

# The IMA Desktop Implementation Guide

## Privacy and Access

---

### Contents

<b>Introduction</b>	<b>2</b>
<b>Guidelines</b>	<b>3</b>
<b>Safeguarding the IMA Desktop</b>	<b>5</b>
<b>Action Steps</b>	<b>6</b>
<b>Basic Access</b>	<b>7</b>
<b>Portals</b>	<b>8</b>
<b>Individualizing the Portal</b>	<b>13</b>
<b>Define Operators</b>	<b>15</b>

# The IMA Desktop Implementation Guide

## Privacy and Access

---

### Introduction

The IMA Desktop is a complex data system that can hold enormous amounts of information about clients, their diagnoses and treatment, their financial records, personal details, as well as records of staff members, their activities, agency finances, and much more. A great deal of this information is private or involves records that must be secured for a variety of reasons. The agency's administration is responsible for the safekeeping of all of these records, including paper documents and the information that resides in the computer data system. This section of the Implementation Workbook provides a framework for making important decisions about security that affect the IMA system.

# The IMA Desktop Implementation Guide

## Privacy and Access

---

### Guidelines

#### **Guidelines for Client Privacy**

According to New York State privacy laws and HIPAA regulations, whether particular client information can be shared or not is governed by the principle of “minimum necessary” disclosure.

Following HIPAA guidelines, the use, disclosure, or release of ‘Protected Health Information’ (PHI) must be controlled and limited to purposes connected to treatment, payment, or operations goals, and only to the extent that the ‘minimum necessary’ principle is followed. The agency must control the information and transactions that each user can see and what they are permitted to do with the information they do see.

#### **Guidelines for Confidential Agency Information**

In addition, the agency needs to control access to confidential organization information.

- How do privacy regulations and requirements affect the IMA Desktop?
- What commands in the IMA Desktop control the system and limit the information that particular users can see and work with?
- What basic privacy decisions do system administrators need to make, and how can they put them into effect?

#### **Guidelines for Passwords**

The system administrator needs to determine how strict a level of password security to implement. The basic decisions involve a tradeoff between security and ease of use.

- Minimum size of required passwords – The larger the size, the more difficult it is for unauthorized access. The smaller the size, the easier it is for regular users.
- Composition of password – The administrator may specify that passwords cannot be dates, or that they must be numbers, or that they must consist of a mixture of characters, numbers, and special symbols.
- Periodic password changes - Leaving the same passwords in place forever is a potential breach of security. Deciding how often to change them is a tradeoff between user convenience and security.

# The IMA Desktop Implementation Guide

## Privacy and Access

---

- Policy enforcement – The system may be set up to enforce all or some of the rules established above including the automatic expiration of passwords.

### **Beyond passwords**

A password system is the first level of security, creating an obstacle to prevent unauthorized persons from gaining access at the point of initial entry. The objective of the password security system is the proper identification of the user when they enter the system.

Passwords are not the only way to control access. Reliability of identification can be improved by having the user login with the help of a biometric device. Such a device may read the user's fingerprint and look up the name that belongs to this fingerprint, automatically logging the person in. These devices are now readily and inexpensively available (less than \$200/unit).

### **Security**

Besides fingerprint verification, an administrator can choose from many other methods to accurately identify who is logging in, if conventional password security is found to be insufficient.

As of 2/28/03, the HIPAA "Final Security Rules" have been published. These rules specify the requirements and procedures mandated in securing client data and go into effect April 2005.

### **Additional Concerns**

Passwords and identity verification, while essential, are but a piece of a privacy plan. There are several other aspects of system protection that administrators should take into consideration:

- Physical security of the file server. As a central repository of agency information, this single computer has a critical role. It should be locked in a secure room to which access is tightly controlled.
- Security of all connected computers. Additional protective steps can be taken, such as password-protected screen savers or automatic logouts after a period of inactivity.
- Protection from the outside. Firewall protection is necessary to protect the network against external intruders who may enter through the vulnerable points, such as the internet or other remote connections. It is necessary to protect wide-area networks and remote offices with the same diligence that is given to a main office.

