

	County of Sacramento Behavioral Health Services	Policy No.	00-03
		Issued Date	05-24-10
		Revision Date	07-01-10
AREA: Administration	TITLE: AVATAR Account Management and Password Protection		
Approved by: 			
Uma K. Zykofsky, LCSW Program Manager, Quality Management/Compliance Division of Behavioral Health Services	Mary Ann Bennett Deputy Director, Department of Behavioral Health Services		

Introduction:

AVATAR is a web-based practice management system used by Sacramento County, Department of Behavioral Health Services (DBHS). This mission critical application contains Personal Health Information (PHI) and as such, strict policies regarding the account usage and monitoring of accounts must be in place to prevent unauthorized access to the system. This policy outlines the processes for requesting, managing and deactivating accounts. This policy establishes how monitoring and tracking will take place within the Division of Behavioral Health Services and applies to all AVATAR users in Mental Health and Alcohol and Drug Services.

I. Policy

It is the policy of Sacramento County to create individual named user accounts, activate, manage, and monitor the usage of the accounts and inactivate accounts when access is no longer required. This document describes the criteria and process for account creation, account monitoring procedures, and the procedures for deactivation and re-instatement of user accounts. As AVATAR is a web-based application containing Protected Health Information (PHI), it is policy to closely monitor and maintain user accounts to prevent unauthorized access. AVATAR user reports will be utilized to monitor appropriate access and use of this web-based system.

II. Purpose

The purpose of this policy is to communicate the process that will be followed to request a new AVATAR account, modify an existing account, deactivate an account and re-instate a previously deactivated account.

III. Definitions

Avatar Liaison: Individuals designated at each provider or county operated program with responsibility to disseminate and manage information and information requests relating to the Avatar implementation.

Access Control: The act of limiting a user's access to certain data based on role or job function.

Account Creation: This is the process of creating an account on a computer system and granting it permission to access or use some subset of files or data. AVATAR accounts are comprised of the following components.

- **User ID:** This is a unique identifier assigned to the account. This typically contains the last name, first initial and a numeric value.
- **Password:** A secret combination of characters that are either assigned to you or you can choose that give you access to the computer or the network
- **System Code:** A logical partition in the AVATAR database that restricts access to the Legal Entity responsible for the information.

Breach: Loss of control, compromised, unauthorized disclosure or unauthorized access or potential access of PHI. This is a violation of the HIPAA Privacy Rule and/or Security Rule and “compromises the security or privacy of the individual that may pose a risk of financial, reputational, or other harm” to affected individuals.

Data "Browsing": The act of viewing data or records not directly within the scope of one's job functions at the time. For example, a health care provider looking at records of patients not under that provider's care.

HIPAA (Health Insurance Portability and Accountability Act): A set of standards for the privacy and security of electronic protected health information required of health plans, health care clearinghouses, and certain health care providers.

PHI (Protected Health Information): Individually identifiable health information that is transmitted or maintained in any form or medium. Individually identifiable health information is health information created or received by a health care provider or health plan that identifies an individual and relates to the physical or mental health or condition of an individual or relates to the provision of health care to an individual or relates to the payment for health care. Protected health information includes individually identifiable health information (with limited exceptions) in any form, including information transmitted orally, or in written or electronic form, and includes any information (such as a name, address, photo, etc.) that identifies real people in a health care setting.

III. Procedures

A. New Account Creation

1. Every individual requesting an AVATAR account will have completed an Information Technology (IT) Security Policy agreement in accordance with their organizational structure. Sacramento County staff complete an agreement as part of hiring orientation and sign an “Acknowledgement of Information Security Responsibility.” Sacramento County employees Acknowledgement is maintained in Human Resources records. Contractors are required to maintain equivalent documentation. Such information may be sampled and checked as part of the regularly scheduled triennial MediCal site certification or recertification activities. Contract monitors will also check contractor records for compliance during regularly scheduled contract monitoring site visits. If a provider is utilizing the AVATAR system and is not part of the MediCal/Drug Medi-cal System, the Division Compliance Officer or designee may request confirmation of these policies as deemed necessary.

Account management policies apply to all AVATAR users, irrespective of type of funding or contract.

Any requests for exceptions due to unique user or program responsibilities must be reviewed and approved by Division Compliance Officer. Record of decision and type of access will be maintained in AVATAR account management folder.

2. Unique named accounts are created upon the completion of the account request procedure outlined below. AVATAR user accounts are made of three components:
 - User ID
 - Password
 - System Code
3. Individuals are eligible for an AVATAR user account if all of the following conditions are met:
 - Current employee, contractor, or Named Guest (e.g. Auditor) of Sacramento County, Department of Behavioral Health Services or one of its contracted providers
 - Access to AVATAR is required in order to complete necessary job functions
 - Completed Account Request/Change Form, including supervisor's signature
 - Completion of training provided by Sacramento County, DBHS
 - An available AVATAR license exists for distribution.

If after the creation and use of an AVATAR account and any of the preceding conditions change, the Account Inactivation process outlined below must be immediately followed. The individual is no longer eligible for an AVATAR user account. Examples of this include separation from employment, and or a change in job function that no longer requires access to AVATAR. Access may be limited or denied based on monitoring, investigation, follow-up and action. In order to receive an AVATAR user account the following events must occur:

1. Completion of an AVATAR Account Request/Change Form. **No action without supervisor's signature.**
2. Submit the completed form by email to the AVATAR information inbox (avatar@sacounty.net). If submission is by fax, fax may be sent to (916) 876-6633, Attention: AVATAR Account Request
3. Scheduling and Completion of Avatar Training
4. AVATAR Account Request/Change Forms, once completed, will be scanned and maintained for a minimum of one year. This information will be available for review and audit or compliance investigations or routing reviews by the Division Compliance Officer or designee.

