SANTA BARBARA COUNTY
DEPARTMENT OF
Behavioral Wellness
A System of Care and Recovery

Departmental Policy and Procedure

Section	Information Technology (IT)	**Effective:**	1/26/2017
Sub-section		**Version:**	1.1
Policy	Information Systems For Workforce Access And Termination Requirements	**Last Revised:**	9/12/2018
Policy #	14.000		

Director's Approval _____ **Date** 10/23/18
Alice Gleghorn, PhD

Division Chief's Approval _____ **Date** 10/24/18
Marshall Ramsey

Supersedes: IT-14.000 Information Systems for Workforce Access and Termination Requirements rev. 1/26/2017

Audit Date: 9/12/2021

1. PURPOSE/SCOPE

1.1. To ensure all Department of Behavioral Wellness (hereafter "the Department") workforce members are granted appropriate access and managed in a manner commensurate with the role of each workforce member, and to prevent those who should not have access from obtaining access to sensitive data, restricted data and electronic information systems.

1.2. The Department has adopted an Access and Termination process to comply with the Health Information Portability and Accountability Act (HIPAA) and to establish security and privacy standards to protect the confidentiality and integrity of Protected Heath Information (PHI), Personal Information (PI), and Personally Identifiable Information (PII) as required by law, professional ethics, and accreditation requirements.

2. DEFINITIONS

The following terms are limited to the purposes of this policy:

2.1. **Restricted Data** – data in any format collected, developed, maintained or managed by or on behalf of the Department, or within the scope of the Department's activities that, if confidentiality, integrity, or availability is compromised, would have severe or catastrophic loss to the Department, with potential for significant legal implications, breach reporting obligations to State and/or Health & Human Services (HHS), and possible penalties and fines. This includes Protected Health Information (PHI), Personal Information (PI), and Personally Identifiable Information (PII) as well as the authentication credentials used to access the Department or County systems or networks that provide access to PHI, PI, and PII (for example, information systems user passwords are restricted data).

2.2. **Sensitive Data** – data whose loss of confidentiality, integrity, availability or unauthorized disclosure would disrupt normal Department functions, with potential for substantial legal implications, breach reporting obligations to State and/or Health & Human Services (HHS), and possible penalties and fines. This sensitive data is intended for use by Department workforce members with a legitimate business need (some examples of sensitive data include but are not limited to disaster recovery plans, operational recovery plans, physical facility schematics, risk assessments, and system controls).

2.3. **Workforce** – includes employees, volunteers, trainees, and other persons who provide services or perform their duties under the direct control of the Department, County contracted providers of mental health and/or substance abuse services, or a business associate of the Department, whether or not they are paid by the Department.

2.4. **Protected Health Information (PHI)** – refers to any Protected Health Information (PHI) that is covered under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security regulations, including PHI produced, saved, transferred or received in an electronic form. For example, the combination of past, current or future information related to health, provision of care or payment, ***together with*** any identifying information that is reasonably likely to identify the client constitutes PHI as defined by the HIPAA Privacy Rule.

2.5. **Personal Information (PI)** – any information that is maintained by an agency, including Personal Information (PI) produced, saved, transferred or received in an electronic format, that identifies or describes an individual, including, but not limited to, his or her name, social security number, physical description, home address, home telephone number, education, financial matters, and medical or employment history. It includes statements made by, or attributed to, the individual. [California Civil Code §1798.3(a)]

2.6. **Personally Identifiable Information (PII)** – any information, including Personally Identifiable Information (PII) produced, saved, transferred or received in an electronic format, which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc., alone or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.

3. POLICY

3.1. Role and Responsibilities Related to Information Access Management: In addition to any specific responsibilities noted below, the following groups and/or individuals within the Department are responsible for the management of access to the Department's sensitive data, restricted data and electronic information systems:

Authorization	**Modification**	**Termination**
Quality Care Management (QCM)	Quality Care Management (QCM)	Quality Care Management (QCM)
Supervisor / Manager	Supervisor / Manager	Supervisor / Manager
Human Resources (HR)	Human Resources (HR)	Human Resources (HR)
Information Technology (IT)	Information Technology (IT)	Information Technology (IT)
Health Information Mgmt. (HIM)		Chief of Compliance
Chief of Compliance		Privacy Officer
Privacy Officer		

4. PROCEDURE

All procedures for granting, maintaining, and terminating access to Department sensitive data and restricted data will be consistent with related County and Department policies and procedures as specified below.

4.1. **Authorizing and Maintaining Access**: The Department will implement procedures to establish, document, periodically review and modify if appropriate each workforce member's right to access systems and networks that contain Department electronic sensitive data and restricted data, according to the member's role, and the classification of the Department sensitive data and restricted data.

4.2. **Information Technology (IT) will manage all users with authorized access to include:**

1. Establishing the workforce member's user account and permissions according to the requested authorization for access.
2. Alerting supervisors of any suspicious access to system.
3. Providing notification of anomalous user behavior to each supervisor or manager as well as the Department's Privacy and Security Officers.
4. Provide a process to enable supervisors to review the following information on a quarterly basis:
   a. Network Active Directory user account listing;
   b. Clinicians Gateway user account listing;

c. Sharecare user account listing; and

d. Permissions for which that supervisor is responsible.

