COUNTY OF YOLO

HEALTH AND HUMAN SERVICES AGENCY

POLICIES AND PROCEDURES

SECTION 5, CHAPTER 4, POLICY 003

PRIVACY OR SECURITY INCIDENT REPORTING

A. PURPOSE

To provide Yolo County Health and Human Services Agency (HHSA) Behavioral Health staff with guidance on the requirements for identifying a privacy or security incident, individual responsibility for reporting an incident, and how to report an incident to the HHSA Behavioral Health Compliance Officer immediately upon discovery.

B. FORMS REQUIRED/ATTACHMENTS: N/A

C. DEFINITIONS:

1. **Department Personal Information (DPI):** personal information accessed in a database maintained by the Department of Health Care Services (DHCS), received by HHSA from the DHCS or acquired or created by HHSA in connection with performing the functions, activities and services specified in the State Agreements on behalf of the DHCS.
2. **Personal Information (PI):** any information that is maintained by an agency, including DHCS, 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.
3. **Personally Identifiable Information (PII):** any information that can be used to distinguish or trace a consumer's identity (e.g., his or her name, Social Security Number, biometric records) alone or when combined with other personal or identifying information that is linked or linkable to a specific consumer (e.g., date of birth, place of birth, mother's maiden name).
4. **Privacy/Security Incident:** The attempted or successful unauthorized access, use, disclosure, modification, or destruction of PHI or interference with system operations in an information system that does not result in a breach.
5. **Protected Health Information (PHI):** individually identifiable health information that is created or received by a health care provider, health plan, employer, or health care clearinghouse and that relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual in any form or medium (electronic, paper, microfiche, or verbal).
6. **Unauthorized Access:** Inappropriate/ impermissible entry, contact, review, opening or viewing of employee, public, or client information without direct need for medical diagnosis, treatment, business purpose or other lawful use; and any other unlawful use not permitted by state or federal laws governing the use or disclosure of confidential information, medical or otherwise personal.

7. **Unauthorized Disclosure**: Inappropriate/impermissible release, announcement, publication or statement of employee, public or client PHI without direct need for medical diagnosis, treatment, business purpose or other lawful use; and any other unlawful release not permitted by state or federal laws governing the use or disclosure of confidential information, medical or otherwise personal.
8. **Unauthorized Use:** Inappropriate/ impermissible handling, application, operation, or management of employee, public or client information without direct need for medical diagnosis, treatment, business purpose or other lawful use; and any other unlawful application not permitted by state of federal laws governing the use or disclosure of confidential information, medical or otherwise personal.

D. POLICY

It is the policy of HHSA Behavioral Health to adhere to state and federal regulations pertaining to the reporting of privacy and/or security incidents, including breaches.

E. PROCEDURES

1. The following are examples of actions that may be considered a privacy or security incident. Staff are required to report such actions to the HHSA Behavioral Health Compliance Officer immediately upon discovery. Examples include, but are not limited to, the following:

   a. Faxing or emailing PHI/PII/DPI/PI to the wrong recipient.
   b. Emailing PHI/PII/DPI/PI to anyone outside the County network, including yourself, without encryption. Email subject lines must not include PHI/PII/DPI/PI information.
   c. Sending correspondence to the incorrect person.
   d. Releasing PHI/PII/DPI/PI to a person or entity with an expired ROI or Authorization for Release of Protected Health Information.
   e. Misplacing/losing a medical record after a thorough search.
   f. Accessing/using HHSA and/or County resources to verify if a family, friend, or acquaintance are clients.
   g. Accessing, using or disclosing information obtained from MEDS other than to assist in the administration of the Medi-Cal program.
   h. Accessing, or viewing a medical record you did not need to access for a legitimate business purpose or to perform job tasks/duties.
   i. Being the victim of theft where HHSA medical records or HHSA property are taken.
   j. Leaving medical records or PHI/PII/DPI/PI in an unattended vehicle.
   k. "Checking in" baggage containing medical records or PHI/PII/DPI/PI on modes of public transportation; not keeping items in personal custody as carry on.
   l. Giving or using another person's login and password HHSA systems.
   m. Leaving medical records or PHI/PII/DPI/PI unsecured, examples: open and unattended on the desk, unlocked medical charts, unlocked PII, etc.

n. Allowing unauthorized persons in the work area without a legitimate business purpose.

o. Discussing with or disclosing to others PHI/PII/DPI/PI without a legitimate business purpose and/or without authorization from the client.

p. Discarding PHI/PII/DPI/PI or medical records improperly and/or not in accordance to retention timeframes.

