County of Marin **Mental Health & Substance Use Services (MHSUS)**	POLICY NO. MHSUS-ADP-06 Next Review Date: July, 2018
POLICY: **USE OF ELECTRONIC HEALTH RECORDS** **SUPERCEDES: MHSUS PROGRAMMATIC AND ADMINISTRATIVE POLICIES, PROCEDURES, STANDARDS AND PRACTICES FOR ALCOHOL, TOBACCO AND OTHER DRUG SERVICES**	Date Reviewed/Revised: July 30, 2015 By: Suzanne Tavano Suzanne Tavano, PhD MHSUS Director

POLICY: USE OF ELECTRONIC HEALTH RECORDS

I. **PURPOSE:** The purpose of this policy is to ensure that the Protected Health Information (PHI) and Personally Identifiable Information (PII) of all Alcohol and Drug treatment clients served under public funding is managed and protected in accordance with HIPAA, 42 CFR,HITECH Act and the California Code of regulations.

II. **REFERENCES:**
Net Negotiated Agreement pg. 35
42C.F.R §438.242
California Code of Regulations, tit.9 §1810.376

III. **POLICY:**
It is the Policy of Marin County Mental Health and Substance Use Services that all client electronic health information must be stored in a qualified Health Information System (HIS) that meets the standards of 42 C.F.R. §438.242 and is consistent with California Code of Regulations., tit.9 §1810.376.

IV. **AUTHORITY/RESPONSIBILITY:**
Contract Managers
Alcohol and Drug Administrator
Marin WITS Administrator
MHSUS Director

V. **PROCEDURE:**
County of Marin MHSUS staff and contracted providers must use a qualified HIS to store and submit CalOMS, TEDS and NOMS data and electronic health records.

Pursuant to 42 C.F.R. §438.242 and consistent with Cal.Code Regs., tit.9 §1810.376, Marin County Mental Health and Substance Use Services maintains Marin WITS as its Substance Use Disorders Services Health Information System that collects, analyzes, integrates, and reports data. The system provides information on areas including, but not limited to, utilization, grievances, and appeals.

County and contracted treatment providers are required to use Marin WITS to fulfill CalOMS data requirements, as identified in the MHSUS CalOMS Treatment Policy and record and submit service information for reimbursement. All CalOMS, TEDS and NOMS data must be stored and submitted via Marin WITS, a Health Information System that:

a. Collects data on beneficiary and provider characteristics as specified by the State, and on services furnished to beneficiaries as specified by the State;
b. Ensures that data received from providers is accurate and complete by
    i. Date, Time, and User stamping all the data entry and review of client information;
    ii. Provides a log to track both provider activity and client chart activity;
    iii. Incorporates business rules that screen the data for completeness, logic and consistency;
    iv. Collects service information in standardized formats.

In addition contractors are permitted to use Marin WITS as their Electronic Health Record. Contractors who use another Health Information System in addition to or instead of Marin WITS must attest annually at contract renewal [Attachment A] that their Health Information System meets 42 C.F.R, HIPAA, and HITECH by meeting the following requirements:

a. Has a unique log-in and password as well as specific permissions set for each user. Ref: HIPAA Requirement: Access Control. A covered entity must implement technical policies and procedures that allow only authorized persons to access electronic protected health information (e-PHI).
b. Has a protected access log that records any access to the system and an audit log for access to client information for clinical or billing purposes. Ref: HIPAA Requirement: Audit Controls. A covered entity must implement hardware, software, and/or procedural mechanisms to record and examine access and other activity in information systems that contain or use e-PHI.
c. Has safeguards to ensure information cannot be inappropriately erased, altered or destroyed ref: HIPAA Requirement: Technical Safeguards Integrity Controls. A covered entity must implement policies and procedures to ensure that e-PHI is not improperly altered or destroyed. Electronic measures must be put in place to confirm that e-PHI has not been improperly altered or destroyed.
d. Meets the Transmission Security HIPAA requirement: Transmission Security. A covered entity must implement technical security measures that guard against unauthorized access to e-PHI that is being transmitted over an electronic network.
e. Meaningful Use/ 42 CFR Requirements: handles client requests to make an amendment to their record.
f. Logs users off after a specified period of inactivity.
g. Permits an identified set of users to access electronic health information during an emergency.
h. Tracks disclosures of PHI.
i. Can generate an electronic copy of a client's record.

ASSURANCE OF QUALIFIED HEALTH INFORMATION SYSTEM

FISCAL YEAR 2015/16

_____

Agency/Organization Name

As the duly authorized representative of the agency/organization named above, I understand that all client health information that is stored or transmitted electronically must be within a qualified Health Information System (HIS). I certify that my agency uses:

____ Marin WITS as our only HIS system. We do not collect, store or transmit e-PHI (i.e. diagnosis, treatment notes or plans, or services rendered) in any other system.

____ Marin WITS and _____ (name of HIS) a product of _____ (vendor) which meets the following criteria:

a. Has a unique log-in and password as well as specific permissions set for each user. Ref: HIPAA Requirement: Access Control. A covered entity must implement technical policies and procedures that allow only authorized persons to access electronic protected health information (e-PHI).24
b. Has a protected access log that records any access to the system and an audit log for access to client information for clinical or billing purposes. Ref: HIPAA Requirement: Audit Controls. A covered entity must implement hardware, software, and/or procedural mechanisms to record and examine access and other activity in information systems that contain or use e-PHI.25
c. Has safeguards to ensure information cannot be erased, altered or destroyed ref: HIPAA Requirement: Technical Safeguards Integrity Controls. A covered entity must implement policies and procedures to ensure that e-PHI is not improperly altered or destroyed. Electronic measures must be put in place to confirm that e-PHI has not been improperly altered or destroyed.26
d. Meets the Transmission Security HIPAA requirement: Transmission Security. A covered entity must implement technical security measures that guard against unauthorized access to e-PHI that is being transmitted over an electronic network.27

e. Meaningful Use/ 42 CFR Requirements: handles client amendments to a record.
f. Logs users off after a specified period of inactivity.
g. Permits an identified set of users to access electronic health information during an emergency.
h. Tracks disclosures of PHI.
i. Can generate an electronic copy of a client's record.

Director of Agency or Authorized Signatory:

_____		_____
Signature	Date	Print Name and Title