SmartCare User Request Form

&

Confidentiality and Network Agreement Form

Request Form Requirements

1. Request form must be submitted from the user's supervisor. The form will not be accepted if it is submitted by the user requesting the account.
2. User's name on request form must be their legal name and/or name on their license.
3. User receiving account must **electronically** sign the Confidentiality Agreement located at the bottom of the request form. The form will not be accepted if the Confidentiality Agreement is not signed or if it is not electronically signed.
4. Request form must be typed with an electronic signature. No hand-written form or **scanned in** form will be accepted.
5. Request form must be sent to the appropriate Provider Network Manager for approval first. Do not send the request form straight to the helpdesk, as it will not be accepted.

If you have any questions or issues submitting an electronic form/signature, please contact our HelpDesk at HelpDesk@kazoocmh.org

KALAMAZOO COMMUNITY Mental Health & Substance Abuse Services	**SMARTCARE USER REQUEST FORM**

***Required Field**

Type of request (Check One) *	☐ New / ☐ Change (Please indicate changes)		
Date of request*		Effective date*	
Name of User* (Legal Name)			
Credentials of user (Signature Suffix)			
Phone # of user		NPI of user	
Email address of user*			
Title/role*			
Responsibilities* (Related to SmartCare)			
Agency*			
Location(s)			
Name / Phone # of Requester			
User's Supervisor*			
User to clone for access* (Please provide user to clone **OR** SmartCare Role(s) below)			

Please select the appropriate role(s) that apply below, **only if a user to clone is not provided above**.

	SmartCare Role Name	Role Description
☐	Ancillary Clinician	**Read-only** access to all consumers in your program.
☐	Primary Clinician	Able to view and enter clinical information & documentation for consumers in your program (Including Authorization requests).
☐	Access (Intake)	Assigned to a user whom acts as an Access point and thus can see **ALL** consumers in the KCMHSAS system, in all programs and agencies. Users in this role can create new clients ****Caution**** should be used in selecting this role. Users in this role may be subject to additional auditing.
☐	Provider Insurance Maintenance	Modify rights to insurance information for consumers in your agency.
☐	External Provider Claim Entry	Access to enter and modify professional claims for consumers in your program and to view and print check details along with corresponding Remittance Advice for claims submitted by your program. Also, access to view CM authorization details for consumers in your program.
☐	External Provider view	**Read-only** access to claim details for claims submitted by your program and access to view authorization details for consumers in your program.

NPI	National Provider Identifier (10-digit number for the individual) See https://nppes.cms.hhs.gov Needed for individuals who perform professional services. These services can be billed to a third-party insurer. This does not include people who serve in a case management type role.
Credentials	The initials for all your credentials to include in your digital signature. If more than one, please circle your billing credentials.

KALAMAZOO COMMUNITY Mental Health & Substance Abuse Services	**CONFIDENTIALITY AND NETWORK AGREEMENT FORM**

***Required Field**

Access to consumer, employee and business information is a privilege granted on a need-to know (role based) basis. Every user must sign the KCMHSAS CONFIDENTIALITY AND NETWORK ACCESS AGREEMENT before access to any computer system will be granted – this includes KCMHSAS employees, students, interns, contractual providers, volunteers, consultants, associates, business partners and vendors who access our data.

The following rules for Confidentiality and Network Access apply to all consumer and business information (Confidential Information) of KCMHSAS and related organizations. The rules also apply to the business information of joint ventures, or of other entities and persons collaborating with KCMHSAS, to which the user has access. As a condition of being permitted to have access to Confidential Information relevant to my job function or role, I agree to the following rules (as applicable):

