Maine Center for Disease Control and Prevention
WIC Nutrition Program

Effective: October 1, 2011 Policy No. IS-04
Revised: August 1, 2016

Data Security

Authority

42 U.S.C. §1320 (d)(1)-(d)(8) - Health Information Portability and Accountability Act of 1996 (Public Law 104-91) (HIPAA)
Maine CDC Administrative Policy CDC-P3
Maine DHHS OIT Policy to Safeguard Information on Portable Computer and Storage Devices (Section 1)
Maine DHHS Policy Concerning the Use of State Automation Equipment (Section IV, E, 9)

Policy

1. Acting as a "covered entity" under HIPAA provisions, all data collected and stored by the Maine CDC WIC Nutrition program shall be classified according to the Maine CDC classification scheme of restricted and unrestricted data.
2. The Maine CDC WIC Nutrition program shall participate in the ME CDC's agency-wide *Data Inventory* (Appendix IS-4-A) and *Data Use Plan* (Appendix IS-4-B) to assure appropriate management and confidentiality of the data, and to assure that all users maintain the integrity of program data.
3. A single designated individual within each Local Agency and at the State Agency level shall manage all release of both restricted and unrestricted data. This person should receive, review, respond and track each data request.
4. All data releases should be checked and verified by two qualified staff persons (i.e. a staff person who is familiar with the program's data and has received both basic and more detailed training on this policy) prior to their release to ensure data confidentiality.
5. In the event of a public health emergency, where specific information is vital for public safety, release of confidential information shall be at the discretion of the Maine CDC Privacy Officer.

Procedure

1. Annually, the Maine CDC WIC Nutrition Program shall fill out the Maine CDC's Data Use Plan (Appendix IS-4-B) to document the names of programs sharing data, types of data shared, frequency of use, and purpose of use.

2. The Data Plan shall incorporate all data used that is collected and stored in other programs, including data used for program planning and evaluation, epidemiology, case investigation, emergency response, and management/administration.

3. Once established, restricted data shall only be released to appropriate internal users as defined by the current Data Use Plan.

4. Once included in the Data Use Plan, programs may share restricted data on an ongoing basis without additional approval.

5. As new areas for data sharing are identified, the Maine CDC WIC Program shall submit a written request to the program of interest on the Application for Release of Unrestricted Data form (Appendix IS-4-C).

6. The Data Plan shall be overseen by the office of the Maine CDC Privacy Officer, with assistance from the Maine CDC Data Committee. Program and Division Directors shall facilitate data-sharing requests, with assistance from the Privacy Officer as appropriate.

7. The Maine CDC Data Inventory shall catalogue all data collected by Maine CDC programs. Maine CDC WIC shall complete a Maine CDC Data Inventory form (Appendix IS-4-A) annually for all data sources collected by the program, whether paper or electronic.

    7.1 For each data source, the inventory shall summarize the nature of the data (e.g. surveillance, service data, etc.), how it is stored, description of the data collected, and type of routine summary reports that are available.

    7.2 The Data Inventory shall be overseen by the office of the Privacy Officer, with assistance from the Maine CDC Data Committee.

8. To reduce the risk of breaching confidentiality, the following guidelines shall be implemented when releasing data:

    8.1 County level data shall be released, regardless of the numerator cell size, if the underlying population of the cell is 5,000 or greater. ("Underlying population" refers to the total subpopulation described by the data, i.e. 15-24 year-old males.)

    8.2 County level data with cell sizes of 5 or fewer shall be suppressed if the underlying population of the cell is less than 5,000.

    8.3 For geographic areas smaller than the county, regardless of the underlying population size, cell sizes of 5 or fewer shall be suppressed

    8.4 When releasing data that include small cell sizes, Maine CDC WIC Program shall use the methods of aggregation and suppression to maintain confidentiality:

8.4.1 Aggregating data is the primary method used to collapse a dataset in order to create tables with no small numbers as denominators or numerators in cells. Aggregation of data values is appropriate for fields with large numbers of values, such as dates, diagnoses, and geographic areas.