# The IMA Desktop Implementation Guide

## Privacy and Access

---

### Safeguarding the IMA Desktop

**BASIC ACCESS: Who is allowed to get into the system?**

This is called 'Operating System Access.' At this level, the system administrator controls which individuals can use the system by giving them login credentials (user ID and password).

**PORTALS: What will they see when they get in?**

A specific user does not need access to, or even a view of, all the functions, data structures and elements available in the IMA Desktop. There are a number of different **Portals** through which a user is admitted into the system. Each of these portals is associated with a unique **HomePage** (also called a Windows Menu) that gives the user access to a specific sub-set of the system. Typically this would correspond to the functions associated with the individual's specific job assignment.

**FINE-TUNING A PORTAL: Do they need special privileges or limits?**

Some users may need access to a feature that is outside of their portal; others need to be restricted from some specific feature that is available on their portal; still others may need some specific restriction requiring supervisory staff with extra authority to sign off on; some users can be granted the right to exchange email via the Internet, while others may be restricted to internal email only. These 'special permissions' add additional levels to the security within the IMA Desktop.

**DIVISIONAL SECURITY: Are all client records accessible to all users?**

This choice is an optional setting that must be initialized on the server by IMA. The agency may decide to segregate clients by organization and restrict staff access to only the clients within their own division. Divisions are established and clients, programs and end users are assigned to each.

Divisions can be program specific or can group like programs together. Divisions are defined in table DIVSON.

If the agency decides to implement divisional security, assign Programs and Operators to divisions. Clients will belong to divisions, as well, based on their Program enrollments.

# The IMA Desktop Implementation Guide

## Privacy and Access

---

### Action steps

- Start by identifying users who will use the system and what their basic roles are.
- Next, organize the users into functional groups and determine which portal works best for each group.
- Then, determine if certain users need to be restricted from using certain functions that are generally available through that role's portal.
- Next, extend special privileges to users for protected functions.
- Finally, if it has been decided that it is necessary, define divisions and indicate which user belongs to each. Users of the IMA Desktop can belong to up to ten (10) divisions.

# The IMA Desktop Implementation Guide

## Privacy and Access

---

### Basic Access

#### Which individuals can use the system?

Basic user access to the system is controlled by the Unix (Linux, AIX, or SCO) Operating System and is called “Operating System Access.” At this initial level, the person logs on to the computer system, identifies him/herself with a name and password, and is then connected and given permission to operate within that system.

#### How to Create User IDs and passwords

For each individual that will use the IMA Desktop:

1. A unique **User ID**. This is the name they use to log on to the system.  
Example for Mary Jones: jonesm, or maryjons, or maryj.  
The ID must be unique, with a minimum of 3 and maximum of 8 characters. It is recommended that a method be standardized for creating User IDs.
2. A **Password**. The user password keeps unauthorized people from gaining access to the computer.  
Example: Mary Jones’ password is “2shore.”  
Common sense dictates that this should not be obvious like someone’s first name or a date.
3. An **IMA Operator Code**. This is a 3-character identifier that is attached to IMA user.  
Example: MAJ or MJ1.

