

Integrated Funds, Distribution,

Control Point Activity, Accounting

And Procurement

(IFCAP)

Security Guide

Version 5.1

October 2000

Revised April 2014

Department of Veterans Affairs

Office of Information and Technology

Product Development

THIS PAGE INTENTIONALLY LEFT BLANK.

Revision History

| Date | Description  | Project Manager | Technical Writer |
| --- | --- | --- | --- |
| April 2014 | Patch PRC\*5.1\*187. Change references to the IFCAP V.5.1 Technical Manual, to remove references to specific chapters. See sections 3.2, 3.3, and 3.4. | REDACTED | REDACTED, Developer; REDACTED, Technical Writer |
| January 2014 | Patch PRC\*5.1\*174 (IFCAP/eCMS Interface)Patch PRC\*5.1\*174 - added new PRCHJFIS Key. See Section 3.1Added IFCAP/ECMS EVENT TYPE 414.07 to Chapter 7 File and Security Access. See Section 7.1. | REDACTED | REDACTED, Analyst; REDACTED, Technical Writer |
| September 2013 | Patch PRC\*5.1\*171. Removed option Enter/Edit Control Point Users from menus. See page 11. | REDACTED | REDACTED, Developer; REDACTED, Technical Writer |
| September 2013 | Patch PRC\*5.1\*168 changed PRCFA SUPERVISOR code sheet, KEEP AT TERMINATE, from “YES” to “NO”. | REDACTED | REDACTED, Developer; REDACTED, Technical Writer |
| September 2012 | Editorial review and technical updates | REDACTED | REDACTED, Analyst; REDACTED, Editor |
| April 2012 | Patch PRC\*5.1\*159 changed security key PRCSCPO from KEEP AT TERMINATE: YES, to NO. See page [11](#Ticket01).  | REDACTED | REDACTED |
| October 2011 | Patch PRC\*5.1\*158 Modification of title for IFCAP VA Form 1358. See page [3-1](#PRC_158A). | REDACTED | REDACTED |
| August 2011 | Remedy Ticket HD512314 make option lists complete.  | REDACTED | REDACTED |
| July 2011 | Patch PRC\*5.1\*153 – New message interface with Austin for 1358 Obligations see pp. [13](#PRC_153a) and [17](#PRC_153b). | REDACTED | REDACTED |
| April 2011 | Per patch PRC\*5.1\*151 – removed reference to Security Key - PRCSOBL, see page [12](#PRC_151). | REDACTED | REDACTED |
| 1/05/2011 | Per Patch PRC\*5.1\*148 – removed references to Obligation Data option.  | REDACTED  | REDACTED |
| 8/21/09 | Added documentation related to PRC\*5.1\*130 | REDACTED  | REDACTED |
| 3/05/2008 | Added documentation for new menu option PRCHPM CS PURGE ALL | REDACTED | REDACTED |
| 3/2007 | Edits for the GIP ODI patch PRC\*5.1\*98 and for POU (patches PRC\*5.1\*1 and PRC\*5.1\*24) | REDACTED | REDACTED |
| 1/13/05 | Updated to address Deloitte's findings/recommendations. |  | REDACTED |
| 12/29/04 | PDF file checked for accessibility to readers with disabilities. |  | REDACTED |

THIS PAGE INTENTIONALLY LEFT BLANK.

Purpose of the Security Guide

The Security Guide specifies parameters controlling the release of sensitive information related to the Integrated Funds Distribution, Control Point Activity, Accounting, and Procurement (IFCAP) V. 5.1 software.

This document will be excluded from any Freedom of Information Act (FOIA) request releases. Distribution of this document is restricted to the Information Resource Management (IRM) Service and ADP Security Officer (ADPSO). Since certain keys and authorizations must be delegated for proper management of the system, information about these items may be found elsewhere in the technical and user manuals.

Reference Numbering System

This document uses a numbering system to organize its topics into sections and show the reader how these topics relate to each other. For example, section 1.3 means this is the main topic for the third section of Chapter 1. If there were two subsections to this topic, they would be numbered 1.3.1 and 1.3.2. A section numbered 2.3.5.4.7 would be the seventh subsection of the fourth subsection of the fifth subsection of the third topic of Chapter 2. This numbering system tool allows the reader to more easily follow the logic of sections that contain several subsections.

THIS PAGE INTENTIONALLY LEFT BLANK.

Table of Contents

[1. Introduction 1](#_Toc384039869)

[1.1. Security Management - Restrictions for Using Fiscal and Procurement Data 1](#_Toc384039870)

[1.2. Modifying Routines 1](#_Toc384039871)

[1.2.1. Procedures for Site Implementation 1](#_Toc384039872)

[1.3. Modifying Data Dictionaries 2](#_Toc384039873)

[1.3.1. Procedures for Modifications to Data Dictionaries 2](#_Toc384039874)

[1.4. Menu Assignments 3](#_Toc384039875)

[1.5. System Security Controls 3](#_Toc384039876)

[1.6. Security Awareness and Training 4](#_Toc384039877)

[1.7. User Security/Kernel Security Tools 4](#_Toc384039878)

[2. Electronic Signatures 7](#_Toc384039879)

[2.1. Overview 7](#_Toc384039880)

[2.2. Electronic Signature Design 7](#_Toc384039881)

[2.3. Identification 8](#_Toc384039882)

[2.4. Authentication 8](#_Toc384039883)

[3. IFCAP Security Keys and Other Features 9](#_Toc384039884)

[3.1. Description of Security Keys 9](#_Toc384039885)

[3.2. Mail Groups 12](#_Toc384039886)

[3.3. Bulletins 12](#_Toc384039887)

[3.4. Archiving/Purging 12](#_Toc384039888)

[3.5. System Lockout Settings 12](#_Toc384039889)

[3.6. Contingency Planning 12](#_Toc384039890)

[4. Interfacing 14](#_Toc384039891)

[4.1. Bar Code Readers 14](#_Toc384039892)

