3.11 System Administration

The System Administration functional area is intended to contribute to the overall flexibility, efficiency, and security required for operating and maintaining the system. Depending on the architecture of the system, system administration functions may vary. This section represents a base level of functions used to support system administration activities.

This functional area provides the capabilities to maintain information contained in system data (reference) tables, to control general access to the system as well as the ability to perform specific functions, to perform system "housekeeping" and maintenance functions, and to move certain files to off-line storage for increased system efficiency. Additionally, this functional area includes reports that are relevant to monitoring system operation and performance.

System Administration is made up of the following functions:

- Maintain System Data Tables
  - Maintain System Code Table Data
- Administer System Security
  - Locate User Record
  - Maintain User Identification
  - Maintain User Capabilities
  - Monitor Unauthorized Access
  - Monitor Record Updates
- Manage System
  - Perform System Back-Up/Restoration
  - Import/Export Data Files
  - Provide Version Control
- Archive System Data
  - Archive and Restore Historical Data
  - Purge Unnecessary Data

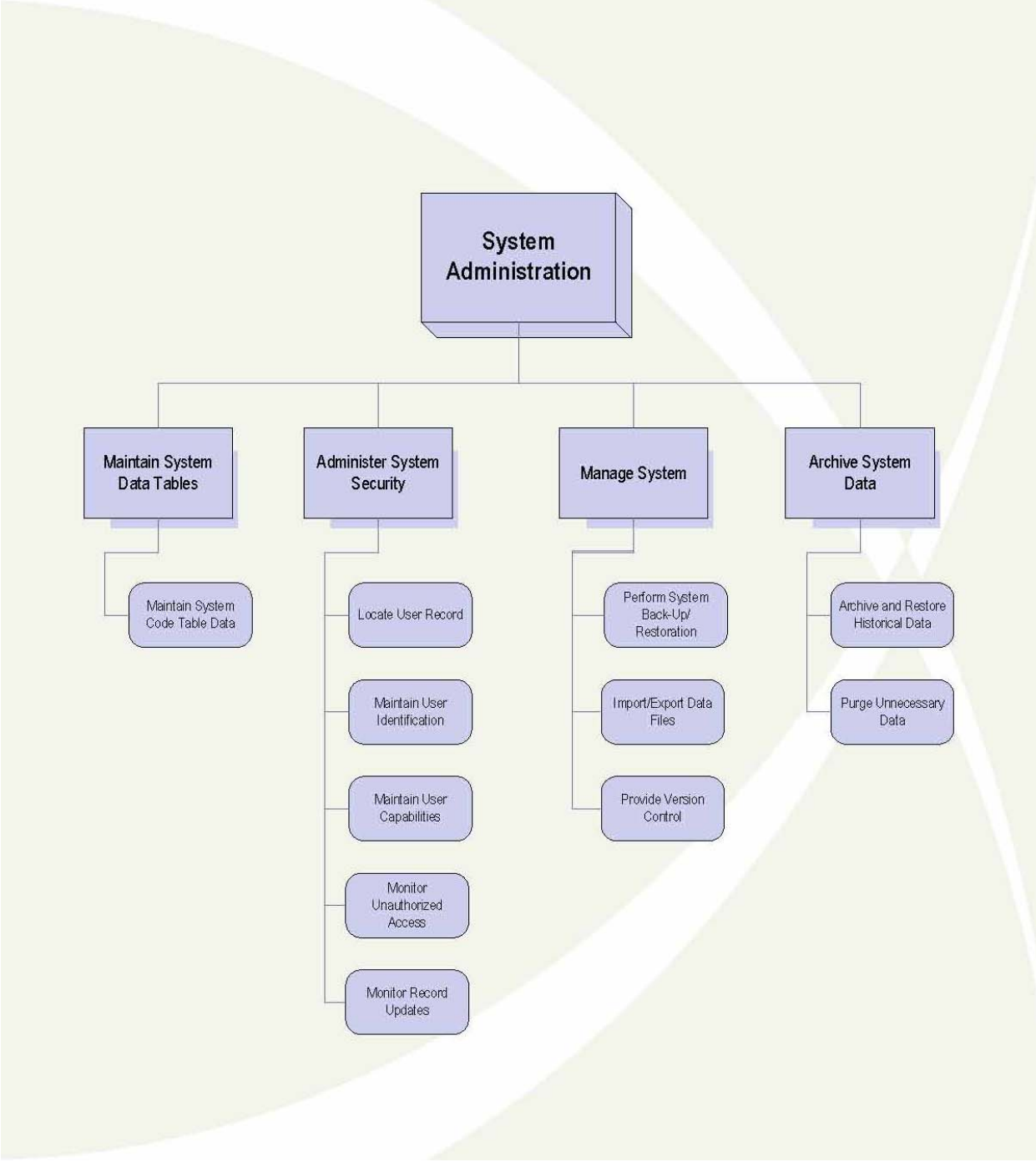

Exhibit 3-11: Functional Decomposition Diagram – System Administration

3.11.1 Maintain System Data Tables

State must have the flexibility to adapt to periodic changes in food packages, nutrition measurement, vendor risk, and other elements of the WIC Program. In an automated system, many of these data elements are stored in data code tables used for data validation and other internal system processes. For the sake of efficiency, many of these data elements are stored as one- or two-digit codes. Each code typically has a full text translation. These codes and accompanying text are established by the State agency. Data elements contained in data code tables could be shared with one or more data stores.

This data code approach to maintaining information becomes useful for entering data entered into the system. For example, when a participant's racial or ethnic origin is recorded during enrollment processing, the racial/ethnic code entered into the system is compared to the legitimate codes contained in the Racial/Ethnic Code data code table. If the code is located in the table, the information is accepted and stored by the system. If, however, the code does not exist in the table, the system returns an error message to the user.

The ability to maintain the system's data code tables is critical to allow the system to easily adapt to changes in the WIC Program. The information in these tables must be current and accurate to ensure the accuracy of the data validation processes that take place in the system. Incomplete or erroneous data in the data tables may permit the entry of invalid data, or prevent the entry of legitimate information.

The system must allow authorized users to review and update the data contained in the system data code tables. It is recommended that the update of data code table elements occur in a real-time mode so that changes can be accessed by the data validation process immediately. This implies that data code tables are shared outside the application programs. However, some tables (e.g., tables unique to a single process) could be hard coded within programs. While this is a design issue, it is important to note it in this discussion.