8.4.2 Suppression: When it is not possible or desirable to create a table where all cell sizes are greater than 5, cell suppression is used. Suppressed data shall be reflected in tables as "five or fewer", "<5", "fewer than 6" or "<6." The method of "primary cell suppression" is used to withhold the numerator in the cell that does not meet the threshold. In the event that one cell is too small, two other "complementary" cells also need to be suppressed, including the next-larger cell and the total. This rule applies to both rows and columns whenever totals are presented. Complementary cell suppression must be completed in order to avoid inadvertent disclosure through back-calculation.

Storage of Restricted Data

9. At a minimum, written records and paper files containing restricted client data shall be stored in locked file cabinets.

   9.1 As is practical, office spaces should be locked and alarmed when unoccupied.

   9.2 If more than one person has access to written data and paper files, a single staff person shall be designated as responsible for "signing out" restricted records used by other staff. This individual shall be notified by other staff whenever confidential files are removed from their locked storage area. This designee shall track files through a written checklist or tally.

   9.3 If an entire program requires access to paper files with restricted data, staff shall be individually responsible for returning records to file cabinets or temporarily storing records or any material with restricted data in a locked storage area when office hours are concluded.

10. Data should be transported off-site only when absolutely necessary. When possible, data should be transported in locked briefcases or lockable file carriers.

11. Written records determined to be non-essential by program staff (e.g. records entered into a computer database, phone messages, computer-generated line lists) shall be shredded after use.

12. At minimum, electronic records containing restricted client data shall be stored either on removable computer devices, (which are then treated in the same way as written records) or on password-protected computers stored in locked and alarmed offices.

13. Data should be encrypted using 128-bit or higher encryption software, with access limited to those working directly with the data.

14. For shared computer programs on a LAN, data files shall be password protected, with user rights limited to those staff who work directly to collect, enter or analyze these data. LAN backup tapes shall be treated in the same way as written data.

15. Restricted data on portable devices should be safeguarded by properly classifying data, using encryption to prevent unauthorized access, and requiring written authority to copy data, as outlined in the Office of Information Technology (OIT) Policy to Safeguard Information on Portable Computer and Storage Devices (Section I). Examples of portable computer and storage devices include laptops, pocket personal computers, Blackberries, hand-held devices (PDAs), USB thumb drives, cell phones etc.

16. When practicable, data stored on a portable device (such as an encrypted USB drive) should be copies of data stored on a secure state network drive; the user assumes the responsibility for any original data stored on a portable, encrypted device when the device itself or password is lost.

17. When replacing computer hardware, any equipment used for storing restricted electronic records must be thoroughly purged of data before being removed from program offices. Purges must be conducted by qualified OIT staff who ensures data is "unrecoverable."

18. Removable storage devices no longer used to store restricted data must be either purged or destroyed by qualified OIT staff.

19. Program Managers must inform OIT staff when any equipment being replaced had been used to store restricted electronic data. The OIT staff for each division is responsible for ensuring that purges are completed as appropriate.

Transmission of Restricted Data

20. If possible and feasible, all non-essential identifiers shall be removed when transmitting restricted data by U.S. mail, private mail carriers, facsimile or electronic mail.

21. All restricted data sent through U.S., private mail carriers, or interoffice mail shall be placed in envelopes stamped "Confidential."

22. Restricted data transported between staff offices shall be placed in envelopes marked "Confidential."

23. All incoming restricted data shall be dated and appropriately distributed to program staff. At the end of each day, all materials with restricted data must be appropriately stored.

24. Restricted public health data that are transmitted electronically should be:

    24.1 Limited to those situations that require immediate receipt of the data; and

    24.2 Must be safeguarded against interception or access by persons who do not have clearance to view or use them.

25. Use of email and cell phones to transmit/discuss restricted data is allowed only under limited circumstances. Pursuant to the DHHS Policy Concerning Use of State Automation

Equipment (Section IV, A): "Non-encrypted cell phones and unsecured/non-encrypted Internet connections must not be used to discuss or disclose confidential or personal/protected health information (such as HIV status, substance abuse/treatment, mental health condition(s), etc.)."

