SAN MATEO COUNTY HEALTH SYSTEM
BEHAVIORAL HEALTH AND RECOVERY SERVICES

DATE: January 23, 2017

BHRS POLICY: 17-01

SUBJECT: Security of Information (PI/PII/PHI) and Electronic Health Record (EHR), and Electronic Signatures & Terminations

AUTHORITY: Department of Health Care Services (DHCS) contract; DMH Letter No: 08-10 (December 4, 2008); CA Dept of Alcohol and Drug Programs (ADP) Bulletin No. 10-01; California Government Code Section 16.5 (d); California Government Code Section 16.5 (a), California Code of Regulations (CCR) Section 22002; Office of Management and Budget (OMB) Circular No. A-130, 45 CFR Section 164; The Health Information Technology for Economic and Clinical Health Act (HITECH); The Health Insurance Portability and Accountability Act (HIPAA); Organized Delivery System (ODS) Waiver Contract with DHCS Exhibit G; BHRS Policy 03-01: Confidentiality/Privacy of PHI; BHRS Policy 93-11: Critical Incident Reporting for Mental Health and AOD Providers.

AMENDED: August 15, 2017

ATTACHMENTS:
A: DHCS; DMH Letter No: 08-10
B: eCC Electronic Signature Agreement Form
C. Look Up Only Avatar Access Form
D. Mental Health Contractors Avatar User Request Form
E. AOD Contractors Avatar User Request Form
F. Staff/Contractor Request to Block Access to Chart Form
G. MH Contractor Credentialing Termination
H. AOD Contractor Credentialing Termination
I. ADP Electronic Signature Agreement & Electronic Signature Certification
J. ADP Bulletin No. 10-01

Attachments are located at: http://www.smchealth.org/bhrs-policies/electronic-medical-record-security-and-electronic-signatures-17-01

PURPOSE:

BHRS and contractors will maintain records and information in accordance with the HITECH Act, HIPPA, 45 CFR, California medical records law and other authorities listed above.

This policy ensures that access to the San Mateo County Behavioral Health and Recovery Services (BHRS) Electronic Health Record (EHR, aka AVATAR) is limited to qualified individuals who require access for their role in the BHRS system of care. This policy covers the privacy and security of Personal Information (PI) Personally Identifiable Information (PII) and Personal Health Information (PHI) both subject to and not subject to HIPPA. BHRS and contractors may use or disclose Department of Health Care Services (DHCS), BHRS, or BHRS contractor PI, PII, PHI only to perform functions, activities or services specified in the contract with DHCS and/or BHRS.

The policy details processes to ensure:

1) Access is limited to authentic and specific need;
2) Charts/information are blocked as required to protect confidentiality and privacy;
3) Documents that are created and signed electronically meet all requirements for the BHRS EHR and any external EHR's used to document services.

DEFINITIONS:

Access Levels to the BHRS EHR (Avatar)

1. Look Up Only Access:
   Internal BHRS staff including MH/AOD administrative staff, non-BHRS county staff, and contractors needing Look-Up Only access, (e.g., PES, Correctional Health, Aging & Adult Services) will only see content appropriate for their role and cannot document into the EHR.
2. MH Contractor Access/AOD Contractor Access:
   Contract Agency staff needing access to the BHRS EHR and who use Practice Management (PM) or Clinical Workstation (CWS) will have access to the EHR as appropriate to their role and document limited information into the EHR as determined for each role and agency.
3. BHRS Staff or On-site Contractor Access - General Access:
   Clinical and administrative staff, including volunteers and trainees may document in the EHR and access information appropriate to their position.
4. BHRS Staff or On-site Contractor Access -Full Access:
   This is a limited group including MIS, QM, executive management, limited administrative staff, and IT who have full access to the EHR as necessary for their function and support role.

Protected Information

"Personal Information" (PI) - DHCS PI" means Personal Information (PI), accessed in a database maintained by DHCS, received by BHRS or contractor from DHCS or acquired or

created by BHRS in connection with performing the functions, activities and services specified in a contract with DHCS and San Mateo County on behalf of the DHCS.

"Personally Identifiable Information" (PII) has the meaning given to this term in the IEA and CMPPA. "IEA" shall mean the Information Exchange Agreement currently in effect between the Social Security Administration (SSA) and the California DHCS. "CMPPA Agreement" means the Computer Matching and Privacy Protection Act Agreement between the SSAand the California Health and Human Services Agency (CHHS).

"Protected Health Information" (PHI). Under the US Health Insurance Portability and Accountability Act (HIPAA), PHI that is linked based on the following list of 18 identifiers must be treated with special care:

1. Names
2. All geographical identifiers smaller than a state, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census: the geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and the initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000
3. Dates (other than year) directly related to an individual
4. Phone numbers
5. Fax numbers
6. Email addresses
7. Social Security numbers
8. Medical record numbers
9. Health insurance beneficiary numbers
10. Account numbers
11. Certificate/license numbers
12. Vehicle identifiers and serial numbers, including license plate numbers;
13. Device identifiers and serial numbers;
14. Web Uniform Resource Locators(URLs)
15. Internet Protocol (IP) address numbers
16. Biometric identifiers, including finger, retinal and voice prints
17. Full face photographic images and any comparable images
18. Any other unique identifying number, characteristic, or code except the unique code assigned by the investigator to code the data

POLICY:

Any safety concern about the privacy or security of any BHRS or DHCS related information including PI, PII and PHI will immediately be reported to BHRS QM/Privacy Officer by utilizing BHRS Policy 93-11 and completing a Critical Incident Report. QM will investigate the situation and report to the San Mateo County Security Officer and BHRS Compliance

Officer. Any required reporting or notification to DHCS or other governmental bodies will be conducted by BHRS QM/Privacy Officer.

