County of Sacramento **Department of Health Services** **Division of Behavioral Health Services** **Policy and Procedure**	Policy Issuer (Unit/Program)	**QM**
	Policy Number	**QM-00-03**
	Effective Date	**05/24/2010**
	Revision Date	**01/01/2024**

Title: **Electronic Health Record (EHR) Account Management and Password Protection**	Functional Area: **Administration**

Approved By: (Signature on File) **Signed version available upon request**

Alexandra Rechs, LMFT
Program Manager, Division of Behavioral Health Services

Ryan Quist, PHD
Deputy Director, Division of Behavioral Health Services

BACKGROUND/CONTEXT:

SmartCare is a web-based Electronic Health Record (EHR)system used by Sacramento County, Division of Behavioral Health Services (BHS). 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 EHR users in Specialty Mental Health and Substance Use Prevention and Treatment (SUPT). Each provider must ensure that all staff are trained and adhere to all State and Federal laws and regulations separate and independent of EHR User training. All providers training must include Health Insurance Portability and Accountability Act (HIPAA) training on privacy and security as well as 42 Code of Federal Regulations, Part 2, as specific areas of attention to the business of healthcare that is delivered in these contracted and county operated programs. Such training is provided prior to requesting an EHR Account for any individual. EHR Account Training/Registration Forms (see attached), 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.

DEFINITIONS:

- **EHR Liaison:** Individuals designated at each provider or county operated program with responsibility to disseminate and manage information and information requests relating to the EHR implementation.
- **EHR Control:** The act of limiting a user's access to certain data based on role or job function.
- **EHR 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. EHR 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
    - **CDAG (Clinical Data Access Group):** To abide by HIPAA and Title 42 CFR, SmartCare uses Clinical Data Access Groups, or CDAG to limit what users can see in the SmartCare system. A user CDAG will be determined by the program where they work and are set by the system administrator.

- **Authorized Approver:** Individuals who have the authority to request a user account creation or deactivation for their agency staff.
- **Breach:** The acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E (Privacy of Individually Identifiable Health Information) which compromises the security or privacy of the protected health information. This is a violation of the HIPAA Privacy Rule and/or Security Rule and or 42 CFR, part 2.
- **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 all protected health information required of health plans, health care clearinghouses, and health care providers.
- **42 CFR, Part 2:** Under the statutory provisions quoted in §§2.1 and 2.2, these regulations impose restrictions upon the disclosure and use of alcohol and drug abuse patient records which are maintained in connection with the performance of any federally assisted alcohol and drug abuse program.
- **PHI (Protected Health Information):** PHI is individually identifiable health information that a health care plan, health care provider, health care clearinghouse, or business associate creates, maintains, receives or transmits that identifies an individual, or could be used to identify an individual, and relates to:
  - The individual’s past, present, or future physical or mental health condition;
  - The provision of health care to the individual; or
  - The past, present, or future payment for the provision of health care to the individual.

  PHI can be written, spoken or electronic.

PURPOSE:

The purpose of this policy is to communicate the process that will be followed to request a new EHR account, modify an existing account, deactivate an account, and re-instate a previously deactivated account. This Policy update replaces QM-00-03 AVATAR Account Management and Password Protection.

DETAILS:

1. New Account Creation

Every individual requesting an EHR 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 site certification, recertification activities. Contract monitors will also check contractor records for compliance during regularly scheduled contract monitoring site visits.

Account management policies apply to all EHR 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 the County Behavioral Health Services Compliance Officer. Record of decision and type of access will be maintained in EHR account management folder.

Unique named accounts are created upon the completion of the account request procedure outlined below. EHR user accounts are made of two components:

A. User ID

B. Password

Individuals are eligible for an EHR user account if all of the following conditions are met:

A. Current employee, contractor, or Named Guest (e.g. Auditor) of Sacramento County, Division of Behavioral Health Services, Specialty Mental Health and Substance Use Prevention and Treatment or one of its contracted providers.

B. Access to the EHR is required to complete necessary job functions.

C. Completed Account Request/Change Form, including supervisor's signature, sent by the agency Authorized Approver.

D. Completion of the EHR training provided by Sacramento County, BHS.

E. An available EHR license exists for distribution.

2. Modification of Account Access

If after the creation and use of an EHR account, an individual's duties change that impact the need to access EHR, the EHR account must be updated to ensure that access is in alignment with the updated duties. Access to the EHR system is role based and user roles are assigned based on job function.

