



945 20th Street South
St. Petersburg, FL 33712
Office: (727) 822-0443

Date: October 11, 2016

To: Community Health Workers

From: Board of the Mount Zion Human Services and Community Development Corporation and Interim Executive Director

Subject: Community Health Worker Consumer Privacy & Confidential Information Policy

On October 7, 2016, Mount Zion Human Services and Community Development Corporation (MZHSCDC) received preliminary approval to be established as a certified application counselor (“CAC”) organization. Several individuals associated with the CHAMPS program have also attained certification as a certified application counselor (“CAC”).

The job responsibilities, of the individual CACs to assist consumers with health care options and choices, requires and involves obtaining an individual’s Personally Identifiable Information (PII). Examples of PII include, but aren't limited to, an individual's date of birth, place of birth, mother's maiden name, social security number, or income.

This policy will provide guidelines and procedures for obtaining, working with, and the maintaining of an individual’s PII.

Privacy, Confidentiality, and Security

Privacy is a consumer’s right to control how their personal information is used or disclosed.

Confidentiality means respecting any limitation on information access and disclosure according to relevant law and the consumers’ wishes to protect their personal privacy and proprietary information.

Security refers to the safeguards (including systems and physical safeguards) in place to protect the privacy and confidentiality of personal information.

The MZHSCDC CAC organization is committed to keeping consumers’ personal information private, confidential, and secure.

Therefore:

1. Prior to requesting any PII from an individual to assist them with health care options a consent form must be signed by the consumer. The consent form is attached to this policy.
2. A written record of that consent must be maintained for at least six years under 45 Code of Federal Regulations (CFR) §155.210(e)(6)(ii), §155.215(g)(2), and §155.225(f)(2).
3. Prohibited Uses and Disclosures of PII: A CAC cannot collect PII beyond what is necessary to perform authorized functions without consumer consent, or to use PII to

Carl R. Lavender, Jr.
Chairperson

Angela Merck
Operations Manager

discriminate inappropriately against consumers, such as by refusing to assist individual who are older or have significant complex health care needs.

4. PII (consent forms and / or any other relevant health information in a case file) must be kept in a locked cabinet in an office with controlled access.
5. Any PII or relevant health information in a consumers' case file must be kept in a locked trunk when travelling to consumers' locations or health-related facilities when not in the locked office cabinet.
6. In the event any PII is transmitted electronically, the CAC must password protect their device (PC / mobile) and use a secure electronic interface.
7. CACs must ensure that consumers take possession of their documents and mail their own written applications if applicable, a CAC may provide postage or mailing materials.
8. CACs must not leave files or documents containing PII or tax return information unsecured and unattended on desks, printers, personal computers, phones or other electronic devices, and fax machines.
9. CACs must always return originals or copies of official documents that contain a consumer's PII to consumers and only make copies if necessary to carry out required duties.
10. CACs must not send or forward e-mails with PII to personal e-mail accounts (e.g., Yahoo, Gmail).
11. CACs must protect e-mails that contain PII (e.g., encryption).
12. CACs must not upload PII to unauthorized websites (e.g., wikis).
13. CACs must not use unauthorized mobile devices to access PII.
14. CACs must lock up portable devices (e.g., laptops, cell phones).
15. CACs must clear web browser history to avoid other users accessing PII.
16. CACs must disable auto-fill settings on web browsers.
17. For a CAC using Social Media, do not mention any private information, such as consumers' specific names or medical conditions.
18. If a consumer gives a CAC his or her contact information, such as by filling out a contact card, this is considered consent by the consumer for future contact, as long as the consumer was clearly made aware the information might be used for future contact. In this case, follow-up contact with the consumer is permitted; however, the CAC should obtain a complete authorization if and when following up with the consumer in accordance with your organization's standard authorization procedures.
19. PII is only used or disclosed to authorized persons. In the event of a disclosure or situation in which a consumer's PII has been compromised in any way (accidentally or otherwise), the CAC must alert the manager on duty of the unauthorized disclosure to report the incident to CMS as required within one hour of discovery.
20. In the event of a data breach where multiple consumer's PII may have been compromised, the MZHSCDC CAC must file a report to the CMS Information Technology Help Desk at 800.562.1963.

This Policy is to go into effect immediately and full compliance is required. We thank you for your support.

Carl Lavender Jr. - Chairman of the Board of Directors

Joseph Cuenco – Interim Executive Director