	County of Sacramento **Department of Health Services** **Division of Behavioral Health Services** **Policy and Procedure**	Policy Issuer (Unit/Program)	BHS-CMH-YDF
		Policy Number	08-01
		Effective Date	10/2009
		Revision Date	07/2017
Title: Administrative, Technical and Physical Safeguards		Functional Area: Health Information Management	
Approved By: Matthew Quinley, LCSW Health Program Manager Christopher Eldridge, LMFT Mental Health Program Coordinator			

Background/Context:

The Sacramento County Juvenile Justice Institutions Mental Health Team (JJIMHT) is a Health Insurance Portability and Accountability Act (HIPAA) covered component. As such, JJIMHT is required to implement reasonable safeguards to ensure the confidentiality, integrity and availability of clients' protected health information (PHI) and limit incidental uses or disclosures made pursuant to an otherwise permitted or required use or disclosure. The information to be safeguarded may be in any medium, including paper, electronic, oral and visual representations of confidential information.

Under the federal HIPAA, those provisions of HIPAA concerning the privacy and confidentiality of a person's confidential health information do not supersede those California state law provisions and other federal law provisions that are more stringent than HIPAA.

Title 15, Section 1407 requires the Youth Detention Facility (YDF) to establish policies and procedures, consistent with applicable laws, for the multi-disciplinary sharing of health information. The nature and extent of the information shared shall be appropriate to treatment planning, program needs, protection of the youth or others, management of the facility, maintenance of security, and preservation of safety and order.

Purpose:

The objective of this policy and procedure is to implement reasonable and appropriate safeguards within the workplace that JJIMHT members shall use to minimize the risk of unauthorized access, use or disclosure and to protect the PHI of youth being served within the Youth Detention Facility (YDF).

Details:

1. Workplace Practices for Oral Communications
   A. JJIMHT members must take reasonable precautions to protect the privacy of all verbal exchanges or discussions of confidential information, regardless of where the discussion occurs.

B. Discussions concerning confidential information shall not take place in public areas. JJIMHT members shall be aware of the risk levels associated with locations within the facility where verbal exchanges may take place:
    I. Low risk: enclosed offices, enclosed spaces on the living units, conference rooms, unoccupied classrooms and enclosed visiting center rooms
    II. Medium risk: employee only areas, telephones, individual cubicles, unoccupied unit day space
    III. High risk: public areas, open area in the visiting center, occupied unit day spaces, hallways, shared cubicle areas
C. JJIMHT members shall be aware of the risk levels associated with interviewing youth and verbal communication with other disciplines within the YDF and will consider available resources to reduce the risk of inadvertent verbal disclosures of confidential information.

2. Workplace Practices for Paper Documents
    A. The JJIMHT retains files and documents in locked file cabinets in a secure, locked chart room.
    B. Those JJIMHT members authorized, based on work role that have a business need for the use of printed information from Avatar, Probation and/or other disciplines within the facility, may print or obtain a copy of the information (e.g. Diagnosis and Movement History, Progress Notes, Assessments, YDF Daysheet, Inmate Information Per Housing Location, etc.)
    C. Each authorized individual who either prints or is issued paper documents for use according to their work role shall ensure the information is protected during use and placed in the locked, confidential shred box immediately upon completion of the task requiring use of the information.
    D. JJIMHT members having a business need to remove documents from YDF shall ensure the documents are in a secure, locked case and remain in their possession at all times. The documents shall be placed in the locked, confidential shred box immediately upon completion of the task requiring use of the information and return to YDF.
    E. In work stations, JJIMHT members shall take reasonable efforts to ensure the safeguarding of confidential information and the minimum necessary access to PHI by turning documents face-down, placing unattended documents in file cabinets/drawers and out of sight of unauthorized individuals who may enter the mental health suite. This includes: desks, fax machines, photocopy machines and computer printers.
    F. When necessary to pass information to another member not currently present, JJIMHT members shall place all documents containing PHI face-down in the other member's in-box under a cover sheet.
    G. All documents containing PHI awaiting scanning to the electronic mental health record (EHR) shall be placed face-down in the designated area of the secure chart room and immediately placed in the locked, confidential shred box upon verification of having been scanned into the EHR.

H. JJIMHT members shall not keep “personal” shred boxes in their work stations, documents awaiting destruction shall be placed in the locked, confidential shred box located in the secure chart room.

3. Workplace Practices for Electronic Devices
   A. JJIMHT members must ensure that observable confidential information is adequately shielded from unauthorized disclosure on electronic equipment, including desktop computers; laptop computer screens, cellular devices and other electronic devices used to access or print such information.
   B. JJIMHT members shall lock computer screens when leaving their cubicle or office area and exercise other effective means of safeguarding PHI as available.
   C. Cellular devices, electronic tablets and other devices capable of cellular or internet access are prohibited within the secure perimeter of the YDF. JJIMHT members shall not utilize such devices while in the YDF. (Pagers may be worn.)
   D. JJIMHT members shall ensure documents on printers, fax machines, photocopy machines are removed promptly. When scanning, faxing or sending documents by e-mail, members shall monitor the device during the transmission process and clear the device (press the function clear button) upon completion of the transmission.
4. Workplace Practices for Administrative Safeguards
   A. The implementation of role based access and the minimum necessary policy will promote administrative safeguards. Role based access is a form of security authorizing access to data based on job function in accordance with Division of Behavioral Health Services (DBHS) security procedures. JJIMHT members shall be assigned to a role based set allowing members access only to the minimum necessary information to fulfill their job functions.
   B. DBHS has written policies and procedures designed to comply with the HIPAA Privacy Rule. The policies and procedures are reviewed and shall be changed when necessary to comply with changes in the law.
   C. As a HIPAA covered entity, JJIMHT receives regular assessments in order to evaluate and improve the effectiveness of current safeguards for PHI.
   D. JJIMHT members receive initial HIPAA training within a specified number of days of hire and regularly scheduled HIPAA training according to the law or as assigned.
   E. DBHS regularly reviews electronic applications that contain PHI to evaluate and improve the effectiveness of current safeguards.
   F. DBHS shall apply sanctions, including appropriate disciplinary action, against members of the workforce who fail to comply with HIPAA policies and procedures. All sanctions shall be documented. There are specific exemptions to the application of sanctions.
   G. DBHS has a designated privacy official who is responsible for the development and implementation of the County’s privacy policies and procedures, and a contact person/office responsible for receiving complaints and providing information about matters covered by the required Notice of Privacy Practice.

Reference(s)/Attachment(s):

BHS-HIPAA-AS-100-05-Administrative, Technical and Physical Safeguards

Related Policies:

BHS-CMH-YDF-02-03-Confidentiality

BHS-CMH-YDF-08-02-DBHS Compliance Program

BHS-CMH-YDF-08-06-HIPAA Complaints and PHI/EPHI Breach Protocol

BHS-CMH-YDF-08-07-Record Management

BHS-CMH-YDF-08-08-Penalties for Privacy Violations

BHS-CMH-YDF-08-09-Release of Protected Health Information

BHS-CMH-YDF-08-10-Release of Verbal Information in a Medical Emergency

BHS-CMH-YDF-08-11-Methods for Releasing Protected Health Information

BHS-CMH-YDF-08-12-Accounting of Disclosures

BHS-CMH-YDF-10-01-Facility Access Policy

BHS-CMH-YDF-10-04-Use of Computers

Contact Information:

Christopher Eldridge, LMFT, Mental Health Program Coordinator, (916)876-9339, eldridgec@saccounty.net