The suggested data code tables for an automated State system and their definitions are listed in *Section 4.2: Data Tables*.

3.11.1.1 Maintain System Code Table Data

The system should support this function by allowing authorized users to add, delete, or change data elements in the defined tables via the application (i.e., screen).

Inputs:

The system should allow addition, deletion, or update of any unrestricted data element contained in the data code table. Most data code tables consist of a code and a description of the data that each code represents. The individual data elements for each of the suggested data tables are contained in *Section 4.2, Data Tables*.

Process:

- Edit new and updated data elements
- Store edited data in appropriate data code table

Outputs:

Screen display and report of data code table

Implementation Approaches

- When values may change regularly (such as income guidelines), data tables could be easily updateable by non-technical users. If drop down lists are used, authorized non-technical staff should be able to update the values as needed.
- Non-programming users must not be allowed to change any of the characteristics of the data elements, such as field length or field type, through this function. Those types of changes necessitate programming modifications by programming staff (e.g., IT resources or contractor programming engineers).

3.11.2 Administer System Security

Federal regulations require that only authorized individuals have access to WIC information. Access to sensitive health and income information must be limited to those individuals at State and local agencies that require such information to serve WIC participants and administer the Program. The issuance of food benefits is another sensitive area that requires tighter controls than most other management information or participant processing functions. The various controls placed on access to the system in general and these areas in particular, constitute a large part of system security.

Administering system security is important because it protects the access to information in the system. System security prevents unauthorized individuals from entering or updating WIC information. It also provides a means of ensuring that only those individuals that have been adequately trained in system operations can access any of the system's functions. Finally, accurate identification of the users enables the system to create a complete audit trail of all transactions in the system.

In general, the system should support standard security features such as system generated user codes, passwords, timed logouts, and access lockout after a given number of unsuccessful system access attempts. The system must be able to distinguish between those capabilities that can be performed by a State agency user and those that can be performed by a local agency user. For example, enrollment processing is usually performed at the local level, while food management is primarily the domain of the State agency. In this specific function, the WIC IS should allow authorized users to add, delete, or update user access and identification information in the system.

Optimally, the system should provide the ability to record and control the specific capabilities of each user at a level defined by the State agency. State and local agencies might also want the capability to record and review attempts at unauthorized access to the system.