1. Permitted and required access, use and disclosure:
   - I will access, use or disclose Confidential Consumer Information (PHI) only for legitimate purposes of diagnosis, treatment, obtaining payment for consumer care, or performing other health care operations functions permitted by Michigan Mental Health Code (MMHC), 42 CFR Part 2, and HIPAA.
   - I will only access, use or disclose the minimum necessary amount of information needed to carry out my job responsibilities or business duties.
   - I will access, use or disclose Confidential Business Information only for legitimate business purposes of KCMHSAS.
   - I will protect all Confidential Information to which I have access, or which I otherwise acquire, from loss, misuse, alteration or unauthorized disclosure, modification or access, including:
     - Protecting my KCMHSAS password(s). Not sharing my KCMSHAS password(s) with others.
     - Making sure that paper records are not left unattended in areas where unauthorized people may view them.
     - Using password protection, screensavers, automatic time-outs or other appropriate security measures to ensure that no unauthorized person may access Confidential Information from my workstation or another KCMHSAS device.
     - Appropriately disposing of Confidential Information in a manner that will prevent a breach of confidentiality and never discarding paper documents or other materials containing Confidential Information in the trash unless they have been shredded.
     - Safeguarding and protecting portable electronic devices containing Confidential Information including laptops, smartphones, PDAs, CDs and USB thumb drives.
   - I will disclose Confidential Information only to individuals who have a need to know to fulfill their job responsibilities and business obligations.
   - I agree to carefully read the messages displayed upon successful log in and agree to the terms or directions.
   - I will call the KCMHSAS Helpdesk with any immediate concerns, 269-553-8059 or email Helpdesk at helpdesk@kazoocmh.org .
   - I will comply with KCMHSAS access and security procedures, and any other policies and procedures that reasonably apply to my use of the KCMHSAS computer systems and/or my access to information on or related to the KCMHSAS computer systems including off-site (remote) access using portable electronic devices.
2. Prohibited access, use or disclosure (as applicable):
   - I will not access, use or disclose Confidential Information in electronic, paper, or oral forms for personal reasons, or for any purpose not permitted by KCMHSAS policy, including information about co-workers, family members, friends, neighbors, high profile persons or myself.
   - I will follow the required procedures at KCMHSAS, and any KCMHSAS provider agency to request access to my own PHI in medical and other records.

- I will not use another person's KCMHSAS login ID, password, other security device or other information that enables access to KCMHSAS computer systems, networks, or applications, nor will I share my own with any other person.
- If my employment or association with KCMHSAS or any provider agency ends, I will not subsequently access, use or disclose any KCMHSAS Confidential Information and will promptly return any electronic devices and other KCMHSAS property. I will not engage in any personal use of KCMHSAS computer systems that inhibits or interferes with the productivity of employees, including myself, or others associated with KCMHSAS operations or business, or that is intended for personal gain. I will not engage in the transmission of information which is disparaging to others based on Age, Ancestry, Beliefs, Citizenship, Color, Culture, Family/marital status, Gender, Mental or physical ability, National origin, Physical appearance (i.e., weight and height), Political affiliation, Race, Religion, Sexual orientation, Gender identity or which is otherwise offensive, inappropriate or in violation of the mission, values, policies or procedures of KCMHSAS.
- I will not utilize the KCMHSAS network to access Internet sites that contain content that is inconsistent with the mission, values, and policies of KCMHSAS.

  Some examples of prohibited use of KCMHSAS computer resources:
  - Impersonating another person by sending forged messages.
  - Soliciting non-KCMHSAS business.
  - Intentionally interfering with the normal operation of the KCMHSAS network, including introducing and propagating computer viruses and sustained high volume network traffic such as chain letters.
  - Using the KCMHSAS email system for illegal or unethical purposes.
  - Revealing or publicizing any proprietary or confidential information such as consumer information, financial information, or system or network access codes.
  - Sending, receiving or storing any messages or files that are discriminatory, offensive, obscene, defamatory, pornographic or harassing.
  - The intentional installation of any unauthorized or unapproved software on KCMHSAS-owned devices.

3. Accountability and Sanctions:
   - I will immediately write an incident report and notify the KCMHSAS Breach Response Team at breachresponseteam@kazoocmh.org if I believe that there has been improper/unauthorized access to the KCMHSAS network or improper use or disclosure of confidential information in electronic, paper, or oral forms.
   - I understand that KCMHSAS will monitor my access to, and my activity within, KCMHSAS computer system, and I have no rightful expectation of privacy regarding such access or activity.
   - Specific to the KCMHSAS E-mail system, I understand that E-mails, sent, received or stored on KCMHSAS's system are treated as business records and KCMHSAS reserves the right to access, review copy and delete any messages. An E-mail message should be treated as if it is being sent under KCMHSAS letterhead with the understanding that it may be printed, forwarded, duplicated and subpoenaed in legal proceedings.

By signing below, I verify that I have read the KCMHSAS CONFIDENTIALITY AND NETWORK ACCESS AGREEMENT, understand my responsibilities and agree to follow this policy.

Printed/Typed Name* Date*

Agency*

X_____

Electronic Signature*