4.3. **Each supervisor or manager is responsible for:**

1. Completing a New Staff Integration Checklist, Network Account Request, and Service Provider ID Application form (See Attachments A/B, C and D) upon the hire of new workforce members.
2. Authorizing access to Department systems and networks containing sensitive data and restricted data for his or her subordinates. Workforce members are not permitted to authorize their own access to sensitive data and restricted data; access must be granted by a person in their chain of command.
3. Ensuring that the access to sensitive data and restricted data granted to each of his or her subordinate workforce members is the minimum necessary access required for the subordinate's job role and responsibilities.
4. Periodically reviewing the level of access to sensitive data and restricted data granted to each of his or her workforce member subordinates and for modifying such access if appropriate with a completed Service Provider Information Update form (see Attachment E).

4.4. **Responsibilities of Community Based Organizations (CBOs) and Business Associates:** All County CBOs and Business Associates (BA) performing duties under the direct control of the Department must implement procedures to establish, document, periodically review and modify workforce member access if appropriate. CBOs and BAs must comply with the following requirements:

1. Upon the hire of new workforce members the supervisor or manager will complete a Service Provider ID Application form (see Attachment D).
2. Authorize access to Department systems and networks containing sensitive data and restricted data for his or her workforce member subordinates. Workforce members are not permitted to authorize their own access to sensitive data and restricted data or be granted authorization from another CBO or BA supervisor.
3. Ensure that the access to sensitive and sensitive data and restricted data granted to workforce member subordinates is the minimum necessary access required for each such subordinate's job role and responsibilities.
4. Periodically reviewing the access to sensitive data and restricted data granted to each workforce member subordinate, and modifying such access if appropriate with a completed Service Provider Information Update form (see Attachment E).
5. CBO user accounts will be authorized in 90 day increments from date of hire and will be disabled at the expiration of this period unless the CBO provides notification to the Department that user accounts should remain active. Upon notification from the CBO that the user account should remain active, IT will extend account access for an additional 90 days.

4.5. **Modification of Access Upon Change of Job/Role Status Within The Department:** Upon a change of position, the workforce member's new supervisor or manager is responsible for requesting access to Department sensitive data and restricted data commensurate with the workforce member's new role and responsibilities. If appropriate, the supervisor or manager will complete a Service Provider Information Update form (see Attachment E). IT shall terminate or suspend the workforce member's current access to Department systems, networks, and/or sensitive data and restricted data dependent on his or her current role as of the date of transfer, and upon approval of the Service Provider Information Update form, will change the workforce member's status to allow the access requested.

4.6. **Terminating Access**: When a workforce member's employment terminates or their contract ends, access to Department sensitive data and restricted data is not extended to the workforce member beyond the date of such separation or termination unless the workforce member's access is re-authorized.

1. Supervisors, managers, CBOs, and BAs shall notify IT 30 days prior to when a workforce member is scheduled to separate from employment, or immediately when a workforce member has been terminated from employment. An exit checklist shall be initiated by the supervisor, manager, CBO or BA (see Attachments G and H).
2. IT will be responsible for ensuring that the workforce member's accounts to access Department sensitive data and restricted data are suspended or terminated. For voluntary termination, this shall be the last day of employment or contract. For involuntary termination, this will be within one hour of notification to IT of the event.
3. Upon separation or termination, the workforce member's access to all facilities housing Department sensitive data and restricted data shall cease, including but not limited to card access, keys, codes, and other facility access control mechanisms. Codes or passwords for systems, equipment access passwords (routers and switches), administrator passwords, and other common access control information shall be changed when appropriate.
4. Access to Department sensitive data and restricted data is not extended to a workforce member beyond the separation date of such workforce member's employment unless IT is notified of one of the following conditions:
    a. The workforce member's separation status has been extended to a future date; or
    b. The workforce member is authorized for temporary access from appropriate management staff.

ASSISTANCE

Celeste Andersen, Chief of Compliance

HIPAA Privacy Officer

HIPAA Subcommittee

REFERENCE

Code of Federal Regulations – Public Welfare
Title 45, Section 164.308(a)(4)

California Civil Code
Section §1798.3(a)

RELATED COUNTY OF SANTA BARBARA POLICIES

User Access Policy

Acceptable Use Policy

Information Classification Policy

Information Protection Policy

Remote Access Policy

ATTACHMENTS

Att. A – Integration Checklist for licensed Doctors and Physician Assistants

Att. B – Fiscal New Hire Checklist

Att. C – Network Account Request Form

Att. D – Service Provider ID Number Request Instructions

Att. E – Service Provider Information Update Form

Att. F – Service Now – Help Desk Ticket Order Request form

Att. G – Staff Separation Checklist

Att. H – Contract Providers Separation from Service form

REVISION RECORD

DATE	VERSION	REVISION DESCRIPTION
9/12/2018	1.1	• Outlined the different types of protected information: PHI, PI, and PII • Updated Service Now Help Desk Ticket Order Request form

Culturally and Linguistically Competent Policies

The Department of Behavioral Wellness is committed to the tenets of cultural competency and understands that culturally and linguistically appropriate services are respectful of and responsive to the health beliefs, practices and needs of diverse individuals. All policies and procedures are intended to reflect the integration of diversity and cultural literacy throughout the Department. To the fullest extent possible, information, services and treatments will be provided (in verbal and/or written form) in the individual's preferred language or mode of communication (i.e. assistive devices for blind/deaf).