[4.2. HL7 Messaging 14](#_Toc384039893)

[4.2.1. IFCAP/DynaMed 14](#_Toc384039894)

[4.2.2. IFCAP/eCMS 14](#_Toc384039895)

[5. References 16](#_Toc384039896)

[6. Remote Systems 18](#_Toc384039897)

[6.1. EDI Transactions 18](#_Toc384039898)

[6.2. Procurement History Transactions 18](#_Toc384039899)

[6.3. LOG Transactions 18](#_Toc384039900)

[6.4. Transactions to Financial Management System in Austin, TX 19](#_Toc384039901)

[6.5. Receiving Reports 19](#_Toc384039902)

[6.6. Clinical Logistics Report Server data extracts 19](#_Toc384039903)

[6.7. 1358 Transactions to OLCS 20](#_Toc384039904)

[6.8. 2237 Transactions to eCMS 21](#_Toc384039905)

[7. File Protection and Security Access 22](#_Toc384039906)

[7.1. File Protection 22](#_Toc384039907)

[7.1.1. Files and Security Access 22](#_Toc384039908)

# Introduction

## Security Management - Restrictions for Using Fiscal and Procurement Data

The IFCAP (Integrated Funds Distribution, Control Point Activity, Accounting, and Procurement) V. 5.1 package deals with the activities and data related to the fiscal and procurement processes at your facility. The need for package security is addressed throughout this software, affording every effort to restrict the mishandling of IFCAP functionality. A significant amount of testing, as well as VA Central Office review, has been conducted on the entire IFCAP package. The Office of Acquisition and Materiel Management (OA&MM), and the Office of Budget and Finance, have requested that each facility utilizing the IFCAP package appreciate the sensitivity of these issues. It is for these reasons that each facility is reminded that local modification of program code is expressly prohibited.

## Modifying Routines

The modification of IFCAP V. 5.1 routines is covered by the Veterans Health Administration (VHA) Manual, M-11, “Information Resources Management,” Chapter 9, “Software Management.” The complete text may be found at REDACTED

A portion is quoted below:

### Procedures for Site Implementation

b. Local Modification of Software

1. Where a national package implements a controlled procedure (e.g., payroll processing, procurement, fee basis, medical quality control) which in turn reports data to a data base outside the VHA environment (e.g., CALM, Automated Medical Information System (AMIS)), there must be no alteration of that package except by the Development ISC. National package routines relating to security features or fiscal integrity also must not be altered except by the Development ISC.

…

1. Local modifications of national package routines are strongly discouraged. If local modifications are made to existing routines in national packages it will then be the responsibility of the modifying health care facility to maintain those modifications.

## Modifying Data Dictionaries

The modification of IFCAP V. 5.1 data dictionaries is covered by the Veterans Health Administration (VHA) Manual, M-11, “Information Resources Management,” Chapter 4, “Data Base Administration.” The complete text may be found at REDACTED

A portion is quoted below.

### Procedures for Modifications to Data Dictionaries

a. Modifications to national package data dictionaries should be restricted to the addition of new data elements and to the creation of input and output templates to meet specific needs of local sites. To ensure the capability of installing new releases of the application packages, it is important that any local additions to the data base be made in areas that will not conflict with elements contained in the nationally distributed data base.

b. When adding new data elements to the VA FileMan data dictionary, the numbering conventions used for creating new files should also be used for data elements.

1. A data element number should be entered that is in the numbering range of the assigned numbering prefix multiplied by 1000.
2. The same convention should be applied to global subscripts for local data add-ons to previously defined globals.

c. The VA FileMan sub dictionary numbers should be assigned at the high end of the numbering sequence, following the numbering convention outlined. For example, a VA FileMan sub dictionary number added to the Patient file (File 2) by station 368 should be 2.368001, a second sub dictionary should be assigned 2.368002, and so forth.

d. The VA FileMan data dictionary may be modified only through tools provided by the VA FileMan or by tools specifically referenced in the VA FileMan Programmer's Manual.

e. To keep conflicts with cross-references to minimum, field facilities creating custom cross-references must use the number range assigned to the site and prefix with "AZ" or "Z".

1. National packages are not permitted to use these cross-references.
2. Cross-reference numbers should be assigned based on the station number multiplied by 1000.

f. All other types of local data modifications to national packages are strongly discouraged. If local modifications are made to existing data elements in a national package data dictionary, it will then be the responsibility of the site to maintain those modifications as new versions of the package are installed.

g. When software components are incorporated into the package, the names associated with the new components (e.g., routines, options, templates) should be prefixed by the package namespace followed by the letter "Z".

1. For example, a local option called "LOG" for the PSIV package would have the option name "PSIVZLOG".
2. Prefixing allows the site to readily differentiate between components developed locally and those associated with the DHCP national packages.
3. Namespaces of one, two, three, or four characters followed by "Z\*" shall not be exported in nationally developed software, but shall be reserved for local use.

## Menu Assignments

The concern for package security includes the menus assigned to the IFCAP user. ***NO IFCAP USER should have access to all of the options available.*** Just as a Control Point Official should not have the ability to enter a Ceiling Transaction, neither should a Purchasing Agent be able to obligate a Purchase Order. The standardized menus that accompany this package were specifically designed to account for those functions that are performed in Fiscal, A&MM, and Control Points. Although you have the ability to customize menus for a user, be aware of potential conflicts of interest and the requirement for proper segregation of duties. Be careful not to circumvent the checks and balances required in your daily operations.

## System Security Controls

Management, development, and implementation of system security controls are addressed in the IFCAP system security plan. The completion of a system security plan is a requirement of OMB Circular A-130, “Management of Federal Information Resources”, and of Public Law 100-235, “Computer Security Act of 1987”. The purpose of the security plan is to provide an overview of the security requirements of the system and describe the controls in place or planned for meeting those requirements. It also delineates responsibilities and expected behavior of all individuals who access the system.