# The IMA Desktop Implementation Guide

## Privacy and Access

---

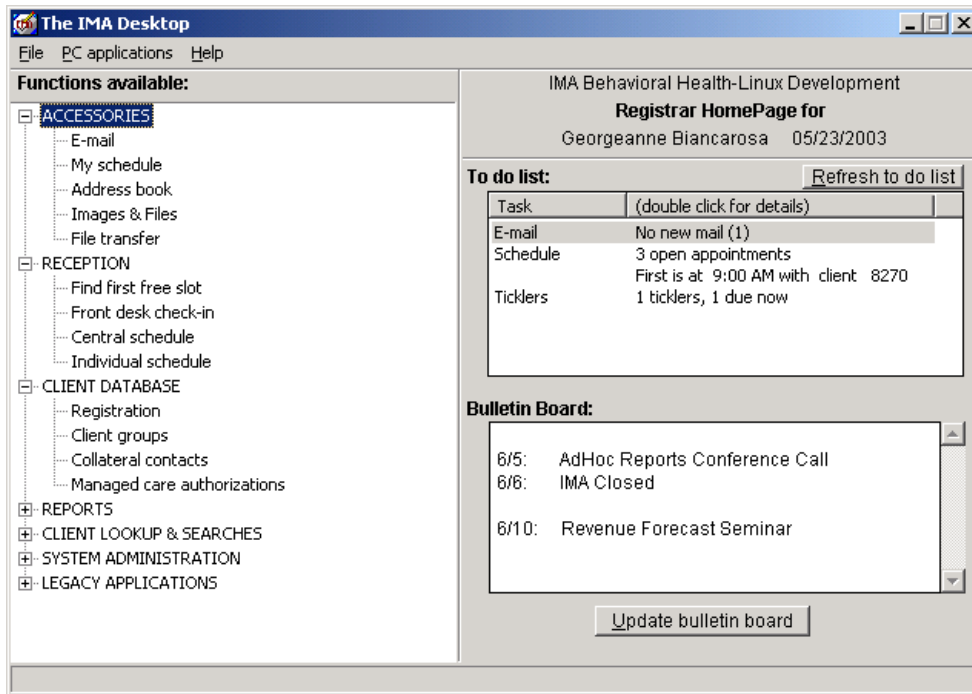
## Portals

### Define Portals for Staff Roles in the Agency

In the IMA Desktop, after staff members sign in, they are presented with an individualized HomePage that is associated with the **Portal**. Each portal offers a subset of the complete IMA list of available functions and databases. For example, a receptionist's portal shows registration and scheduling; a therapist sees charting and treatment planning; an accountant works with financial reporting.

Some of the portals currently available:

