Computer, Internet, and Email Usage
ISP 1.0.0 Information Security Policy HIPAA Introduction
ISP 1.1.0 Security Management Process
ISP 1.2.0 Information Security and Privacy Violation
ISP 1.3.0 Workforce Security Policy
ISP 1.4.0 Information Access Management
ISP 1.5.0 Access Authorization, Establishment and Modification
AG_Business Associates

KEYWORD TAGS:

Protection, safeguards, security, HIPAA