Local WIC Agency Data Processing

All contract agencies shall comply with the instructions outlined in the Iowa WIC Policy and Procedure Manual for use of the automated data processing system in provision of WIC food instruments and monitoring of WIC services. No contract agency is exempted from adherence to any portion of these instructions.

Authority

IAC 641—73.20(135)

Procedures

I. Local and State WIC Staff access to 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 <mark>Iowa Department of Health and Human Services</mark>. State WIC office staff will also conduct data system reviews on a regular basis.

    A.　WIC coordinators must email a signed New User Request Form and WIC User Information Form to the WIC HelpDesk (WICHD@idph.iowa.gov) when new staff is hired. Focus forms are found on the WIC Web Portal

    B.　To assure program and data integrity of the WIC data system, each user will be assigned the appropriate level of access as 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

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.

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

   a. Two-Factor Authentication Requests: 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 ID, password, two-factor authentication QR code, secret key code, and instructions on how to use the two-factor authentication

   b. 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 made available if the user will be using a new Smartphone or computer.

D. 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.

E. 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. Focus forms are found on the WIC Web Portal

II. 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 the Iowa Department of Health and Human Services. The Contractor and their subcontractors shall comply with the security requirements specified in the contract with the Iowa Department of Health and Human Services, USDA and Agency policies and procedures to protect client confidentiality and assure security of the client information, including electronic files. The State of Iowa Office of the Chief Information Officer (OCIO)'s security standards can be found here: https://ocio.iowa.gov/standards.

A. 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.

B. Software- Local agencies must have the minimum:
   - Iowa Department of Health and Human Services approved security software is required for all data system equipment running the Focus suite of applications.
   - Windows Operating System Windows 10 service pack and current updates.
   - 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.
- Email – All local agency staff and all subcontractors and contracted staff must have a business email address. Personnel email addresses shall not be used.
- Contractors must be able to utilize the Department's file sharing platform.

C. 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)).

D. Cell phones
- Smartphone with a data plan

III. Data System Equipment.
The local agency is responsible for providing their own data system equipment, including laptops, desktops, printers/scanners, signature pads, and card readers. Local agencies must ensure all equipment is functioning properly.

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.

IV. Focus Security Compliance and Inventory Report
Contractors must submit required verification of compliance software (operating, application, and security), security updates, required Focus Security Compliance and Inventory Report, and any other information requested by the Iowa Department of Health and Human Services. The required Focus Security Compliance and Inventory Report should be from the Contractor's approved security software and must be documented at the individual computer level

V. Local Computer and Technical 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.

VI. Local Agency Security Plan
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.

A. All local agencies are required to have a security plan in place. A 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.
B. 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.
   - 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
C. 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.
D. 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).
E. 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).
F. All WIC participant information must remain confidential (See Policy "Confidentiality of Participant Information". 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.

Best Practices

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