**REGISTRAR** Reception, typical job: registration, data entry, scheduling

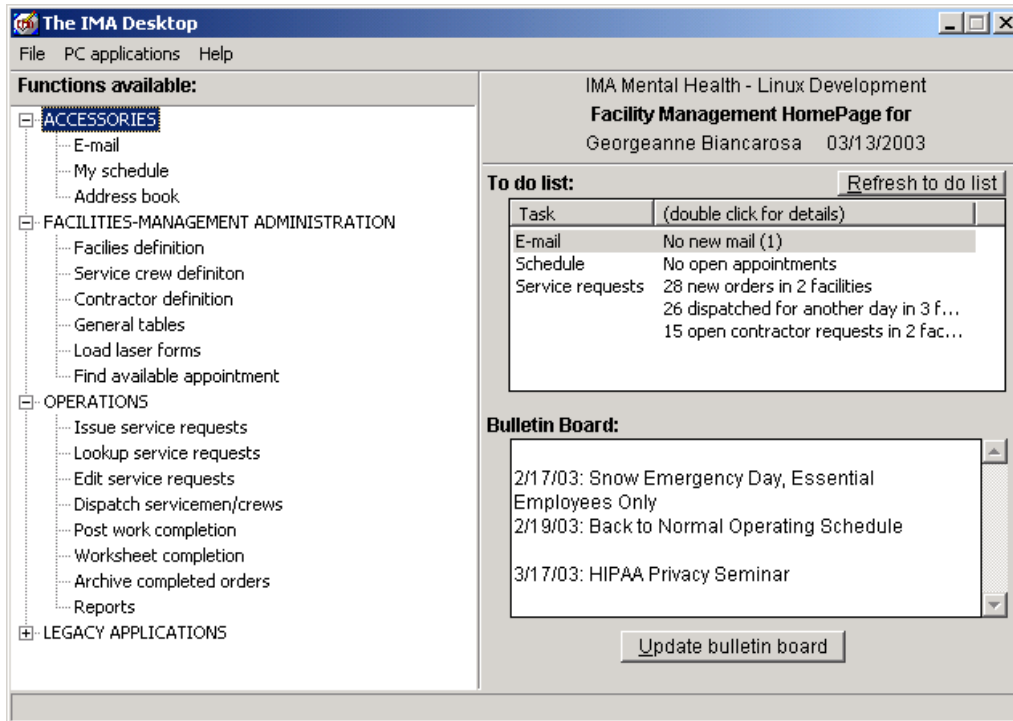


# The IMA Desktop Implementation Guide

## Privacy and Access

---

**FACILITY** Facility maintenance, typical job: maintenance, purchasing

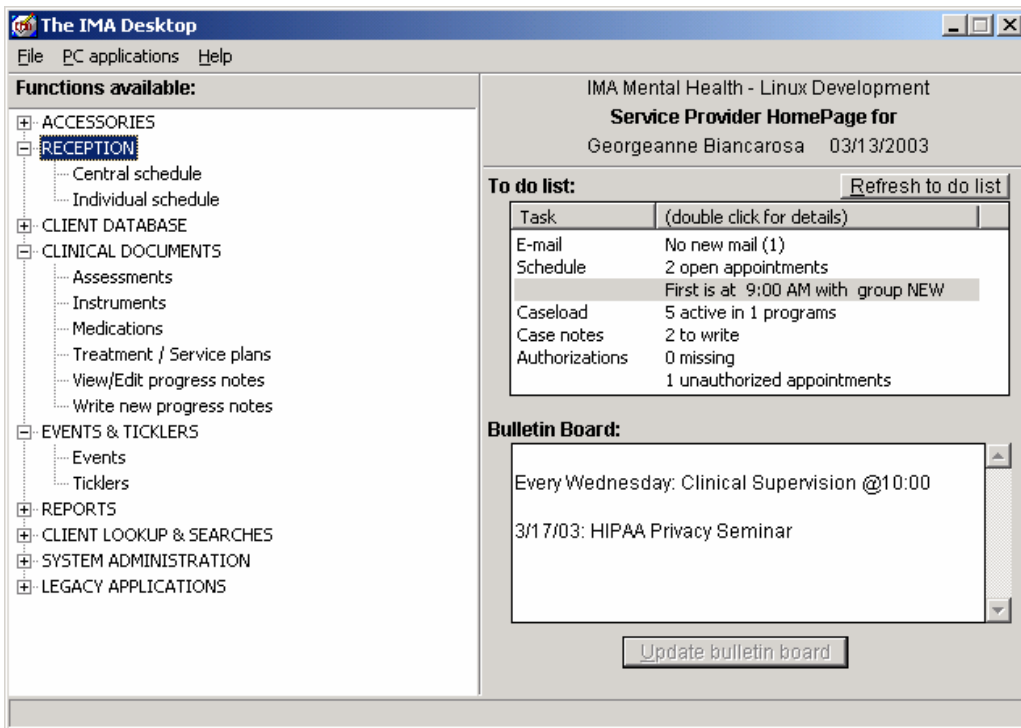


# The IMA Desktop Implementation Guide

## Privacy and Access

---

**PROVIDER** Service provider, typical job: therapist, clinician, doctor, RNP

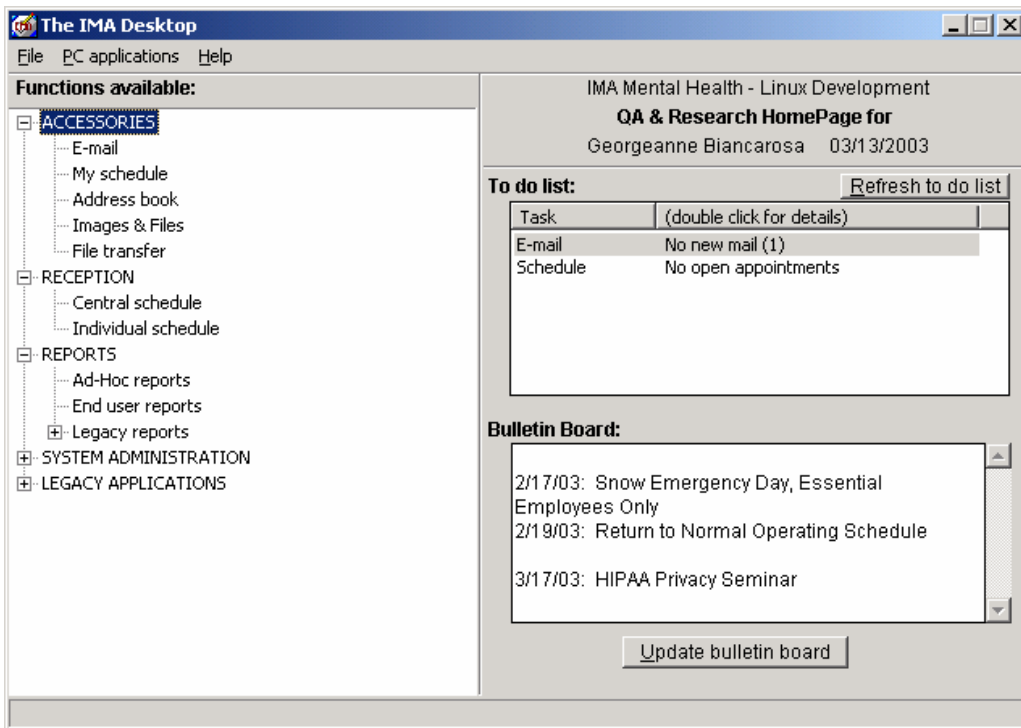


# The IMA Desktop Implementation Guide

## Privacy and Access

---

**QA** Quality Assurance, typical job: QA, Research



Other portals include:

<b>PGMANAGER</b>	Administrator, typical job: program manager, supervisor
<b>RESIDENCE</b>	Residence, typical job: residence staff or supervisor
<b>SYSADMIN</b>	System administrator, typical job: Desktop support, IS/MIS
<b>EXEC</b>	Executive, typical job: Executive Director, CEO, CFO
<b>BILLING</b>	Billing, typical job: Billing Manager, A/R

# The IMA Desktop Implementation Guide

## Privacy and Access

---

When the operator login has been created and a specific portal has been assigned to a user, we can say that we have established the “**User Profile**” for this user.

### **A typical agency scenario**

How an agency might assign their Portals:

Sarah	Therapist	Provider
Joan	Receptionist	Registrar
Mark	Accountant	Billing
Ellen	Maintenance	Facility
Joe	Residence supervisor	Residence
Elaine	Executive	Exec
Julian	Program Manager	Manager
Tom	Therapist	Provider

# The IMA Desktop Implementation Guide

## Privacy and Access

---

### Individualizing the Portal

After assigning a portal to a staff member, it is customized. Special privileges can be granted for access to administrative options, or for the ability to sign notes and to send Internet email, for example. Privileges can also be restricted, by the limiting of a specific report or option from the user within the assigned portal.

#### Permissions and Allowed Options

The IMA system is based on a well-developed menu. Each possible menu selection has been assigned a unique letter and number code. On the graphically visual IMA Portal, the user never sees the codes. They use simple mouse clicks to make selections and to move forward.