3.11.2.1 Locate User Record

> *After a record is created or to determine if a data record exists in the system, staff members have to have the ability to locate the record for viewing or data entry.*

The system should have the capability to search for user records using predefined criteria.

Inputs:

Data elements included in a search function will vary based on design and State agency preferences. See Implementation approaches for examples.

Process:

- Compare data search criteria with existing database records
- Display records that match search criteria
- Allow user to access the data record(s) matching search criteria

Outputs:

Screen display of matching records

Screen display of selected record

Implementation Approaches

- Various data elements could be included in the search, such as identification number, name, user type (e.g., clerk, super user), or local agency.

3.11.2.2 Maintain User Identification

The system should allow authorized users (usually the system administrator) at the State agency level to add, delete, or update users in the system. When a new user is entered, the system should assign a User Identification that uniquely identifies the user.

Inputs:

User Identification End Date

User Identification Number

User Identification Start Date

User Name

User Organization Supervisor

User Password (Encrypted)

User Social Security Number

User Supervisor Telephone Number

User Telephone Number

User Title/Role

Process:

- Create User Identification (if not entered)
- Store edited user data in the User data store

Outputs:

User ID confirmation notice

Screen display of all users

Implementation Approaches

- Users could be assigned to specific local agencies/clinics or to statewide access.
- The system could produce a notice to be sent to the user, which provides the new User ID and a temporary password to gain initial entry into the system. The user could be required to change their temporary password upon initial login.

- Users could be required to change their passwords on a regular basis (30 to 60 day intervals are suggested). The system should prompt users to change their passwords 7 to 14 days in advance of password expiration.
- The system could maintain a list of the last few (10 to 12) used passwords so that the user cannot select a password that they recently used.
- The system could require strong passwords (combinations of letters, numbers, and special characters).
- In the future, advanced technologies may be used to more securely verify a user's identity before access is granted to the system. Such technologies may include the use of an integrated circuit chip (smart card) to maintain a user's password or a digital certificate. When a user logs onto the system, the security application may read the smart card and retrieve either a password or a digital certificate for verification. The identity of the cardholder could then be verified prior to granting access to the system. This technology would operate similarly to the use of passwords.

3.11.2.3 Maintain User Capabilities

The system should control access to specific functions within the system. Access to these functions should be controlled for each user by indicating which functions the user is authorized to perform. For example, a clerk may be allowed to enter eligibility data, but not allowed to assign risk codes.

The system should enable authorized users (e.g., System Administrator) to update these indicators for each user. The system should provide a display screen that identifies the authorized capabilities, and print a listing with the names of all users at a site authorized to perform a specific function.

Inputs:

User Access Function Code

User Access Function Privilege

User Identification Number

Process:

- Accept user-entered user access function and function privileges
- Validate User Identification and capability data
- Store or update capability data in the User Access data store

Outputs:

User capability profile

Audit file

Implementation Approaches

- The system could have a series of roles that are comprised of various functions or access rights. Users could be assigned to applicable roles based on their function in WIC.
- Users could be set up with differing access rights depending on which clinic data set they are accessing (if the State separates data set access by clinic). For example, a CPA may have one set of access rights at Clinic A and another set of rights at Clinic B.

3.11.2.4 Monitor Unauthorized Access

The system should monitor attempts to access the system. Unsuccessful attempts should be logged for follow-up, if necessary.

Inputs:

Unauthorized Access Date

Unauthorized Access Function Code

Unauthorized Access Terminal Identification Number/IP Address

Unauthorized Access Time

User Identification Number

Process:

- Record user ID, date, time, and terminal location or IP address for each unauthorized access attempt
- Generate Unauthorized Access Report upon request

Outputs:

Unauthorized access report

Implementation Approaches

- The system could monitor attempts by users (who have access to the system) to gain access to specific functions for which they are not authorized according to their assigned capabilities. The system could produce a report, upon request, that lists individuals who have attempted to gain unauthorized access to WIC functions.

3.11.2.5 Monitor Record Updates

To support detailed auditing of system usage, the system should capture the user who has updated system records. Each time a user enters or changes a data element, the system should associate a user ID with the modified data field, as well as a date for the data element change. If there is any need to trace changes to the database, system audit files produced as a result of this function could be reviewed. The system should produce a report that lists specific changes and the user and date associated with these changes. This is especially important for tracking certification functions that must be performed by different entities.

