

O. MANAGEMENT INFORMATION SYSTEM

In this section

This section contains the following topics:

Topic	See Page
O.1. Required Reports	2
O.2. Computer System Security	4

Utah WIC Policy and Procedures Manual

Section O: Computer Reports

O.1. Required Reports

Policy: Required Reports

Procedure

Listed below are all of the reports required to be run or researched by local WIC clinics as well as how often each report should be run. Please refer to the VISION reports menu for a complete listing of reports available within the system. Refer to the Reports tab on SharePoint to access any ad hoc reports that have been created or to request additional ad hoc reports.

Report Name	Frequency	Purpose
Voided FIs that have been Redeemed or Rejected	Monthly	Sent by State office to clinic staff along with copies of checks voided as lost that were redeemed. Clinic staff must research this report to find participant violations and resolve clinic errors. Refer to Section E.11 for instructions.
Intrastate Dual Participation	Each morning	Compares participant names and birthdates with other participants in the system to find potential dual participants. Refer to Section G.8 for detailed procedures
Check Stock Inventory and Adjustments	Monthly	This is not a report, but is a process that must be checked and completed monthly in order for VISION to report accurate estimates of blank check stock inventory to the State Office. Refer to Section E.2 for instructions.

- I. Some required reports require that research be done at the clinic level to resolve errors and findings on the report. Follow instructions to conduct research on reports and consult with the Help Desk as needed to correct any problems that cannot be corrected at clinic level.
- II. When using the computer system to document appropriate information:
 - a. Be concise and to the point.
 - b. Comments should be understandable to others
 - c. Do not delete relevant comments.

Utah WIC Policy and Procedures Manual

Section O: Computer Reports

- III. Most reports within VISION and the ad hoc reports that have been created are used for local and State Agency information and evaluations. These reports can be run as needed.

O.2. Computer System Security

Policy: Computer System Security and Training

Computer hardware and software must be protected from misuse. Data integrity must be monitored and guarded against data theft, loss, and errors. Computer users must be trained on system use and security. Local agencies must coordinate with the State WIC Help Desk/DTS staff and county/local health department IT departments in providing for the security and training on the Management Information System (MIS) and computer hardware.

Procedure:

- I. Local agencies should require each end user to sign an Acceptable Use Policy form. (This is commonly required by and coordinated with the County/Health Department IT Department)
- II. At least every two years each local agency should conduct training on computer security which covers the following topics:
 - a. Computer access
 - b. Appropriate internet use
 - c. Protecting confidential participant information
- III. Staff must be trained on the **VISION** system.
- IV. Clinic directors should fill out the Security Access form, available on SharePoint, for requesting changes to security access for employees. This includes new employees and terminating access for former employees. A copy of the form should be submitted to the WIC Help Desk for the access to be updated.
- V. Staff should monitor the use of the computer system to prevent loss of data due to theft, errors, and misuse.
- VI. Issues and errors with the computer information system and computer hardware should promptly be reported to the WIC Help Desk.
- VII. Users must sign off/log off terminals when leaving the computer workstation. Each individual staff using the terminal must log in with their own security information; multiple users cannot utilize the same log in.
- VIII. Software unrelated to WIC, clinic operations or local health department business should not be loaded onto WIC owned machines.

Utah WIC Policy and Procedures Manual

Section O: Computer Reports

- IX. Computer hardware should be kept in a secure environment during clinic hours; portable equipment not in use must be locked in a secure location to avoid theft.

- X. Clinic staff should never change/alter or tamper with the computer's system calendar. The date and time shown in the Windows task bar of the computer (bottom right corner) must be accurate with the current date and time. Changing the system date in the computer causes serious data issues and errors with VISION. Staff altering the system date to attempt to correct issues may be unintentionally committing fraud. Avoid using this as a calendar to prevent accidental changing of the system date.