A system may have as many **Menu Permission Codes** as needed in a users' security profile to grant or deny specific levels of access to any particular menu item. (All of the possible menu choices and their corresponding codes are listed in an Appendix to this Guide.

The Menu Permission Code is always preceded by a **plus or minus sign**, translating access to a menu selection as either:  
**granted** (plus +) or **denied** (minus -).

To specify what permission or restriction to apply to a menu item, add a **Rights Code** of 2 characters following the menu code. The combination of Menu Codes and Rights Codes allows control of every aspect of each user's experience with the IMA Desktop.

The general Rights Codes and their corresponding privileges:

??	full rights to all functions within Menu option
SH	show or display only, look-up
LS	list
CH	change or edit information
AD	add records
DE	delete records (depending on option)

The full **Menu Permission Code** is six characters long:

Indicate + or - (to grant or deny) and then;  
IMA Menu *letter* (one character);  
Function *number* (two characters: either two digits or a single digit followed by a space);

# The IMA Desktop Implementation Guide

## Privacy and Access

---

Rights Code (two characters).

The formula for constructing a Menu Permission Code:

\_\_ (+ or -)\_\_ (Menu Letter) \_\_ \_\_ (Function Number) \_\_ \_\_ (Rights Code)

### Typical menu permission codes

- +X????** The user can use all the functions in their assigned Windows Menu or Portal.
- or
- +A2 ??** The A2 menu controls services and visits. Here the user can do everything within A2 including posting electronic service records, manual entry of single sessions, or closing services from a list of scheduled items.
- or
- A2 DE** In conjunction with the above permission for access to all of the A2 Menu, this restricts the A2 'DE', 'delete' option.
- or
- +C21SH** C21 controls billing record maintenance. Only the 'SH' or 'show' option, is allowed so this user can only view the billing record.
- or
- +?????** The system administrator gets five question marks granting him or her full access to all menus and functions.

