ENCOMPASS FAMILY HEALTH HOME
Care Management
Policy & Procedure Manual

Care Management Policy #26 Confidentiality

Effective Date: 3/1/16
Revised Date: 9/1/16

Policy: Encompass Health Home will ensure that all providers of Care Management Services ensure confidentiality and privacy in regard to history, records, and discussions about Participants served. All Participant information maintained by Care Management Agencies, will be will be protected and managed in accordance to New York State laws, Federal Laws and Health Home Standards: New York State's Mental Health Confidentiality statute (section 33.13 of the Mental Hygiene Law); NYS Public Health Law Article 27-F; 42 Code of Federal Regulations Part 2; HIPAA Privacy Rule (45 CFR Parts 160 and 164).

Procedure:

A. All Care Management Agencies (CMA) will enter into a Business Associate Agreement (BAA) with the Health Home, identifying responsibilities of both parties in the use and disclosure of Protected Health Information to perform Health Home/Care Management services.
B. CMA will develop policies and procedures that address responsibility and guidelines to adhering to all confidentiality laws.
    1. CMA will update their policies as changes in laws occur.
    2. All Care Management staff will be trained to, and demonstrate their understanding of confidentially laws and security measures prior to access to any confidential Health Home information or electronic platforms.
    3. Care Management Staff will be re-trained as changes to the law develop, or annually, whichever occurs first.
        i. Documentation of training will be maintained in personnel records.
C. All Health Home Participants/Consenters will sign a Health Home Consent, and will identify those individuals or providers with whom the CMA may communicate and coordinate services with.
    1. Consents will be updated as required to add additional individuals/providers, or to revoke permissions per the Participants/Family's request.
    2. Changes to the Consent Sharing information including the addition or deletion of individuals/providers, will each be initialed and dated by the Participant/Consenter. A review of individuals identified for data sharing will be conducted no less than annually with the Participant, and updated as needed.
    3. If Participant/Consenter chooses to revoke consent from the CMA, but not the Health Home, the consent will be updated by the CMA, to indicate those parties that the Participant has revoked their consent from. The updated consent will be attached to the EHR.
    4. When a Participant/Consenter chooses to revoke consent from the CMA **AND** Health Home, a Health Home Withdrawal of Consent Form will be completed and signed, if possible.
D. All sharing of Participant information will be limited to the minimum amount necessary to support outreach efforts, engagement and the effective coordination of services.
E. CMA will develop and adhere to accepted practices to maintain security of protected information while conducting business under the Health Home. This will include, but is not limited to:
    1. All electronic transmission of protected information will be encrypted.

Care Management Policy #26 Confidentiality

2. All paper disclosures will be accompanied by a statement prohibiting re-disclosure of information.
    i. All disclosures will be documented according to Privacy law standards.
3. All verbal disclosures will be related to the provision of Care Management services, and limited to those who are involved with the Participants care, or are determined to have a need to know.
4. When faxing confidential information, a cover sheet will be used, containing a confidentiality statement.
    i. Fax machines used to send and receive Health Home information will be kept in a secure location.
5. All portable electronic devices utilized by Care Management Staff will be password protected/encrypted for Health Home use.
    i. Portable electronic devices will not be used to store confidential information , unless they are encrypted.
    ii. Missing or stolen devices will be reported to the CMA immediately, and the Health Home informed.
6. All confidential/protected information will be stored on premises in a locked, secure area, and limited to those who require access.
    i. CMAs will determine staff access based on role and necessity.
    ii. CMAs will develop policies and protocols to ensure security and confidentiality, if the need, if any, presents to transport any records outside of the premises.
7. Access to Electronic Health Records (EHR) will be assessed based on role and need to know protocols.
    i. Staff access to Health Home EHR, will be coordinated through the Director of Health Information Systems (DHIS).
    ii. Access passwords issued to Care Management staff will be kept confidential, and not shared with anyone
        a) CMA will notify DHIS immediately if passwords have become compromised.
    iii. Care Management staff will access electronic records in a secure location, and will utilize secure internet connections.
    iv. CMA's will notify the DHIS immediately when roles change, or access is no longer required.
    v. CMA's will maintain a list of Staff, roles and access levels, and will submit to the Health Home upon request.
    vi. Access to other platforms containing confidential information, will be coordinated by the CMA, and use monitored per confidentiality agreements.

F. Violations of privacy, or breaches of confidential Health Home information, will be reported to the Health Home according to BAA contracts, and addressed according to CMA Policies and applicable privacy laws.
    1. Investigations will be conducted, and Participants notified if applicable.

G. Security audits will be conducted by the CMA, and forwarded to the Health Home upon request.