Inputs:

Created Date

Created User

Last Modified Date

Last Modified User

User Identification Number

Process:

- Record user ID, date, and time each change to system data
- Create Audit File

Outputs:

Modified data element audit file/report

3.11.3 Manage System

The system should automatically monitor and support the ongoing operation of the system and its components.

3.11.3.1 Perform System Back-Up/Restoration

> *The system should be backed-up at least daily so that data can be restored in the event of a system outage. The method for back-up may vary from system to system. Typically in centralized systems the data are backed-up at the data center. If a system failure occurs, the backed-up data are used to restore the database to its existing state just prior to the failure.*

The system should have the capability to perform an automated data back-up at a scheduled time without user intervention. To restore the database, the data should be copied from the back-up file to the database tables.

Inputs:

All newly entered data since last back-up

Process:

To back-up the data, the system should:

- Initiate timed back-up procedure
- Create Back-Up File

To restore the data, the system should:

- Load Back-Up File
- Copy Back-Up File to Database

Outputs:

Screen display confirming completion of successful data back-up/restoration

Implementation Approaches

- A mirrored back-up on a back-up drive could provide redundancy for quick recovery in case of drive failure.
- Data could also be "striped" across more than two back-up drives.
- Offsite storage of the application and vital programs at a remote hotsite could be addressed in case of disaster.

3.11.3.2 Import/Export Data Files

Some functionality needed to support WIC business processes may be automated but performed outside the main system. This functionality is provided through stand-alone applications that operate on separate hardware platforms, but require the use of data collected and maintained through the main system. For example, some states perform caseload management and financial analyses in Commercial-Off-the-Shelf (COTS) spreadsheet packages. These generic packages need financial and participation data collected through the WIC IS to perform this functionality.

Alternatively, legacy applications may create data that is needed for processing within the WIC IS. For example, a WIC IS may use

information imported from the state Medicaid files to determine adjunct income eligibility.

The WIC system should be able to import data from other systems as well as to extract data to be exported to external systems.

Inputs:

Required data elements depend upon the type of data being exported/imported.

Process:

To export the data, the system should:

- Retrieve Data
- Format Data
- Create export file

To import the data, the system should:

- Receive import file
- Update system database with data from import file

Outputs:

Required data elements depend upon the export file type

3.11.3.3 Provide Version Control

The requirements for configuration management vary according to the architecture of the system. In a centralized web-based system, software version control is relatively easy to manage. The data center staff controls the version of software running on the central host to which all sites are linked. When an update to software is made, the software is replaced on the central processor

The system should accept version updates at the central host.

Inputs:

Software Updates

Process:

- Log software version release
- Install new software at the host

Outputs:

Updated software

Updated version indicator in software

3.11.4 Archive System Data

WIC Program requirements stipulate that program records be kept for a period of time. To satisfy this requirement while preserving efficient system operation, it may be necessary to remove information that is not required for the day-to-day processing in the system. Historical WIC data can be stripped from the system and stored off-line (archived) for potential future use.

3.11.4.1 Archive and Restore Historical Data

The system should archive historical WIC participant records according to parameters specified by the State agency. It should be possible to specify different periods for different types of records since it is important to retain some types of data for longer periods than other data. The system should leave some type of indicator that informs a user that a record was previously stored in the system and is now located in the system archives. The system must also be able to retrieve those files for user access within a specified period of time (e.g., 24 hours), upon request.

Inputs:

Archive End Date

Archive File Number

Archive Location

Archive Name

Archive Parameters to select data for archiving

Archive Record Type Code

Archive Start Date

Process:

To archive historical data, the system should:

- Copy historical data to storage medium based on user-provided date parameters
- Strip archived data from the system

To restore archived data, the system should:

- Load data files or individual records according to user-specified parameters

Outputs:

Archive files

Restored data

Implementation Approaches

► Operating procedures could be established at local agencies and clinics to request retrieval of this information so that participants are not turned away because their files are not available on line.

3.11.4.2 Purge Unnecessary Data

> *This process is identical to the archive process described above, with the exception that the data are not stored before they are stripped from the system. State agencies may collect some types of information that are of no use after the period that they are needed online.*

The system should allow this information to be purged completely.

Inputs:

Purge Parameters

Process:

- Retrieve data that meets the purge parameters
- Strip data to be purged from the system

Outputs:

Purge file

Purge report