330.10
Local WIC Agency Data System Guidelines

Overview

Introduction
Local WIC agencies must have safeguards in place to assure that participant information, food instruments, and equipment are secure. A local WIC agency data system security plan should be in place and reviewed each year. Appropriate changes should be made to the plan as needed.

Focus
Local WIC agencies are required to use and document clinic services and program benefits in the Focus data system. The applicant may not substitute any other data system for the Iowa WIC Program. Local WIC agencies are expected to establish routine procedures to assure the security and quality of electronic records, food instruments and data reports. Data system equipment and software, including operating, application, and security software, will be subject to security audits by the State. Local agencies must submit monthly verification of compliance of software (operating, application and security), security updates, monthly Focus inventory reports, and any other information requested by the IDPH. State WIC office staff will also conduct data system reviews on a regular basis.

Local Agency Computer Support
Local agencies are required to provide local agency computer support and maintenance of local hardware and operating software, including operating, application, and security software. This includes providing patches and updates to computers and software, including operating application, and security software, and troubleshooting any local issues. This may be agency staff or a contract with a local computer company.

Theft or Damage
Theft or damage of data system equipment should be reported to the state office immediately. Computers/devices supplied by a local agency, or other third party entity, shall be wiped using a DoD approved process when no longer used with the Focus application.

In This Policy
This policy contains the following sections.

Clinic Safeguards

Physical Site Check
Local agency staff should periodically review their physical locations to determine if equipment or food instrument stock is in any potential danger. Review area for:

- Windows or doors that may be left open that could lead to theft opportunities or damage by weather,
- Windows or doors that leave equipment or records in full view, and
- Exposed water pipes or drain areas that could leak on equipment or materials.

WIC Data System Equipment
The following safeguards must be in place:

- WIC data system equipment is not to be used for personal use,
- Do not open or download personal files and visit only work-related websites. Visiting certain websites and/or downloading certain files can contain viruses that can harm the computer,
- Computers are locked in a cabinet or in a limited access area when not in use,
- When traveling to satellite clinics, laptops and printers should not remain in an unattended vehicle overnight,
- To protect against electrical spikes and to keep systems from shutting down prematurely, surge protectors or uninterrupted power supply units should be used,
- When transporting equipment, laptops and printers should be carried in appropriate bags or containers,
- Quarterly cleaning of equipment, and
- Practice good housekeeping with data system equipment. Encourage regular use of canned compressed gas on keyboards, printers, and intake/exhaust ports.

Food Instruments
Local WIC agency staff must assure that theft or destruction has not occurred to food instruments. This includes:

- Storing all food instrument in a secure or limited access area during non-distribution, and
- Securing all food instrument stock out-of-sight and out-of-reach of participants. Staff must secure all food instruments if a clinic is left unattended and staff is not present (example: lunchtime).

Participant Records
All WIC participant information must remain confidential. This includes:

- Not displaying electronic participant records on the screen while the computer is unattended;
- Shredding WIC participant information that is no longer needed; and
- Not allowing non-WIC staff to have access to the WIC data system.

Security Access/Two Factor Authentication

Policy
Local and state WIC staff must use the two factor authentication to access Focus.

Access Levels
To assure program and data integrity of the WIC data system, there are multiple levels of security access. Data system security access is determined by position and clinic responsibilities. Access levels include:

- WIC Coordinator,
- CPA,
- CPA Admin,
- Non-CPA Professional,
- Support Staff,
- Support Staff Admin,
- Scheduler-only,
- Breastfeeding Peer Counselor,
- LA Reports Only,
- View Only

Two-Factor Authentication Requests
WIC coordinators must email a signed New User Request Form to the WIC HelpDesk (WICHD@idph.iowa.gov) when new staff is hired. After these documents are received and after the new employee completes data system training, the WIC HelpDesk will mail the WIC Coordinator instructions on the new user's user ID, password, two-factor authentication QR code, secret key code, and instructions on how to use the two-factor authentication.

Note: Only WIC personnel (as funded by WIC grant funds) are allowed access to the electronic WIC data system, including the rights to "read" and "edit" records.

Using Two-Factor Authentication
Instructions on how to use the two-factor authentication process will be provided via the WIC HelpDesk.