2. It shall be the responsibility of the HHSA Behavioral Health staff to report any incidents/breach of PHI/PII/DPI/PI to the HHSA Behavioral Health Compliance Officer, who shall conduct an investigation and determine reporting requirements in accordance to State, Federal, and Local rules and regulations.

   a. HHSA Staff shall be responsible for reporting any privacy/security incidents immediately, and no later than the date of discovery to:

      HHSA Behavioral Health Compliance Officer
      137 N. Cottonwood St. #2611
      Woodland, CA 95695
      530-666-8654

   b. HHSA Subcontracted Providers shall be required to remain in compliance with all applicable provisions of HIPAA, the HITECH Act, to ensure the physical and technical safeguards to protect PHI/PII/DPI/PI.

      Additionally, subcontracted providers shall be required to report any privacy/security incidents immediately, and no later than the date of discovery to:

      HHSA Behavioral Health Compliance Officer
      137 N. Cottonwood St. #2611
      Woodland, CA 95695
      530-666-8654

      A completed report of the investigation and remediation shall be provided to the HHSA Behavioral Health Compliance Officer, to include findings within five (5) working days. If additional time is necessary to submit a completed report, weekly updates shall be required until a completed final report is submitted.

   c. The HHSA Behavioral Health Compliance Officer shall be responsible for, upon discovery of a security incident or breach, the following steps to ensure prompt reporting:

      i. Notifying DHCS immediately by telephone call or email or fax upon the discovery of a breach of unsecured PHI/PII/DPI/PI in electronic media or any other media, or is reasonably believed to have been, accessed or acquired by an unauthorized person.

      ii. Notifying DHCS within 24 hours (one hour if SSA data) by email or fax of the discovery of any suspected security incident, intrusion or unauthorized access, use or disclosure of PHI in violation to applicable state and federal rules and regulations.

iii. Notice shall be provided to the Information Protection Unit, Office of HIPAA Compliance by calling 916-445-4646, 866-866-0602 or via email at privacyofficer@dhcs.ca.gov; using the Privacy Incident Report form.

iv. The compliance officer shall implement prompt corrective action to mitigate any risks or damages involved with the breach and to protect the operating environment; and any action pertaining to unauthorized disclosure required by Federal and State laws and regulations.

v. Immediately investigate any suspected security incidents, breach, or unauthorized access, use or disclosure of PHI and submit a Privacy Incident Report within 72 hours upon discovery and submit to the above-mentioned Information Protection Unit.

vi. A completed report of the investigation shall be submitted to applicable state agency program managers and the Information Protection Unit within ten (10) working days of the discovery of the breach or unauthorized use or disclosure.

vii. Notify affected individuals in accordance to Federal and State laws and regulations.

viii. Issue a memo to the Deputy Director of Mental Health to include recommendation of corrective actions.

ix. Provide guidance to the Deputy Director of Mental Health and Senior Management to ensure corrective action is implemented and completed.

d. HHSA Program Managers shall be responsible for ensuring completion of corrective actions if applicable to their staff and/or program.

3. HHSA Behavioral Health staff and subcontracted providers may be subject to the following actions due to a privacy and/or security violation:

   a. Corrective action including, but not limited to, receiving re-training on privacy and security measures, reviewing existing policy and signing policy acknowledgement forms.

   b. Disciplinary action, up to and including termination of employment or subcontracts.

   c. Civil or criminal liability.

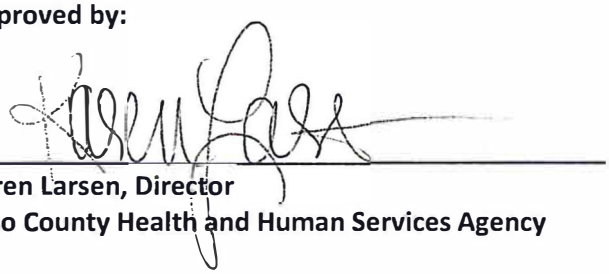
4. Omission or failure to report a privacy or security incident may subject members of HHSA Behavioral Health and its' subcontracted providers to disciplinary action, up to and including, termination of employment or subcontracts.

F. References

1. Cal. Civ. Code §§56 et seq. (The Confidentiality of Medical Information Act)
2. Department of Behavioral Health Medi-Cal Privacy and Security Agreement
3. Cal. Welf. & Inst. Code §14100.2
4. Social Security Act, §1137 and §453
5. 45 C.F.R. §164 et al.
6. 42 C.F.R. Part 2

7. Health Insurance Accountability and Portability Act of 1996

Approved by:



Karen Larsen, Director
Yolo County Health and Human Services Agency

12/20/17
Date