

Attn: Information Systems 1900 Embarcadero Cove, Suite 400 Oakland, California 94606 (510) 567-8181 / Fax (510) 567-8161 QIC 28004

BHCS SYSTEMS & DATA Confidentiality, Security and Usage Agreement

Systems

InSyst, Clinician's Gateway, eCURA, Yellowfin, CANS/ANSA, MEDS, etc.

Purpose

The purpose of this agreement is to establish an environment of security for the electronic storing and usage of client confidential information and records including the usage of portable electronic devices for this purpose.

Background

Any person accessing Alameda County BHCS (Behavioral Health Care Services) data is required to protect confidential information relating to clients, patients, and residents on a daily basis, and have a duty to protect this information from loss, theft, or misuse whether the information is in paper or electronic form. Additionally, users are required to protect any electronic device assigned to them or in their possession used to gain access to BHCS systems.

Confidential Information

Confidential Information shall include all Alameda County BHCS systems, documents, data, and other materials. User agrees that the Confidential Information is to be considered confidential and shall hold the same in confidence, shall not use the Confidential Information other than for the purposes of its business with BHCS, and shall disclose it only to its authorized employees or other authorized users with a specific need to know. User will not disclose, publish or otherwise reveal any of the Confidential Information and must use secure email for any communications outside of Alameda County regarding Confidential information.

Secure and Private Work Environment

User is responsible for taking proper security and privacy precautions ensuring a secure and private work environment while utilizing portable devices in order to safeguard client information displayed.

Security Agreement

User agrees to the stated required security criteria in order to access and utilize the BHCS systems.

I understand that sharing my account ID and password, client information or any breach of security is a HIPAA (Health Insurance Portability and Accountability Act) violation which may result in prison, fines up to \$25,000 and/or revocation of my license.

I attest that I have completed HIPAA security and privacy requirements training for protecting the confidentiality, integrity, and availability of protected health information under HIPAA within the past 12 months.				
 User Signature	User Printed Name	Date		

The supervisor agrees 1) to employee's usage of the system and 2) to provide information and direction for secure uses and practices while utilizing network resources.

The supervisor attests that the user has 1) signed an Oath of Confidentiality, 2) signed an Ethical Conduct Policy and 3) been trained in HIPAA security and privacy requirements.

•		
Supervisor Signature	Supervisor Printed Name	Date



Attn: Information Systems 1900 Embarcadero Cove, Suite 400 Oakland, California 94606 (510) 567-8181 / Fax (510) 567-8161 QIC 28004

ELECTRONIC SIGNATURE AGREEMENT

This Agreement governs the rights, duties, and responsibilities of Alameda County in the use of an electronic signature in Alameda County. The undersigned (I) understands that this Agreement describes my obligations to protect my electronic signature, and to notify appropriate authorities if it is stolen, lost, compromised, unaccounted for, or destroyed. I agree to the following terms and conditions:

I agree that my electronic signature will be valid for one year from date of issuance or earlier if it is revoked or terminated per the terms of this agreement. I will be notified and given the opportunity to renew my electronic signature each year prior to its expiration. The terms of this Agreement shall apply to each such renewal.

I will use my electronic signature to establish my identity and sign electronic documents and forms. I am responsible for protecting my electronic signature. If I suspect or discover that my electronic signature has been stolen, lost, used by an unauthorized party, or otherwise compromised, then I will immediately notify the County Mental Health Director or his/her designee and request that my electronic signature be revoked. I will then immediately cease all use of my electronic signature. I agree to keep my electronic signature secret and secure by taking reasonable security measures to prevent it from being lost, modified or otherwise compromised, and to prevent unauthorized disclosure of, access to, or use of it or of any media on which information about it is stored.

I will immediately request that my electronic signature be revoked if I discover or suspect that it has been or is in danger of being lost, disclosed, compromised or subjected to unauthorized use in any way. I understand that I may also request revocation at any time for any other reason.

If I have requested that my electronic signature be revoked, or I am notified that someone has requested that my electronic signature be suspended or revoked, and I suspect or discover that it has been or may be compromised or subjected to unauthorized use in any way, I will immediately cease using my electronic signature. I will also immediately cease using my electronic signature upon termination of employment or termination of this Agreement.

I further agree that, for the purposes of authorizing and authenticating electronic health records, my electronic signature has the full force and effect of a signature affixed by hand to a paper document.

_I understand that sharing my account ID and password, client information or any breach of

security is a HIPAA violation which may result in prison, fines up to \$25,000 or revocation of my license.		
→ EHR User Signature:	Date:	
User's Printed Name:	Staff ID Number:	
BHCS MHS Director or Director's Designee Signature:	Date:	
Title:		

Please fax signed copy to 510-567-8161 or email to HIS@acgov.org.

