


County of Marin Behavioral Health and Recovery Services (BHRS)	POLICY NO. BHRS-SUS-08
	Next Review Date: June 2021
POLICY:	Date Reviewed/Revised: June 29, 2018
<u>MARIN WITS ELECTRONIC SIGNATURE POLICY</u>	 By: _____ Jen Africa, PsyD Director of Behavioral Health and Recovery Services
SUPERCEDES: MHSUS-ADP-08	

POLICY: MARIN WITS ELECTRONIC SIGNATURE POLICY

I. PURPOSE:

The purpose of this policy is to ensure the verity of each staff persons electronic signature in Marin WITS.

II. REFERENCES:

42C.F.R. § 438.242
Cal. Code Regs., tit.9, § 1810.376
ADP Bulletin 10-01
WITS User Change Request Form

III. POLICY:

Behavioral Health and Recovery Services (BHRS) staff and contracted providers and their employees and subcontractors must sign and abide by the terms of a Marin WITS electronic signature agreement in order to receive or maintain access to Marin WITS and the attached electronic signature.

IV. AUTHORITY/RESPONSIBILITY:

Contract Managers
Marin WITS Administrator
Alcohol and Drug Administrator
MHSUS Director

V. PROCEDURE:

The County of Marin provides Marin WITS (CCMS EHR Certification ID 30000005YWLAEAS) to its BHRS staff and contracted providers to use as an Electronic Health Record and Billing program. Marin WITS meets the state's definition of a Health Information System as outlined in the State/County contract pursuant to 42C.F.R. § 438.242 and consistent with Cal. Code Regulations., tit.9, § 1810.376.

County of Marin Behavioral Health and Recovery Services (BHRS)	POLICY NO. BHRS-SUS-08
POLICY: <u>MARIN WITS ELECTRONIC SIGNATURE</u> <u>POLICY</u>	Next Review Date: June 2021 Date Reviewed/Revised: June 29, 2018

Access to Marin WITS may only be granted by designated BHRS staff or FEI, Inc. Marin WITS tracks electronic access and Electronic Signatures of all users within the system. This information will be used in regular monitoring activities as well as in investigations into grievances and appeals.

To ensure the verity of each staff and contractors electronic signature in Marin WITS, County BHRS will:

1. Require all staff and contractors to email a completed Marin WITS user request/change form [Attachment A] to the Marin WITS Administrator and copy their Contract Manager. When users leave or change roles this must be submitted prior to or within 24 hours of the change.
2. BHRS staff and each contractor and its employees and subcontractors must sign and abide by the terms of a Marin WITS Electronic Signature Agreement [Attachment B] in order to receive or maintain access to Marin WITS and the attached electronic signature. This agreement requires users to not share their password and pin with anyone including other contractor staff, county staff or other contractors. Completed agreements should be emailed to the Marin WITS Administrator and copy their Contract Manager.
3. Upon receipt and approval of all completed documents the Marin WITS Administrator or Contract Manager will make the requested changes within 10 business days.
4. The Marin WITS system creates and emails a new password and pin to the signatory's email account. To ensure that the signature remains protected the receiving email account must be approved by the requester's management and accessible only to the owner of the electronic signature.
5. Users of the Marin WITS system must immediately inform the BHRS Marin WITS Administrator by phone or in writing if they know or suspect that their signature has been compromised. BHRS Marin WITS Administrator will inform the appropriate BHRS and/or Agency privacy specialists of the suspected issue for review.
6. If the signature has been or is suspected of being compromised Marin County BHRS will terminate access to Marin WITS.
7. A new signature and access may be granted if a review finds that the compromised signature was not the fault of the signer, did not result in a breach of PHI or PII, or was not a violation of the electronic signature agreement.
8. To protect the integrity of Electronic Signatures the Marin WITS Administrator will review user access a minimum of four times per year and deactivate any accounts that have not been used within 90 days.