Examples of this include a change in job function that no longer requires access to clinical information in EHR. Access may be limited or denied based on monitoring, investigation, follow-up, and action.

In order to modify an EHR user account, the following events must occur:

A. Completion of an EHR Account Request/Change Form. **No action without Authorized Approver Signature.**

B. Submit the completed form to the BHS-EHR information inbox (bhs-ehrtrainingregistration@saccounty.net). If submission is by fax, fax may be sent to (916) 876-6633, Attention: EHR Account Request.

C. Scheduling and Completion of EHR Training.

3. Account Deactivation

If any of the following conditions are met, an EHR account must be deactivated:

A. Separation of an employee, contractor or named guest of Sacramento County, SMHS, SUPT, or its contracted Providers.

B. Extended Leave of Absences.

C. Access to EHR is not required to complete job functions.

D. Any restrictions or deactivation due to breaches, monitoring, compliance, investigation.

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

4. **Account Reinstatement**
There are situations where a deactivated EHR 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 EHR less than 60 days from the inactivation date, a signed Account Request/Change form must be submitted by the Authorized Approver. If the inactivation date of the account is more than 60 days from the requested re-instatement date, then training is required prior to reinstating the account.

5. **Account Monitoring**
It is the policy of Sacramento County BHS to require 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, BHS has made available reports identifying individuals with access to Provider data. EHR Liaisons are responsible for verifying access monthly. Accounts are deactivated after 90 days of inactivity. EHR reports will be utilized to audit user activity. Any breaks in security will be reported in accordance with County 42 CFR, part 2 and HIPAA Privacy and Security policies. (See attached.)

6. **Password Protection**
It is the policy of Sacramento County to abide by the following standards regarding Password protection:

A. **Strong Password Requirements**
   a. Passwords must adhere to the following standards
   b. Must be between 8 and 10 characters in length
   c. Must contain mixed case characters
   d. Must contain at least one number
   e. Passwords must be reset at least every 180 days
   f. Passwords cannot be re-used for a minimum of 365 days
   g. Passwords should not contain dictionary words or names

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).

B. **Events Necessitating Password Change**
If any of the following events occur, a password change is mandatory:
   a. **Temporary password issued after initial training; user must create new password for ongoing access to the EHR system.**
   b. Unauthorized password discovery or usage by another person.
   c. System compromise (unauthorized access to a system or account).
   d. Insecure transmission of a password, for example via email or instant message.
   e. Accidental disclosure of password.
   f. 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 EHR Liaison to ensure program level awareness and monitoring of password changes.

C. **Account Verification**
Access to the system can only be granted by identified Account Approvers. BHS Quality Management maintains a list of Authorized Account Approvers for each Provider. Requests for account creation or modification will be returned to the submitting entity if the Authorized Approver has not signed the Account Request Form.

D. **Password Transmission**

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

a. **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.

b. **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.

c. **Oral:** When transmitting a password orally, take measures to ensure that the conversation is not overheard by unauthorized individuals.

E. **Access Control**
Access to data contained within the EHR Application is controlled by the creation and maintenance of CDAG within the EHR application. There is a minimum of one CDAG per user. Sacramento County, BHS periodically audits the data accessed within the EHR application. All access must be on a "need to know basis" in accordance with HIPAA privacy and security rules and 42 CFR part 2. Data browsing is strictly prohibited.

REFERENCE(S)/ATTACHMENTS:

- HIPAA Incident Reporting - http://inside.compliance.saccounty.net/Pages/IncidentReporting.aspx
- 42 CFR, Part 2 - https://www.law.cornell.edu/cfr/text/42/part-2

RELATED POLICIES:

- County of Sacramento HIPAA Privacy Rule Policies and Procedures - http://inside.compliance.saccounty.net/Documents/2018%20HIPAA%20Privacy%20Rule%20P&Ps.pdf
- County of Sacramento Security Rule Policies and Procedures - http://inside.compliance.saccounty.net/Documents/HIPAA%20Security%20Rule%20PPs%202016.pdf

DISTRIBUTION:

Enter X	DL Name	Enter X	DL Name
X	BHS Staff Adult & Child	X	SUPT Contracted Youth Providers
X	Mental Health Treatment Center	X	SUPT Contracted Adult Providers
X	BHS Adult Contract Providers	X	BHS EHR Team
X	BHS Children's Contract Providers		Specific grant/specialty resource
X	Substance Use and Prevention Treatment		
X	Quality Management, Cultural Competence, Research and Evaluation		

CONTACT INFORMATION:

- Quality Management
  QMInformation@SacCounty.net