Adirondack Health Institute

Lead Empower Innovate

Title: Health Home Systems Access and Identity Assurance

Department: Health Home Serving Adults and Children

Effective Date: 7/1/2021

Date Revised: 10/1/2022;10/1/2023; 10/1/2024

Purpose of Policy

The Adirondack Health Institute Health Home (AHIHH) takes an active role in monitoring privacy and security measures for Health Home Service Providers and other individuals and entities who access Medicaid Confidential Data (MCD). The intent of this policy is to ensure all system users have met appropriate access and identify credentials safely and securely access participant's Personal Health Information (PHI) and Personal Identifying Information (PII). Protecting Health Home participant's PHI and PII is a major priority for the AHI Health Home and its stakeholders. Periodic review of this policy will assist in ensuring privacy security for our clientele. The policy establishes a framework for issuing and managing trusted identify credentials to all HHSP's and other stakeholders who access Health Home Systems and the associated PHI and PII.

Scope

1. This policy must be distributed to all AHI Health Home Program staff and all subcontracting Health Home Service Providers and other relevant stakeholders.
2. All recipients of this policy must acknowledge their receipt and understanding of the policy by referring any questions, problems, or compliance issues with the policy within ten days of the issue date to the AHI's Quality and Performance Improvement Specialist.
3. All questions regarding this policy or its implementation may be directed to the AHI's Quality and Performance Improvement Specialist.

Statement of Policy

AHI shall develop, disseminate, and review at least annually a Health Home Systems Access and Identity Assurance policy that addresses the purpose, scope, roles and responsibilities, management commitment, coordination among organization entities, and compliance. AHI shall formalize documented procedures to facilitate the implementation of the Health Home Systems Access and Identity Assurance policy.

Definitions

AHIHH: AHI Health Home, a designated lead Health Home by the New York State Department of Health

Health Home Participant: A Health Home Candidate who is participating in the AHI Health Home and is assigned to an AHI Health Home Services Provider for care management. Also referred to as a "client" or "member".

Health Home Service Provider: An organization that has a fully executed contract (the "Health Home Services Provider Agreement") with the Adirondack Health Institute to provide health home outreach and/or care management services. Also referred to as "Care Management Agencies (CMAs)".

Electronic Health Record System: A structured information system inclusive of Health Home Participant Personal Identifying Information (PII) and Protected Health Information (PHI), maintained by the Adirondack Health Institute Health Home (AHIHH), and made available for Health Home Service Providers and Health Home Network Partners to utilize, as applicable and appropriate to their role in the Health Home. Also referred to as Netsmart CareManager or Care Management Record System.

NYS DOH: New York State Department of Health

Quality Assurance: QA is a process undertaken by an organization that assures care is maintained at acceptable levels in relation to specifications of standards for service quality and outcomes. QA is a continuous process that assesses organizational performance, both prospectively and retrospectively, including where and why performance is at risk or has failed to meet standards.

Multi-factor authentication: (MFA) Multi-factor authentication is an authentication method in which a computer user's identity is confirmed by successfully presenting two or more pieces of evidence (or factors) to an authentication protocol before access is granted to the Electronic Health Record System.

Personal Identifying Information: (PII) Refers to information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. PII is not attached to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. It is important to recognize that non-PII can become PII whenever additional information is made publicly available - in any medium and from any source - that, when combined with other available information, could be used to identify an individual.

Protected Health Information: (PHI) means individually identifiable information relating to past, present or future physical or mental health or condition of an individual, provision of health care to an individual, or the past, present or future payment for health care provided to an individual.

Background

The Health Home Systems Access and Identity Assurance at AHI is intended to facilitate the effective implementation of security processes necessary to meet the Health Home Program standards and requirements as stipulated by the NYS DOH, federal regulations, and best practices. This policy directs that AHI meet these requirements.