A minimum set of management controls directed at individual IT users is required to protect IT resources, and technical and operational controls support the management controls. Management controls focus on the management of the computer security system and the management of risk for a system. The types of control measures must be consistent with the need for protection of the system or application. Examples of management controls include risk assessment and management, security controls assessments, signed rules of behavior documents, and “authority to operate” decisions.

The operational controls address security methods that focus on mechanisms that primarily are implemented and executed by people rather than systems. Examples of operational controls include personnel security, physical and environmental protections, contingency planning, application software change controls, data integrity controls, documentation, and security awareness and training.

Technical controls focus on security controls that the computer system executes. The controls provide automated protection from unauthorized access or misuse, facilitate detection of security violations, and support security requirements for applications and data. Technical controls include identification and authentication measures, access controls, and audit trails.

## Security Awareness and Training

VA has a mandated annual requirement for all VA employees, contractors, students, and volunteers to complete information security awareness training. The Federal Information Security Management Act (FISMA) along with other governing Federal policy mandates that each Federal agency provide periodic training pertaining to information security and accepted computer practices. The Office of Cyber and Information Security (OCIS) provides continually updated computer security awareness training via the VA Cyber Security Awareness course. This course contains Federal and VA specific criteria and requirements as well as an overall view of national security regulations.

All users of VA information systems must fulfill the annual security awareness training requirement every fiscal year. To fulfill the requirement users must complete the training and ensure it is recorded in the training tracking system in use at their location. If the training is completed via the on-line VA Cyber Security Awareness course a completion certificate can be printed, assuring that training has been adequately recorded. Users should retain a copy of the completion certificate when completing the course every fiscal year.

## User Security/Kernel Security Tools

User security is the cornerstone of Kernel’s system security features. Kernel is a set of software utility programs that provides an interface between operating systems, VistA application packages, and users. The purpose of Kernel’s security modules is to restrict access to the VistA computer system to only authorized users, to restrict authorized users to those tasks (menus/options) that they need to perform their jobs, to monitor user actions, to monitor selected changes to the database, and to monitor changes to programs. As such, Kernel offers the system-wide protection of all data on a VistA system.

All VistA applications make use of the Kernel’s security features to segregate functions among employees. The IFCAP package uses security keys to distinguish options that only Control Point Officials may use. Many applications now use the electronic signature feature as a validation of user identity when sensitive or privileged actions are required. All applications now employ the Program Integrity Checker to determine if the package programs have been altered.

**Access Requests:** It is VA policy to grant sufficient and timely access, necessary to perform assigned duties, for all authorized individuals. Access assignments will be made only after requests for access have gone through the request and concurrence process as defined in facility policy. All users of the IFCAP application will safeguard system accounts and passwords and will access only information necessary to perform duties. Violations of access and security policy will result in appropriate disciplinary action and loss of access privileges. All users must sign a “Rules of Behavior” before receiving access. Only authorized IT staff will receive access to programmer menu options, security keys, and file access as determined by IT management. All programmers will be assigned a Programmer Access Code (PAC), providing an added layer of security.

**User Account Inactivity:** The Kernel registers if the user is inactive for a pre-determined length of time. If the user does not interact with the VistA system within the time-out period, Kernel returns them to the previous prompt, eventually terminating the session of the user. VA policy requires facilities to set the Timed Read parameter in Kernel to 300 seconds to prevent unauthorized access to unattended workstations. Exceptions for health care providers are based on Clinical Application Coordinator (CAC) recommendations for extensions of up to 1200 seconds and will be reflected on the new user request form. Requests for increased timed-out greater than 1200 seconds should be handled on a case-by-case basis, require justification, and should be submitted to the designated facility security officer for concurrence. All users who are given access to VA systems and data are required to log off systems before leaving a workstation/device unattended.

**Audits:** Audit features of Kernel, addressed in detail in the Kernel Security Tools Manual, make it possible to monitor a wide range of computing activity. Audit logs provide the data required to identify and prevent unauthorized access, prevent inappropriate levels of access authority, and prevent potential corruption of the VistA database through inappropriate alteration of data or dictionaries. System reviews should be undertaken to examine existing audit logs that are automatically maintained by the system (i.e., the Sign-on Log and the Programmer Mode Log). When considering additional events to audit, research should be done to determine whether a mechanism is already in place within a VistA application package. The IT and security staffs are also urged to collect the minimal amount of audited data and purge the data when it is no longer needed as an audit trail to ensure that system performance and response time are not impacted by audit activities.

**Transfers/Terminations:** The manager or designee is responsible for notifying the system administrator when a user has been removed from, or assigned to, a position to ensure menus reflect current responsibilities. In the event of a suspension or unfriendly termination, the system administrator will be notified prior to, or at the time, the action is issued to the user. It is the system administrator’s responsibility to promptly deactivate accounts on all systems to which the user has access.

**Quarterly User Reviews:** Supervisors/managers are responsible for completing the quarterly user review in coordination with the designated IFCAP and/or ADPAC coordinator and in accordance with facility policy and standard operating procedures. This review ensures that users have access to only the information required to carry out their assigned duties and that access privileges of terminating or transferring staff are rescinded.

THIS PAGE INTENTIONALLY LEFT BLANK.

# Electronic Signatures

## Overview

A primary aspect of security in IFCAP involves the use of Electronic Signatures. Individuals in the system who have authority to approve actions, at whatever level, have the ability to enter and edit their own Electronic Signature Code. This code is required before the documents pass on to a new level for processing or review. Like the access and verify codes used when gaining access to the system, the Electronic Signature Code will not be visible on the terminal screen. These codes are also encrypted so that even when viewed in the user file by those with the highest levels of access, they are unreadable. Electronic Signature codes are required by IFCAP at every level that currently requires a Signature on paper. Electronic Signature codes are required for: Budget Analysts distributing funds to Control Points; Control Point Officials (not Control Point Clerks or Requestors) approving requests; Accountable Officers processing 2237s; Purchasing Agents/Ordering Officials processing purchase orders; Accounting Technicians obligating documents; Voucher Auditors authorizing payments; and Warehouse personnel receiving purchases.

Those individuals with Electronic Signature Codes have a menu option, located on their secondary menu (User’s Tool Box) that allows them to change their Signature Code at any time.

Required Electronic Signatures

* Accountable Officer Process Requests in PPM & Send 2237s to eCMS
* Budget Analyst Release Funds to Control Points
* Control Point Official Approve Requests
* Purchasing Agent/ Sign Purchase Orders
* Accounting Technician Obligate Documents
* Voucher Auditors Certifying Payments
* Warehouse Workers Receiving Reports
* Requisition Clerk Requisition Processing and Code Sheet
* Requirements Analyst Requisition Processing and Code Sheet
* Purchase Card Holder Sign Purchase Card Order
* Approving Official Approve Purchase Card Reconciliation
* Alternate Approving Official Approve Purchase Card Reconciliation

## Electronic Signature Design

An Electronic Signature is designed as a two-part process and is described in the following section.

## Identification

Identification (or “hashing”) is system verification that the person who logged in is the same person accessing a document. This process of identification uses the Electronic Signature (ESIG) Code string, which it passes through a hashing algorithm and compares it to a string maintained in the user file of the person currently logged into the system. A match indicates (unless a user has “shared” his/her ESIG Code with another person) that the person entering the ESIG Code is the “logged-in” user. The identification process can and is used independently of the record authentication function.

## Authentication

Authentication (or “encoding”) marks an electronic record within VISTA with the identification of the user. This process takes the internal record number of the record being secured (i.e., the Signature Block Name of the person signing the record and that person’s internal record number in the NEW PERSON file # 200) and passes it through a second algorithm to create a string. “Decoding” of the string occurs as the reverse of the process just described. The matching of the user Signature Block Name and the outcome of the Decoding process validates that the Electronic Signature is “tamper free”.

#

# IFCAP Security Keys and Other Features

## Description of Security Keys

This list of security keys is also found in chapter 5 of the IFCAP V. 5.1 Technical Manual.

**PRCFA PURGE CODE SHEETS**

DESCRIPTION: This key is required to purge old code sheets from the system.

 (NO OPTIONS)

**PRCFA SUPERVISOR**

KEEP AT TERMINATE: NO

DESCRIPTION: This key must be assigned to the Accounting Supervisor. It locks the following options.

 Purge Transmission Records/Code Sheets [PRC GECS PURGE]

 Retransmit Stack File Document [PRC GECS STACK RETRANSMIT]

 Enter/Edit Date When SOs become ARs [PRC SO TO AR]

 Audit Reports Menu [PRCF AUDIT REPORTS]

 Clear Program Lock [PRCFA CLEAR LOCK]

 Rebuild a Code Sheet Template [PRCFA REBUILD CODE SHEET MAP]

 Stacked Fiscal Documents Menu [PRCFA STACK DOCUMENTS]

**PRCFA TRANSMIT**

DESCRIPTION: This key is required to be held by any user authorized to release Receiving Report code sheet batches to Austin. It locks the following options.

 Retransmit Code Sheets Batch to Austin [PRCFA RETRANSMIT BATCH]

 Transmit Receiving Reports on Transmission List [PRCFA RR TRANSMIT]

 Transmit Code Sheets to Austin [PRCFA TRANSMIT CODE SHEETS]

**PRCFA VENDOR EDIT**

DESCRIPTIVE NAME: PRCFA VENDOR EDIT FMS FIELDS

DESCRIPTION: This security key provides access to edit certain critical fields, such as the FMS Vendor ID and the Alternate-Address Indicator, which are normally populated by incoming transactions sent by FMS. It locks the following options.

 Setup AR selected vendors [PRCO AR VENDOR EDIT]

 Review VENDOR REQUEST [PRCO VRQ REVIEW]

**PRCH AR**

DESCRIPTIVE NAME: APPROVE RECONCILED ORDER

DESCRIPTION: This key locks the Approving Official Menu [PRCH APPROVE] option.

**PRCH TRANSACTION COMPLETE**

DESCRIPTIVE NAME: All Status Amendment Key

DESCRIPTION: This key is required to amend a PO or Requisition, even if the Status is Transaction Complete. It locks the following options.

 All Status Amendment to PO [PRCH ALL STATUS AMEND TO PO]

 All Status Amendment to Req [PRCH ALL STATUS AMEND TO REQ]

**PRCHADVOUCHER**

DESCRIPTION: This key is required to create adjustment vouchers for receiving reports and requisitions. It is recommended that this key is assigned to the chief of P & C. It locks the following options.

 Adjustment Voucher to Receiving Report [PRCH ADJUSTMENT VOUCHER]

 Adjustment Voucher to Requisition [PRCHPM REQN ADJ VOUCHER]

**PRCHASSIGN**

DESCRIPTION: This key allows is required to assign a 2237 request to a specific purchasing agent. It locks the following option.

 Assign a Request to Purchasing Agent [PRCHPC ASSIGN REQUEST]

**PRCHIMP**

DESCRIPTION: This key is required to access to the main menu for processing Imprest Funds type Purchase Orders. It locks the following menu.

 Imprest Funds Processing Menu [PRCHPC IMPREST FUND MENU]

**PRCHITEM MASTER**

DESCRIPTION: This security key enables a "super user" to edit otherwise restricted fields.

**PRCHJFIS**

This key allows IFCAP FISCAL users to access the eCMS/IFCAP Transaction Report option.

 Accounting Utilities Menu Transaction Report [PRCFA UTILITY]/Transaction Report eCMS/IFCAP [PRCHJ TRANS REPORT3]

Budget Utilities Menu [PRCB UTILITIES] /Transaction Report - eCMS/IFCAP [PRCHJ TRANS REPORT3]

**PRCHPM CS PURGE CODE SHEETS**

DESCRIPTION: This key is required to purge LOG, GSA or DLA code sheets from LOG Code Sheet File. It locks the following option.

 Purge Code Sheets (LOG/GSA/DLA) [PRCHPM CS PURGE]

**PRCHPM CS PURGE ALL**

DESCRIPTION: This option allows the user to delete all code sheets from the code sheet file, which have been transmitted to Austin or DLA and which exceed a selectable number of days in age. It locks the following option.

 Purge All Code Sheets [PRCHPM CS PURGE CODE SHEETS]

**PRCHPM CS TRANSMIT**

DESCRIPTION: This key is required to transmit LOG, GSA or DLA code sheets to Austin or DLA. It locks the following options.

 Add Code Sheet to Printed Batch (LOG/GSA/DLA) [PRCHPM CS ADD TO BATCH]

 Delete Code Sheet from Printed Batch (LOG/GSA/DLA) [PRCHPM CS DELETE FROM BATCH]

 Re-transmit Batch to Austin (LOG/GSA/DLA) [PRCHPM CS RE-TRANSMIT BATCH]

 Transmit Code Sheets to Austin (LOG/GSA/DLA) [PRCHPM CS TRANSMIT]

**PRCHRECDEL**

DESCRIPTION: This key is required to delete a Receiving Report for a purchase order. It locks the following option.

 Delete a Receiving Report [PRCHPM PO DEL REC]

**PRCHRPT**

DESCRIPTION: This key locks the Reprints Menu [PRCHOUT REPRINT]

**PRCPAQOH**

DESCRIPTION: This key enables the application coordinator to authorize via the [PRCP LET STAFF REPLACE QOH] option a secondary inventory point manager access for requesting adjustments of the GIP on hand quantities to match the linked supply station quantities within a specified inventory point.

**PRCPODI**

DESCRIPTION: This key enables the application coordinator to use the [PRCP ON-DEMAND USERS] option in order to authorize a primary or secondary inventory point manager the ability to change the on-demand setting of an item within a specified inventory point.

**PRCPSSQOH**

DESCRIPTION: This key allows an authorized secondary inventory point manager to request that the on hand quantities in the inventory point be adjusted to the on hand quantities in the associated supply station via the [PRCP REPLACE ON-HAND INVENTORY] option.

**PRCP MGRKEY**

DESCRIPTION: This key locks the PRCP MANAGER MENU (Primary Inventory)

**PRCP2 MGRKEY**

DESCRIPTION: This key locks the PRCP2 MANAGER MENU (Secondary Inventory)

**PRCPW ADJAPPR**

DESCRIPTION: This key locks the Approve Adjustments Menu [PRCPW ADJUST APPROVAL].

**PRCPW MGRKEY**

DESCRIPTION: This key locks the PRCPW MANAGER MENU (Warehouse Inventory)

**PRCSCPO**

KEEP AT TERMINATE: NO

DESCRIPTION: This key is for the Control Point Official. It locks the following options.

 Approve Requests [PRCSAPP]

 Enter FCP Adjustment Data [PRCSENA]

**PRCT MGR**

DESCRIPTION: This key restricts the ability to modify barcode programs and parameters that will affect the operation of barcode programs. It should only be given to IRM service personnel. This key locks the following menu.

 Programmer (Barcode) Menu [PRCT PROGRAMMER (BARCODE)]

## Mail Groups

A listing and description of Mail Groups appears in the IFCAP V. 5.1 Technical Manual.

## Bulletins

A listing and descriptions of Bulletins appears in the IFCAP V. 5.1 Technical Manual.

## Archiving/Purging

A description of the archiving and purging processes appears in the IFCAP V. 5.1 Technical Manual.

## System Lockout Settings

Access to information systems resources shall be managed by a combination of technical and administrative controls. These controls will ensure that only authorized individuals gain access to information systems resources, that these individuals are assigned an appropriate level of privilege, and that they are individually accountable of their actions. Access will be controlled and limited based on positive identifications and authentication mechanisms as follows.

Passwords shall be at least eight characters in length, and contain three of the following four kinds of characters: letters (upper and lower case), numbers, and characters that are neither letters nor numbers (i.e., "#", "@" or "$").

Passwords shall be changed no less frequently than every 90 days. Information systems shall not permit re-assignment of the last three passwords used.

Accounts that have been inactive for 90 days shall be disabled.

To preclude password guessing, an intruder lock out feature shall suspend accounts after five invalid attempts to log on. Where round-the-clock system administration service is available, system administrator intervention shall be required to clear a locked account. Where round-the-clock system administration service is not available, accounts shall remain locked out for at least ten minutes.

## Contingency Planning

Using services must develop a local contingency plan to be used in the event of product problems in a live environment. The facility contingency plan must identify the procedure for maintaining the functionality provided by IFCAP V. 5.1 in the event of system outage. Field station ISOs may obtain assistance from their Regional Information Security Officer (RISO).

THIS PAGE INTENTIONALLY LEFT BLANK.

# Interfacing

## Bar Code Readers

There are two bar-code readers utilized within VA Medical Centers:

* Intermec 9440 readers
* Janus 2020 bar-code readers

## HL7 Messaging

### IFCAP/DynaMed

IFCAP has HL7 messaging interfaces with the DynaMed system to pass Vendor, Item, and Control Point data and receive Purchase Requisition data to support Inventory management in that COTS system. Note: These interfaces are only to be utilized at the Bay Pines VA Medical Center.

### IFCAP/eCMS

Patch PRC\*5.1\*167 implemented a bi-directional interface between IFCAP and the electronic Contract Management System (eCMS) that is hosted at the AITC.

THIS PAGE INTENTIONALLY LEFT BLANK.

# References

The following handbooks contain materials that are related to IFCAP V. 5.1.

* FMS Handbook
* VHA Handbook 4671.1 - Cost Centers
* VHA Handbook 4671.2 - Budget Object Codes (Draft)
* VHA Handbook 1730.1 - Use and Management of the Government Purchase Card Program

# Remote Systems

The following entries describe the data transmitted from IFCAP V. 5.1 to remote system/facility databases.

## EDI Transactions

Electronic Request for Quotations (X12 840 transaction), Text Message (X12 864 transaction) and Purchase Order (X12 850 transaction) are sent in MailMan e-mail messages from IFCAP systems to the EDI group of OA&MM in Austin, TX. The TCP/IP handles accuracy within the mail transmission. Upon receipt, the receiving mail system sends back a Confirmation Message listing the Identification Number of the message on that mail system and an assigned Confirmation Number. When the transactions are processed by the EDI group's software, an 'ACT' transaction is send to the submitting station if the message could be properly processed, while a 'PRJ' message is sent if there was a problem with the format or content of the transaction. In EDI Purchase Orders whose method of payment is Purchase Card, a VA specific algorithm encrypts the Card Number and Expiration Date fields. The code implementing the encoding, like the rest of IFCAP, is not available under the Freedom of Information Act. With EDI Purchase Orders, a vendor responding to the order may send back a Purchase Order Acknowledgement transaction (X12 855 transaction) indicating acceptance of the order and providing updates to delivery schedule, pricing, and quantity or indicating rejection of the order. The receipt of a POA indicates that the order successfully arrived at the vendor.

## Procurement History Transactions

When items are ordered, IFCAP sends a Procurement History Activity (PHA) transaction in a MailMan e-mail message to a centralized, OA&MM procurement history database in Austin, TX. This contains information on the vendor supplying the goods, description of the goods and pricing. When amendments are done to the order, a Procurement History Modification (PHM) transaction is sent to this database. The TCP/IP handles accuracy within the mail transmission. Upon receipt, the receiving mail system sends back a Confirmation Message listing the Identification Number of the message on that mail system and an assigned Confirmation Number.

## LOG Transactions

IFCAP sends information related to changes in quantities of items in the Supply Fund warehouse inventories and related to orders from federal vendors in LOG code sheets, which are packed into MailMan e-mail messages and sent to an Austin TX OA&MM database. The TCP/IP handles accuracy within the mail transmission. Upon receipt, the receiving mail system sends back a Confirmation Message listing the Identification Number of the message on that mail system and an assigned Confirmation Number.

## Transactions to Financial Management System in Austin, TX

IFCAP sets up documents describing the distribution of funds, financial data on obligations for goods and services, invoice amounts from receipt of goods and services, and requests for transfer of funds between accounts.

IFCAP also sends Vendor Request transactions (VRQs) to add new vendors to the Financial Management System (FMS) vendor database and to request updates to the IFCAP database with the FMS vendor IDs, alternate address indicators, and payment addresses.

 These documents are handed off to the VISTA Generic Code Sheet module. This module then loads the documents into MailMan e-mail messages sent to the Financial Services Center in Austin, TX. The frequency that the Generic Code Sheet processes batched documents is site configurable, with ‘every 15 minutes’ being a common value. Documents can have a future transmission date specified so that they are held for later transmission. The TCP/IP handles accuracy within the mail transmission. Upon processing these transactions, FMS sends a Document Confirmation Transaction (DCT) back to the sending station for updating the status of the record in the Generic Code Sheet Stack file, as accepted or rejected.

## Receiving Reports

Upon the receipt of goods, IFCAP sends a RT transaction to IFCAP Receiving Report Program (IFRR) or Federal Receiving Report Program (INRR) for recording each receipt from a Non-Federal or Federal vendor, respectively. This transaction lists the total cost, cost by item, accounting information and vendor identification. The RT transaction is sent via a MailMan e- mail message to the IFRR/INRR database. The TCP/IP handles accuracy within the mail transmission. As with all MailMan messages send to other MailMan systems, the message transmission status, and the Identification Number of the message in the receiving MailMan system is recorded in the copy at the originating site. Ultimately, receiver information is transferred to the Computer Assisted Payment Processing (CAPP) system, which after matching the receiver against a vendor's invoice generates the Receiving Report to be processed by FMS.

## Clinical Logistics Report Server data extracts

The Clinical Logistics Office (CLO) requires the ability to analyze field data, including specific reporting needs in the area of performance measures and indicators. The Clinical Logistics Report Server (CLRS) will provide a temporary solution. Upon completion of the CLRS monthly reporting, Clinical Logistics data will reside on a server using Microsoft Structured Query Language (SQL) Server-based technology.

The CLRS tracks performance measures/indicators identified by CLO. It also provides a roll-up of station purchase order activity, which enables Clinical Logistics Analysts (CLA) to look at data pertaining to standardization, compliance, contracting, and related issues. CLAs also view Inventory Point (GIP) station level statistics, so that Veterans Integrated Service Network (VISN) supply statistics at the VISN and national levels can be monitored and also review 1358 Obligation transaction data as well.

Chief Logistics Officers and Central Office staff members have the ability to drill-down to some of the indicator data via CLRS and its associated options.

Ultimately, the data gathered using the CLRS option will become part of the National Logistics Data Warehouse (NLD) strategy. The Data Warehousing Managers Group, which manages the Prosthetics server as well, will be performing the system administration functions for the CLRS.

Each month, routines are scheduled to run the data extracts needed for these reports. As part of this run, the *Virtual Memory System (VMS)* or Microsoft *Windows*® flat files for the Procurement and GIP extracts are created for *File Transfer Protocol (FTP)* transmission. One routine handles the Procurement data extracts, while another handles the GIP extracts.

All data will be pulled from the fields identified in the CLRS Reporting (Purchase Order Data) appendix to the *IFCAP Technical Manual.*

Upon completion of the extracts, the extracted data files will be sent via FTP to a directory location on the CLRS. The file transfer automatically occurs following the extract routine. The system sends advisory mail messages to the PRCPLO CLRS NOTIFICATIONS mail group.

Once CLRS receives the extracts, CLAs analyze the data. Station level data is extracted/analyzed/cleansed on a monthly basis by Clinical Logistics Analysts.

## 1358 Transactions to OLCS

Patch PRC\*5.1\*153 established an interface between the IFCAP application and the Online Certification System (OLCS) located at the Financial Services Center (FSC) in Austin, Texas.

The interface is a one-way data exchange of 1358 Obligations data from the IFCAP application to the OLCS. The electronic exchange of 1358 transactions between the IFCAP application and OLCS uses VistA MailMan messages. The mail messages provide OLCS with the 1358 Number (i.e. Purchase Order Number), requestor, approver, and obligator for each 1358 obligated or adjusted in IFCAP to enforce segregation of duties in the OLCS.

The following IFCAP events trigger a MailMan message from the local site to the Online Certification System:

* OBLIGATION Event - when a new 1358 transaction is obligated in IFCAP
* ADJUSTMENT Event - when an increase/decrease adjustment transaction is obligated in IFCAP

Upon receipt of a 1358 transaction message, the FSC receiving mail system sends back a Confirmation Mail Message listing the Identification Number of the message on that mail system and an assigned Confirmation Number.

## 2237 Transactions to eCMS

Patch PRC\*5.1\*167 implemented an interface between the IFCAP application and the electronic Contract Management System (eCMS) located at the Austin Information Technology Center (AITC).

The following IFCAP events will trigger an HL7 message from the local site to eCMS:

* Accountable Officer processes a 2237 and sets the status of the 2237 to *Send to eCMS (P&C).*
* Accountable Officer uses the option: Retransmit a 2237 to eCMS to resend a 2237 to eCMS.

The following eCMS events will trigger an HL7 message from eCMS to the local site:

* eCMS user Returns a 2237 to the Accountable Officer for further processing in IFCAP.
* The Accountable Officer and CP Clerk listed as the Requestor on a 2237 will also receive MailMan messages in IFCAP alerting them that the 2237 was Returned.
* All IFCAP background processing is completed to ensure the 2237 Status is reset to: *Pending Accountable Officer e-Signature.*
* eCMS user Returns a 2237 to the Control Point level for edit and re-approval in IFCAP.
* The Accountable Officer, Control Point Official and Clerk listed on a 2237 will receive MailMan messages alerting them that the 2237 was Returned.
* All background processing is completed to ensure the 2237 status is reset to *Returned to Service by eCMS (P&C).*
* eCMS user Cancels a 2237.
* The Accountable Officer, Control Point Official and Clerk listed on the 2237 will receive MailMan messages alerting them that the 2237 was cancelled.
* All background processing is completed in IFCAP to ensure that the 2237 status is reset to: *Cancelled*: *Cancelled*

# File Protection and Security Access

## File Protection

This file protection information is also found in the IFCAP V. 5.1 Technical Manual, Chapter 4.

The IFCAP V. 5.1 package files contain data that is prepared according to the policy and procedures of the Office of Budget and Finance and the Office of Acquisition and Materiel Management. Therefore, the files used by IFCAP generally carry a high level of file protection. The data dictionaries for IFCAP should NOT be altered. Screening logic has also been enabled on some IFCAP files to prevent access through VA FileMan.

The IFCAP package uses eight (8) VA FileMan file protection levels on its files:

1. None - where no special security is enabled
2. # - Site Manager access
3. @ - Programmer access to files
4. [ - READ Access
5. ] - WRITE Access
6. % - Delete Access
7. $ - LAYGO Access
8. ^ - Cannot be accessed

### Files and Security Access

This file security access information is also found in Chapter 4 of the IFCAP V. 5.1 Technical Manual.