Two-factor authentication can be used on a Smartphone and/or computer. Each user should keep their two-factor authentication QR code and secret key confidential and in a secure location. This information must be available if the user will be using a new Smartphone or computer.

Passwords
Strong passwords shall be used with all computers/devices. Passwords should be kept in a secure area and should not be shared. Local agencies must report any breach of password of security.

Security Access/Two-Factor Authentication, Continued

within 24 hours to the state WIC office.

Inactivate User
Upon the resignation of local agency staff, the WIC coordinator or lead WIC staff must **immediately** complete and submit an Inactivate User Request Form to the state WIC HelpDesk. If a staff member leaves the agency and then returns at a later date, a New User Request Form must be completed.

Changes
If WIC staff have a change of name or change of Focus rights, the WIC coordinator or lead WIC staff must complete and mail or fax the User Change Request Form to the state WIC office.

Location of Forms
Focus forms are found on the WIC Web Portal.

Data System Hardware, Software, and Internet Connectivity Requirements

Data system equipment and software, including operating, application, and security software will be subject to security audits by the state.

The local agency must submit monthly verification of compliance of software (operating, application, and security), security updates, monthly Focus inventory reports, and any other information requested by IDPH.

Hardware
The following are agency hardware requirements:

- Minimum: Processor - I3 3.4GHz or greater – 64 bit dual core, 4GB of RAM, 128GB Hard drive.
- Recommended: Processor - I5 2.4GHz or greater - 64 bit dual core, 8 GB of RAM or greater, 256 GB hard drive or greater.

Windows Operating System
Local agencies must have the minimum:
Windows 10 service pack and current updates.

Software
IDPH approved security software is required for all data system equipment running the Focus suite of applications. The Office of the Chief Information Officer's website provides security information and can be found here: https://ocio.iowa.gov/standards.

The following are software requirements:

- Anti-virus software
- Latest version of Adobe Reader and Internet Explorer 8.0 or higher, and must have TLS 1.1 and 1.2 at a minimum via the browser.
- Microsoft .NET Framework 4.8.1 or higher with the latest patches.
- Department approved security software is required for all data system equipment running the Focus suite of applications.

E-mail
All agency executive directors, WIC Program coordinators, and lead staff in a split agency must have **individual** email addresses with the capacity to send and receive electronic communications (e-mail and attachments).

All agency staff using Focus must have the ability to use local agency email to contact the WIC state office. This can be a group of individual email addresses.

Data System Hardware, Software, and Internet Connectivity Requirements, Continued

Internet Access
All WIC offices (including split offices within an agency) must maintain high-speed Internet access meeting the following requirements:

- Minimum: Bandwidth 1.5 mb
- Recommended: 12mb Cable modem, 7 mg DSL modem, cellular (1.5mb or higher, or 4G (cellular)).

Google ~~Drive~~
Contractors must be able to access Google Drive and Google Hangouts.

Data System Equipment
The local agency is responsible for providing their own data system equipment, including laptops, desktops, printers/scanners, signature pads, card readers, and PIN Pads (PIN Pads optional). See Policy 330.20 for more information on data system supplies.

Local agencies must ensure all equipment is functioning properly.

Local Computer Support
Local agencies are required to provide local agency computer support and maintenance of local hardware and operating software, including operating, application, and security software. This includes providing patches and updates whenever they are made available to computers and software, including operating application, and security software, and troubleshooting any local issues. This may be agency staff or a contract with a local computer company.

Local Agency Security Plan

Local Agency Security Plan
A local agency security plan must include:

- Measures for securing equipment, food instruments, and electronic participant records;
- Assurances that staff are using the two-factor authentication to access Focus;
- Assurances that WIC participant information remain confidential;
- A record of emergency preparedness procedures related to the data system; and
- A physical site checklist related to the present clinic sites.

Personnel Practices
At the beginning of employment, coordinators must discuss confidentiality of records and safeguarding of equipment with staff. A signed Statement of Confidentiality is required at the time of hire.

If an employee is dismissed, they should have no further access to participant records or agency equipment. The WIC coordinator must submit an Inactivate User Request Form to the WIC HelpDesk. Coordinators are encouraged to maintain a record of accesses given to employees.

This page intentionally left blank.