POLICY

It is the policy of AHI Health Home (AHIHH) to protect the confidentiality of Health Home participant information. New York State Law and the Health Insurance Portability and Accountability Act (HIPAA) offer protection of all written and verbal health-related information for individuals who are served by AHIHH. All member information maintained by AHIHH and its partners, including that which is contained in Electronic Health Record Systems, is to be protected in accordance with these laws. Procedures for access to, storage of, and disclosure of health- related information will be followed to ensure compliance with the Mental Hygiene Law, New York State HIV/AIDS Confidentiality Law, and HIPAA laws governing PII and PHI. This policy establishes a trustworthy process, based on national standards, for identity proofing individuals, managing authentication credentials that are tied to an individual's digital identity, and connecting that digital identity to the individual. This standard covers all systems that require authenticated access. This includes all test, quality control, production and other ad hoc systems.

PROCEDURE

All AHI Health Home System users will require a valid and accessible email established through their organization to request access to any and all Health Home Operating Systems/Applications. Each agency must establish an authorized representative a.k.a. Registration Authority (RA) who can attest that the applicant/users identify has been appropriately verified as per New York State Information Technology Standards for Identity Assurance, which is set forth below.

The applicant must provide sufficient evidence to the RA, who must independently verify that the applicant is whom he or she claims to be. The applicant must be uniquely identified, either in-person or remotely, through a managed registration process that includes, at a minimum, the following elements:

For In-person Verification:

Required documentation: Valid current government photo ID containing either address or nationality of record (e.g., driver's license or Passport). Review: RA visually inspects photo ID comparing photo to applicant; and record data for audit purposes including the document type and reviewer. RA reviews personal information in records to support Credential Issuance (in-person) process if records exist.

For Remote Verification:

Required documentation: Submittal of a valid current government ID number or either a financial or utility account number (e.g., checking account, savings account, utility account, loan or credit card or tax ID).
Note: Confirmation of the financial or utility account may require supplemental information from the applicant.
Review: RA verifies that the information provided by applicant including ID number OR account number through record checks either with the applicable agency or institution or through credit bureaus or similar databases, and confirms that: name, DOB, address or other personal information in records are consistent with the application form and sufficient to identify a unique individual. For utility account numbers, confirmation shall be performed by verifying recent account activity. (This technique may also be applied to some financial accounts.)

An authorized representative from each requesting agency will initiate and complete an add/change user form each time there is a new user request or there is a change in the level of access required or when the users access needs to be terminated (see Appendix A). Forms should be submitted to healthhome@ahihealth.org immediately. The Health Home must be notified when there is a change to the RA assigned to the organization.

Quality and Performance Improvement

AHI Health Home will monitor and maintain access documentation and send RA's a user report at least annually. RA's must verify their associated user list and submit the verified users to healthhome@ahihealth.org.

Contact Person: Quality and Performance Improvement Specialist

Responsible Person: Health Home Service Provider, Information Requester

Reviewed By: Director, Care Management and Health Home

Approved By: Chief Compliance Officer

Adirondack Health Institute

Lead Empower Innovate

Appendix A

AHI Health Home Electronic Health Record System Access Form

Please send completed form to healthhome@ahihealth.org

Adirondack Health Institute

Lead Empower Innovate

Add/Change User Form

Requested Action: Choose all that apply			
☐ Add New User	☐ Update Name	☐ Update Role	☐ Deactivate User

Agency Name:	
Agency Address:	
Registration Authority (RA):	
User's First Name:	
User's Last Name:	
User's Date of Birth:	
User's Email Address:	
User's Phone Number:	
What population will they serve?	

Systems Access Request		
☐ Netsmart CareManager	☐ Millin	☐ The Data Den

Requested Security Role (Netsmart only):	
☐ Administrator (Internal AHI only)	☐ Supervisor
☐ Care Manager	☐ HARP Care Manager
☐ Outreach Specialist	☐ Read Only
☐ Other:	

Registration Authority has verified the identity of the requested user as per systems access policy.

Registration Authority Signature:

Registration Authority Phone Number:

Registration Authority E-mail: