COMPREHENSIVE COMMUNITY SERVICES
POLICY AND PROCEDURES

7.15.2020

SUBJECT: Confidentiality, Security, and Privacy
DHS 36.07 (5) (b)

Purpose

This policy outlines expectations for all Comprehensive Community Services (CCS) personnel (including paid staff, student interns, and volunteers) to maintain and secure confidential information received and generated during the course of completing CCS work.

Policy

For Dane County to be in compliance with laws covering confidentiality of CCS participant records, it is essential that all CCS providers and personnel meet and abide by the expectations outlined in this policy and be in compliance with all applicable laws including s. 51.30, Wis. Stats., 42 CFR Part 2, 45 CFR Part 164, and administrative codes DHS 36, 92, and 94, ethical standards, and professional codes. Failure to meet and abide by the expectations outlined in this policy will lead to review and corrective action, including possible removal from the CCS Provider Network Staff Listing. If a CCS provider believes there is a conflict between this policy and existing confidentiality law, the provider will bring the matter to the attention of the Dane County CCS Administrator in order to provide uniformity and clarity of confidentiality requirements for all program service providers.

Expectations

A. Internal Rules, Policies and Standard Operating Procedures. It is expected that each CCS provider agency will develop a professional culture among its workforce respecting the confidentiality of CCS participant information. Each CCS provider agency will have comprehensive rules, policies and standard operating procedures providing for the security and privacy of confidential CCS participant information, which will include at a minimum the following:

1) Rules and standards of confidentiality will be explained to staff, volunteers and student interns during orientation to all work positions within CCS provider agency.

2) Each CCS provider agency will protect CCS participant information from being disclosed to those who are not authorized to receive it or who do not have a need to know the information.

3) Each CCS provider agency will have policies restricting access to and transfer of CCS participant information within the agency.

4) Each CCS provider agency will set up work stations, printers, and waiting areas in a manner to avoid inadvertent disclosure of CCS participant information.

5) To the extent the CCS provider agency keeps paper CCS participant files, it will keep participant records secured in locked filing cabinets or locked rooms. CCS participant records should be removed from the agency only if absolutely necessary.

6) Each CCS provider agency will have procedures for destruction of CCS participant files in a timeframe consistent with contractual requirements that include sanitizing electronic media on which such records are stored and hard copy media associated with the paper printouts, to render the patient identifying information non-retrievable.

7) Authorizations to Release Information must be filled out fully with the CCS participant controlling the content of the release, including the scope, audience or length of time for which the authorization is valid. Authorizations should be reasonably restrictive but enable the CCS provider to coordinate needed services and comply with program requirements. The CCS participant (and parent/guardian) will be informed that permission to release can be withdrawn at any time, except to the extent that action has already been taken in reliance of the document.

8) CCS service providers shall keep all CCS participant records as required by CCS policies and shred notes and drafts containing confidential information when no longer immediately needed.

9) The CCS provider agency will maintain computer equipment compatible with the Dane County Human Services CCS Program database for participant records and will maintain practices and technology support to protect electronically stored CCS participant information from foreseeable threats of breach. Computer equipment used to access the Dane County network must be running a current operating system and be regularly kept up to date with security updates. Any equipment known to be infected with malware may not access the Dane County network.

10) CCS provider agencies must secure all computer equipment, personal devices, and accounts containing CCS participant information with the use of quality passwords. This includes, but is not limited to, cell phones, tablets, laptops, computers and flash drives.

11) All devices containing CCS participant information, including but not limited to cell phones, tablets, laptops, computers, flash drives must be encrypted. All electronic transmissions of CCS participant information via email or by any other means must be encrypted.

12) CCS provider agencies shall not permit the use of employees' personally-owned devices to transact agency business containing any CCS participant information in a way that could identify a CCS participant and shall not permit downloading of any CCS participant information onto personally owned devices. Therefore, where communication occurs by text messages about a participant, the message may not identify the participant by anything other than initials. The use of unsecured communications is strongly discouraged.

13) Sending CCS participant-specific information via email is allowable only when the email is encrypted and password protected. Any unencrypted e-mail about a participant must not provide information that could identify the participant. Never include a CCS participant's name in the title of the e-mail whether or not the message is encrypted.

14) If video conferencing is permitted in the delivery of CCS participant services containing confidential participant information, the application used must be secure, providing end-to-end encryption.

15) Upon discovering any breach of confidential information or security incident, the CCS provider agency shall first take any immediate steps to mitigate the breach or possibility or extent of any breach. Any security incident or breach of confidential information shall be reported within one business day to the Dane County CCS Administrator who, in consultation with the CCS provider, the Division Administrator and Corporation Counsel will determine appropriate course of action to respond to the breach or security incident.

16) Every CCS provider agency shall designate a Privacy Officer responsible for the development, implementation and enforcement of privacy policies and procedures.

17) Every CCS provider agency shall designate a Security Officer responsible for the development, implementation, and enforcement of security policies and procedures to ensure the integrity of information systems and to prevent unintentional disclosures of protected health information. The Security Officer of each CCS provider agency shall keep an inventory of all devices containing PHI.

18) The CCS provider shall report any discovered violations of this policy to the CCS Administrator, who shall investigate and determine a course of action.

19) The CCS program communicates with agency staff by email. Because of this, it is important that agencies are managing email accounts for staff and that the email communication is encrypted.
    a. Each agency must identify its unique agency email domain to the county.
    b. Each agency staff member who is conducting CCS business by email must do so from their agency email account.
    c. Network Access Request Forms are generated by the CCS Provider Network Coordinator. Network Access Request Forms for staff user accounts must include an agency email address for the individual who you are requesting access for.
    d. Your chosen email system must use TLS encryption for email.

B. The Exchange or Transfer of Participant Information.

1) The Dane County Department of Human Services is the custodian of all records required to be maintained in the CCS Program. Certified CCS provider agencies may keep participant records in agency files that meet the privacy and security requirements stated in Section A and as required under federal HIPAA and Part 2 regulations, provided that the provider agency stores all record information essential to the CCS Program in the DCDHS CCS Program records system. If the CCS provider agency keeps any CCS participant records in-house, it will be responsible for responding to all records requests applicable to those records that are not a part of the DCDHS CCS Program record set and will provide timely notice of any such requests to the department.

2) Because the Dane County Department of Human Services is records custodian of CCS records, all third party records requests for CCS participant records will be routed to the department. CCS Provider agencies may provide participant information or records, with proper authorization, to treatment providers to facilitate the participant's recovery plan. Subpoenas, orders, and requests for records from law enforcement, courts, attorneys and the Social Security Administration must be forwarded to the CSS Administrator for response.

3) CCS personnel shall generate a progress note in the CCS Module any time CCS records are released documenting the date of the release, the participant's name, the specific documents disclosed, to whom they were disclosed, and the purpose of the disclosure. Any Release of Information form on which disclosure is predicated must be included in the CCS participant's centralized record, housed at DCDHS.

4) CCS agencies may exchange participant information with DCDHS and other certified CCS providers on the participant's recovery team without the participant's written consent. CCS agencies must obtain written participant consent to exchange participant information with members of the recovery team who are not certified CCS agencies, including pastors, friends and family members. CCS agencies must obtain written participant consent to exchange information or records with treatment providers who are not a member of the participant's recovery team.

5) Agencies will inform participants at the time services are first received from the agency how the participant's information will be shared within the recovery team.

6) The participant will be informed at the time of admission to the CCS Program and at other times requested a summary of his or her rights under s. 51.30, Wis. Stats., 42 CFR Part 2, 45 CFR Part 164, and administrative codes DHS 36, 92, and 94. A written document is available from DCDHS for that purpose.

7) CCS staff will presume in favor of confidentiality. When there is a question about how the law applies, what these guidelines mean, or the best way to proceed in handling a particular confidentiality issue, staff will consult with the agency's Privacy Officer or the DCDHS CCS Administrator, who may consult with DCDHS Corporation Counsel as needed. If such consultation is not possible, the staff's decision and reasons for confidentiality issues will be documented in the records and reviewed with a supervisor in a timely manner.

Approved by CCS Coordination Committee on July 15, 2020.