25.1 Maine CDC-issued cell phones are encrypted.

25.2 Restricted data may be discussed using encrypted cell phones when necessary to perform required job duties, and the person utilizing the encrypted cell phone has made a reasonable effort to conduct the phone call in a private setting where restricted information cannot be overheard.

26. Restricted data may be emailed only between Maine CDC WIC employees in password-protected documents and when the password has been conveyed to the receiver by other means.

26.1 Pursuant to Section IV, E of the DHHS Policy Concerning the Use of State Automation Equipment, all email messages containing password-protected restricted data must have a label placed in the subject line that reads: "Confidential Information Enclosed."

26.2 When electronically transmitting restricted data, senders must ensure that a correct, updated email address or fax number is used.

26.3 The sender must also verify that the data were received by obtaining from the receiver a voice, email or fax confirmation.

26.4 If the data were not received, the sender must work with the State's Office of Information Technology (OIT) staff to determine the destination of the data and retrieve them if possible.

27. Fax machines used to transmit restricted data should be located in low traffic areas or secured locations, such as a locked room.

27.1 The sending or receiving of faxes containing restricted information must be coordinated with the sender/receiver so that each is handled in a timely manner with little or no opportunity for other persons to view these data.

27.2 Fax machines not located in a locked room should be disabled from printing when office hours are concluded.

<u>Confidentiality Notice</u>

28. Because of the potential for unintended receipt, all restricted data transmitted by fax or email shall contain the following confidentiality notice:

28.1 "Confidentiality Notice: This email message, including any attachments, is for the sole use of the intended recipient(s) and may contain confidential and privileged information. If you are not the intended recipient, or an authorized agent of the intended recipient, please immediately contact the sender by reply email or fax

and destroy/delete all copies of the original message. Any unauthorized review, use, copying, disclosure, or distribution by other than the intended recipient or authorized agent is prohibited."

28.2 This Notice must be placed at the bottom of a fax cover page, or as an e-mail footer.

Remote Access to Restricted Data:

29. Maine CDC WIC employees, including non-state contracted workers employed within Maine CDC WIC Nutrition programs and supervised by WIC staff, with access to restricted data may only access restricted data (via saved files or other applications) when working remotely in the following circumstances:

29.1 It is necessary to access the restricted data in that time and setting, and;

29.2 The employee is using a state-issued laptop computer.

29.3 If an employee uses a personal computer that is not provided by the Department, for State business purposes, the PC must have installed and operating the current version of the State-approved anti-virus product and the personal computer must not be used to access, download or store PHI or confidential information.

Work-site Security

30. Restricted data and protected health information must not be discussed in public areas.

31. Program staff shall be individually responsible for protecting their own work station. This responsibility includes protecting keys, passwords, and codes that would allow access to restricted information.

32. Visitors to Maine CDC WIC Nutrition offices must be accompanied at all times after being admitted to the office space.

33. If non-staff persons enter a work area containing restricted information, such data shall be immediately removed from view (e.g. clearing computer screens, placing documents in desk drawers). As appropriate, non-staff visitors should be escorted out of areas containing restricted data, and assisted in locating appropriate program staff or offices.

34. All file cabinets containing confidential records are to be locked when not in use. Staff shall be responsible for double-checking that file cabinets are locked within their workspace before leaving the office each day.

35. When staff are not present in offices for short periods (less than 30 minutes), databases containing restricted data must be closed so they will require use of a password to reopen. In addition, all confidential data shall be turned face-down on desks and office surfaces. When staff depart for periods of 30 minutes or more, all confidential records shall be returned to their locked storage location.

36. Staff-members who utilize restricted data throughout the workday shall be located in low-traffic areas and shall appropriately store materials with restricted data when away from the workstation for 30 minutes or more.

37. All restricted data shall be placed in a locked storage location when office hours are concluded.