Safeguards***:*** These provide appropriate and reasonable administrative, technical, and physical safeguards to protect the security, confidentiality and integrity of BHRS and contractors PI and PII, to protect against anticipated threats or hazards to the security or integrity of BHRS PI and PII, and to prevent use or disclosure of PI or PII other than as provided for within contractual agreements with BHRS. This policy sets forth a written information privacy and security program that includes administrative, technical and physical safeguards and the nature and scope of its activities, which incorporate the requirements of security as described below.

Security: BHRS and contractors shall take any and all steps necessary to ensure the continuous security of all computerized data systems containing PHI and/or PI, and to protect paper documents containing PHI and/or PI. These steps shall include, at a minimum:

a. Complying with all of the data system security precautions listed in The Office of Management and Budget (OMB) Circular No. A-130

b. Providing a level and scope of security that is at least comparable to the level and scope of security established by the Office of Management and Budget in OMB Circular No. A-130, Appendix III - Security of Federal Automated Information Systems, which provides guidelines for automated information systems in federal agencies.

c. If data obtained by BHRS/Contractor from DHCS includes PII, the Contractor shall also comply with the substantive privacy and security requirements in the Computer Matching and Privacy Protection Act Agreement between the SSA and the CHHS and in the Agreement between the SSA and DHCS known as the Information Exchange Agreement. Any misuse of DHCS or BHRS PI, PII, PHI may result in termination of employment or contract and may result in penalties and/or fines.

Declaration of Notice of Confidentiality

All BHRS staff and contractors must sign and attest to maintain confidential all BHRS related data and follow the requirements set forth in the annual agreement. Contractors are required to maintain copies of signed declarations within employment records, which will be available upon request by BHRS or DHCS (or other regulatory body).

Access to the BHRS EHR/Avatar: Granted as needed to perform duties related to BHRS after the required documents and trainings are completed. Instructions and resources needed to obtain access to BHRS's EHR are at: http://www.smchealth.org/bhrs/avataraccess

Before access is granted, all user types must complete the paperwork needed and the required online trainings with surveys to demonstrate completion:

a. Introduction to the BHRS Avatar Electronic Medical Record training
b. BHRS Confidentiality & HIPAA for Mental Health & AOD training

Both trainings are located at: http://www.smchealth.org/bhrs/providers/ontrain

Additional training requirements for clinical staff are located at:
http://www.smchealth.org/bhrs/avataraccesss

Contract agencies must inform BHRS within one business day when a staff person with access to the BHRS EHR is no longer employed or needs a change of access level using either Attachment G or Attachment H. (See Section 4 below.)

1. Request To Block User Access to BHRS EHR: Blocking User Access to specific charts
    a. Avatar users may only view charts for which they have a business need to do so as part of their role at BHRS.
    b. Users are responsible for indicating whether charts should be blocked from their own or others' view by completing Attachment F Staff/Contractor Request to Block Access to Chart Form. Users should complete this form if any of the following are applicable:
        - They are both a client/former client and a staff person/family partner/volunteer; used to restrict co-workers from viewing past/current records
        - They know a client/former client personally outside of BHRS
        - They are a parent/spouse/relative of a client

2. Ensuring Electronic Signatures Meet Requirements
    a. BHRS staff and contractors submitting or documenting services for clients that contain electronic signatures for staff and/or clients must comply with the guidelines set forth in Attachment A, DMH Letter No: 08-10 dated December 4, 2008.
    b. In addition, (Substance Use Disorder) SUD contractors submitting or documenting services for clients that contain electronic signatures for staff and/or clients must comply with the guidelines set forth in Attachment J, ADP Bulletin 10-01.
    c. BHRS EHR users who document in the system must read and sign Attachment B, The eCC Electronic Signature Agreement form to indicate their compliance.
    d. The BHRS EHR is the official medical record; to ensure that documents with electronic signatures are protected and filed correctly, all changes to finalized documents must be approved by BHRS QM.
    e. Organized Delivery System (ODS)/SUDS programs will utilize Attachment I- The ADP Electronic Signature Agreement & Electronic Signature Certification. This form must be signed by all ODS/SUD staff who use an electronic signature and will be maintained in the staff person's personnel file.

3. Terminations
    a. Contractors
        i. Contractor Agency staff must fill out the appropriate Contractor Credentialing Termination form (Attachment G or H) with the effective date of termination.
        ii. Forms must be emailed to the address at the top of the attachment within one business day of termination.

b. BHRS Staff
    i. All supervisors are required to inform payroll/personnel within 24 hours of an employee's notice of termination.
    ii. BHRS payroll/personnel will inform QM within 24 hours of the notice from the supervisor, and provide the effective date of termination.
    iii. QM will inform MIS of the employee's termination date.
    iv. MIS will terminate the practitioner's enrollment and inform the BHRS IT Team.
    v. BHRS IT will terminate the computer and EHR accounts and disable the badge for the terminated employee.

Approved: *(Signature on File)*
Scott Gruendl, MPA
BHRS Assistant Director and
Compliance Officer

Approved: *(Signature on File)*
Stephen Kaplan, LCSW
BHRS Director