Behavioral Health Department
Alameda County Health

Attn: Systems Support
1900 Embarcadero Cove, Suite 400
Oakland, CA 94606
(510) 817-0076 | Fax (510) 567-8161
HCSAsupport@acgov.org | QIC 28004

NETWORK ACCESS REQUEST

https://bhcsproviders.acgov.org/providers/Forms/Forms.htm

This form is to request network access to the ACBH web portal ***for the ability to complete and submit e-forms.***

Date Submitted: _____

CONTACT INFORMATION

Is this request for an Alameda County Employee or Community Based Organization / Provider?

◯ County Employee ◯ CBO / Provider

Contact First Name: _____

Contact Last Name: _____

Organization: _____

Clinic/Program: _____

Contact Cell #: _____

Contact Email: _____

Managers Name for Approval: _____

Managers Email: _____

After completing the form, please fax or email to the Systems Support Help Desk
Fax: 510.817.0076 or HCSAsupport@acgov.org

To Login to the ACBH Network, Use the following link:
https://bhcsportal.cloud.com/Citrix/StoreWeb/#/login

Behavioral Health Department
Alameda County Health

ACBH SYSTEMS & DATA
Confidentiality, Security and Usage Agreement (CSU)

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

Purpose
This Confidentiality, Security and Usage 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 Behavioral Health (ACBH) 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 ACBH systems.

Confidential Information
Confidential Information shall include all ACBH 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 ACBH, 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.
_____ Initial

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. _____ Initial

Security Agreement
User agrees to the stated required security criteria in order to access and utilize the ACBH systems. I understand that sharing any 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.
_____ Initial

Confidentiality, Security and Usage Agreement Acknowledgement
I understand that this Confidentiality, Security and Usage agreement can be revoked at any time. I also 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.

I attest that my Supervisor/Manager has pre-approved access to the system in my initial account request.
_____ Initial

_____	_____		_____
User Signature	User Printed Name	Staff ID#	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. **Supervisor/Manager - Only authorize the level of access to PHI that is necessary for the employee to perform their job per HIPAA.**

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