B. Account Deactivation

If any of the following conditions are met, an AVATAR account must be inactivated:

- Separation of an employee, contractor or named guest of Sacramento County, DBHS or its contracted Providers.
- Extended Leave of Absences
- Access to AVATAR is not required to complete job functions

- Any restrictions or deactivation due to breaches, monitoring, compliance, investigation

In order to deactivate an AVATAR account a submission of a completed Account Request/Change Form is required. This must indicate the last date that AVATAR use is required. Access to AVATAR will be terminated effective this date.

C. Account Reinstatement

There are situations where a deactivated AVATAR account needs to be reinstated for use. One example of this situation is when an employee returns from an extended leave of absence. To re-instate an AVATAR less than 60 days ago from the inactivation date, a signed Account Request/Change form must be submitted. If the inactivation date of the account is more that 60 days from the requested re-instatement date, then training is required prior to re-instating the account.

D. Account Monitoring

It is the policy of Sacramento County, DBHS to require periodic verification of current accounts. This requires an explicit acknowledgement that the account exists is accurately assigned and is still needed and appropriately utilized. Sacramento County, DBHS will provide cyclical reports identifying accounts that have not been used within the preceding 60 days. AVATAR Liaisons will be responsible to provide confirmation of account users based on these reports within **ten business days** of receipt of reports. Accounts can be inactivated after 90 days of inactivity. AVATAR reports will be utilized to audit user activity. Any breaks in security will be reported in accordance with County HIPAA Privacy and Security policies. (See attached.)

E. Password Protection

It is the policy of Sacramento County to abide by the following standards with regard to Password protection.

Password Requirements

- Passwords must adhere to the following standards
 - Must be between 6 and 10 characters in length
 - Must contain mixed case characters
 - Must contain at least one number
- Passwords must be reset at least every 180 days
- Passwords can not be re-used for a minimum of 180 days
- Passwords should be memorized; if this is not possible passwords shall be stored in a format that prevents unauthorized use (e.g. locked encrypted file).

Events Necessitating Password Change

If any of the following events occur, a password change is mandatory:

- **Temporary password issued after initial training; user must create new password for ongoing access to the AVATAR system**
- Unauthorized password discovery or usage by another person
- System compromise (unauthorized access to a system or account).
- Insecure transmission of a password, for example via email or instant message.
- Accidental disclosure of password
- Password is provided to IT support staff in order to resolve a technical issue (It is strongly recommended that IT support staff request an end-user password as a last resort.)

Resetting of a password will be accompanied by an email communication to the AVATAR Liaison to ensure program level awareness and monitoring of password changes.

Password Transmission

Passwords must not be transferred or shared with others unless authorized to do so. The following standards apply for transmission of passwords.

- **Electronic:** Passwords must not be transferred electronically over the Internet using insecure methods. Insecure methods include Post Office Protocol (POP), Internet Mail Access Protocol (IMAP), File Transfer protocol (FTP), Hyper-Text Transfer Protocol (HTTP), and Telnet.
- **Written:** When it is necessary to disseminate passwords in writing, the recipient will take measures to protect the written password from unauthorized access. For example, after memorizing the password, one must destroy the written record.
- **Oral:** When transmitting a password orally, take measures to ensure that the conversation is not overheard by unauthorized individuals.

F. Access Control

Access to data contained within the AVATAR Application is controlled by the creation and maintenance of System Codes within the AVATAR application. There is a minimum of one system code per Legal Entity. Sacramento County, DBHS periodically audits the data accessed within the AVATAR application. All access must be on a “need to know basis” in accordance with HIPAA privacy and security rules. Data browsing is strictly prohibited. Audit logs will be maintained for a minimum of one year and available for routine and special audits or investigations as required or determined by the Division Compliance Officer or designee. AVATAR reports may also be utilized as needed to validate appropriate use of the system.

IV. REFERENCES	Related Policies & Procedures	State/Federal Codes/Other References
	AVATAR Account Request Change Form County of Sacramento IT Security Policy http://inside.itpb.saccounty.net/CountyITPoliciesandStandards/default.htm HIPAA Privacy Rule P&P HIPAA Security Rule P&P http://inside.compliance.saccounty.net/default.htm HIPAA Incident Tracking Tool http://inside.compliance.saccounty.net/Intra_HIPAA_DF_IncidentReport	MHP Contract with DMH MHP Contract with Providers Alcohol & Drug Contracted Services
V. CONTACTS	Name	E-mail
		Avatar@saccounty.net QMInformation@saccounty.net
VI. SCOPE	<input checked="" type="checkbox"/> Mental Health and Alcohol & Drug Services Staff <input checked="" type="checkbox"/> Mental Health Treatment Center <input checked="" type="checkbox"/> Specific grant/specialty resource	<input checked="" type="checkbox"/> Alcohol & Drug Services Providers <input checked="" type="checkbox"/> Adult Contract Providers <input checked="" type="checkbox"/> Children’s Contract Providers