 DD RD WR DEL LAYGO

File Name Number Access Access Access Access Access

------------------------------------------------------------------------------

CONTROL POINT ACTIVITY 410 @ [ ] % $

TRANSACTION NUMBER 410.1 @ [ ] % $

CLASSIFICATION OF REQUEST 410.2 @ [ ] % $

REPETITIVE ITEM LIST 410.3 @ [ ] % $

SUB-CONTROL POINT 410.4 @ [ ] % $

CPA FORM TYPE 410.5 @ [ ] % $

DELIVERY SCHEDULE 410.6 @ [ ] % $

SORT GROUP 410.7 @ [ ] %

DELIVERY POINT 410.8 @ [ ] % $

ADMIN. ACTIVITY SITE PARAMETE 411 @ [ ] % $

FACILITY TYPE (TEMPORARY) 411.2 @ [ ] % $

IFCAP CONVERSION DISCREPANCY 411.3

IFCAP CONVERSION ERROR 411.4

IFCAP PARAMETERS 411.5 @ %

IFCAP/ECMS TRANSACTION 414.06 @ @ @ @ @

IFCAP/ECMS EVENT TYPE 414.07 @ @ @ @ @

 DD RD WR DEL LAYGO

File Name Number Access Access Access Access Access

------------------------------------------------------------------------------

FMS TRANSACTIONS 417

FMS EXCEPTIONS 417.1

FUND CONTROL POINT 420 @ [ ] % $

COST CENTER 420.1 @ [ ] % $

PRCD SD PROGRAM 420.13

PRCD SD FCP/PRJ 420.131

PRCD SD OBJECT CLASS 420.132

PRCD SD JOB 420.133

PRCD SD REPORTING CATEGORY 420.134

PRCD SD REVENUE SOURCE 420.135

PRCD SD SUB-REV SOURCE 420.136

PRCD SD SUB-OBJ 420.137

PRCD SD FMS SECURITY 420.138

PRCD FUND 420.14

PRCD FMS SUB-ALLOWANCE ACCOUN 420.141

PRCD SD ADMINISTRATIVE OFFICE 420.15

PRCD SD DOCUMENT TYPE 420.16

PRCD SD DOCUMENT DATA ELEMENT 420.17

PRCD REQUIRED FIELDS 420.18

PRCD STANDARD DICTIONARY 420.19

PRCD SD STATUS 420.1999

BUDGET OBJECT CODE 420.2 @ [ ] % $

PRCD FUND/APPROPRIATION CODE 420.3 @ [ ] % $

CALM/LOG TRANSACTIONS CODE LI 420.4 @ [ ] % $

UNIT OF ISSUE 420.5 @ [ ] % $

CODE INDEX 420.6 @ [ ] % $

BUDGET DISTRIBUTION CODES 420.7 @ [ ] % $

SOURCE CODE 420.8 @ [ ] % $

INTERMEDIATE PRODUCT 420.9 @ [ ] % $

PRCU IFCAP/FMS CONVERSION 420.92

IFCAP/FMS OBLIGATION RECONCIL 420.96

IFCAP/FMS FCP RECONCILIATION 420.97

IFCAP/FMS FCP RECONCILIATION 420.98

IFCAP TEMP FCP SNAPSHOT 420.99

PRCD SD STANDARD FOR COPYING 420.9999

FUND DISTRIBUTION 421 @ [ ] % $

MULTIPLE DISTRIBUTION 421.1 @ [ ] % $

CALM/LOG TRANSMISSION RECORD 421.2 @ [ ] % $

CALM ERROR MESSAGES 421.3 @ [ ] % $

FISCAL LOCK 421.4 @ [ ] % $

INVOICE TRACKING 421.5 @ [ ] % $

FUND DISTRIBUTION (TEMP TRANS 421.6 @ [ ] % $

INVOICE DLN COUNTER 421.7 @ [ ] % $

FISCAL STACKED DOCUMENTS 421.8 @ [ ] % $

INVOICE PARTIAL COUNTER 421.9

CALM/LOG TEMPLATE MAPS 422 @ [ ] % $

COUNTER 422.2 @ [ ] % $

CALM/LOG CODE SHEET 423 @ [ ] % $

ISMS REASON CODES 423.4 @ @ ^ ^ ^

PRC IFCAP MESSAGE ROUTER 423.5 @ [ ] % $

ISMS/FMS TRANS 423.6 @ [ ] % $

CALM/LOG BATCH TYPE 423.9 @ [ ] % $

1358 DAILY RECORD 424 @ [ ] % $

1358 AUTHORIZATION DETAIL 424.1 @ [ ] % $

VENDOR 440 @ [ ] @

DIRECT DELIVERY PATIENTS 440.2 @ [ ] #

VENDOR EDIT 440.3

PURCHASE CARD INFORMATION 440.5 @ @ @ @ @

 DD RD WR DEL LAYGO

File Name Number Access Access Access Access Access

------------------------------------------------------------------------------

PURCHASE CARD ORDER RECONCILE 440.6 @ @ @ @ @

MONTHLY ACCRUAL 440.7 @ @ @ @ @

PRCH AFC CHARGE TRANSMISSION 440.8 @ @ @ @ @

ITEM MASTER 441 @ [ ] # $

FEDERAL SUPPLY CLASSIFICATION 441.2 @ @ @ @ @

FSC GROUP TITLES 441.3 @ @ @ @ @

DLA/LOG CODES 441.4 @ @ @ @ @

TYPE OF REQUISITION AMENDMENT 441.6

AMENDMENTS TO DELIVERY SCHEDU 441.7

PROCUREMENT & ACCOUNTING TRAN 442 @ [ ] % $

TYPE OF AMENDMENT 442.2 @ @ @ @ @

PURCHASE ORDER STATUS 442.3 @ @ @ @ @

PURCHASE AUTHORITY 442.4 @ [ ] # #

PAT TYPE 442.5 @ @ @ @ @

PAT NUMBER 442.6 @ [ ] %

ADMINISTRATIVE CERTIFICATIONS 442.7 @ [ ] @ $

DELIVERY SCHEDULE (ORDER) 442.8

ELEC RECEIVING REPORT BATCH 442.9 @ @ @ @ @

REQUEST WORKSHEET 443 @ @ @ @ @

IFCAP PURGEMASTER WORKLIST 443.1

IFCAP PURGE PARAMETERS 443.2

IFCAP PURGE INPROCESS 443.3

TYPE OF SPECIAL HANDLING 443.4

P.O./REQUEST/R.R. PRINT LOG 443.5 @ @ @ @ @

AMENDMENTS 443.6 @ @ @ @ @

EDI SENDER 443.75 @ @ @ @ @

EDI ERROR CODES 443.76 @ @ @ @ @

LOCAL PROCUREMENT REASON CODE 443.8 @ @ @ @ @

IFCAP PENDING ARCHIVE 443.9

REQUEST FOR QUOTATION 444 @ [ ] % $

RFQ VENDOR 444.1 @ [ ] % $

SIC CODE 444.2 @ [ ] % $

SIC CODE GROUPS 444.21 @ @ @ @ @

RFQ COUNTER 444.3 @ @ @ @ @

RFQ EDITING PREFERENCE 444.4 @ [ ] @ @

GENERIC INVENTORY 445 @ @ @ @

INVENTORY BALANCES 445.1 @ @ @ @

INVENTORY TRANSACTION 445.2 @ @ @ @

INTERNAL DISTRIBUTION ORDER/A 445.3 @ @ @ @

STORAGE LOCATION 445.4 @ @ @ @

AUTOMATED SUPPLY STATIONS 445.5 @ @ @ @ @

GROUP CATEGORY 445.6 @ @ @ @

CASE CARTS 445.7 @ @ @ @

INSTRUMENT KITS 445.8 @ @ @ @

DISTRIBUTION/USAGE HISTORY 446 @ @ @ @

INVENTORY DISTRIBUTED PATIENT 446.1 @ @ @ @

BARCODE PROGRAM 446.4 @ @ @ @

CUSTOM LABEL 446.5 @ @ @ @

SPECIALTY COMMANDS 446.6 @ @ @ @

CLRS REPORT STORAGE FILE 446.7 @ @ @ @ @

INVENTORY LOCK MANAGEMENT 447 @ @ @ @ @

AUTOMATED SUPPLY STATION PROC 447.1 @ @ @ @ @