### Beyond Menu Permission Codes: Special System Permissions

Menu Permission Codes fine-tune access to menu items through the user's portal. Another kind of codes, **Special System Permission Codes**, control aspects of access that are more general. With these codes, again preceded by a plus or minus access to basic system functions is controlled.

- +SUPER** Grants supervisory privileges for some functions within the schedule, front desk and within progress notes.
- +EEM** By default, all users are able to receive Internet email if Internet email is setup. This permission allows the user to additionally send external/Internet email.
- +H45PW** User can change his/her own password.
- +SNOTE** When the option to restrict who can sign progress notes is initialized, this permission allows the user to sign notes.

# The IMA Desktop Implementation Guide

## Privacy and Access

---

### Define Operators

Steps necessary to create users:

- List all users' names
- Create user IDs
- Establish passwords
- Create operator codes
- Associate each user with a Portal (windows menu)
- Set permissions and allowed options

Name	User ID	Password	Operator	Portal	Special Permissions
John Kramer	jkramer	jk0569	JLK	Provider	+H45PW, +SNOTE
Gloria Smith	gsmith	oriole89	GRS	Billing	+A2 ??, +C????, +H45PW
Nina Lopez	nlopez	nop789	NKL	QA	+G16??, +EEM, +H45PW
Sharon Rosen	srosen	bird395	SRR	SysAdmin	+?????; +SUPER; +EEM, +H45PW
Jeff Anderson	janders	n0g01021	JAA	PgManager	+SNOTE, +EEM, +SUPER, +H45PW

At this point, the system may be set up so that agency staff can start using the IMA Desktop. Referring to the lists that have been created:

- [+] SYSTEM ADMINISTRATION
  - Operator maintenance

The screenshot shows a window titled "Adding a new operator". It has three tabs: "Information", "Security", and "Permissions". The "Information" tab is selected. The form contains the following fields and values:

- Operator:  unix ID:
- Name:  Password:
- Title:  Clock#:
- Inactive?:  Yes  No
- Program org.:
- Printer:
- Forward mail to:
- Menu:
- Windows menu:

# The IMA Desktop Implementation Guide

## Privacy and Access

---

On this screen, in addition to the codes and information discussed already, there are two other items to fill in:

**Title** – This is the employee’s official title or the credentials of the staff member that should be used when signing progress notes and agency documents. It acts as an electronic stamp on the records.

**Default printer** – This should be filled in with the queue name of printer that the employee will print to by default. If it is not filled in, the user will be required to select a default printer each time they initiate an IMA Desktop session.

# The IMA Desktop Implementation Guide

## Privacy and Access

---

The screenshot shows a web-based interface for adding a new operator. The window title is "Adding a new operator". At the top left, there are two buttons: "<-Back" and "Add". Below these are three tabs: "Information", "Security", and "Permissions". The "Security" tab is currently selected. Under the "Security" tab, there is a section labeled "Divisions:" followed by ten vertical dropdown menus. The first dropdown menu is open, showing the text "M? - All mental health divisions". Below the dropdown menus, there is a "Staff access?" label with two radio buttons: "Full" and "Partial". The "Partial" radio button is selected.

*The Security Tab identifies the Divisions of the records to which the operator has access.*

**Division** – With the implementation of Divisional Security assign the operator up to ten division codes on this screen.

Divisions can be program specific or can group like programs, together. Divisions are defined in table DIVSON and are coded as follows, where the “?” serves as a wildcard.

- ?? all divisions
- M1 division M1 only (Example: for MH screening program/programs)
- M2 division M2 only (Example: for MH treatment programs)
- M? all divisions w/in M (Example: includes Divisions M1 & M2)
- R1 division R1 only (Example: for Residence 1)
- R2 division R2 only (Example: for Residence 2)
- R3 division R3 only (Example: for Residence 3)
- R? all divisions w/in R (Example: includes Divisions R1, R2 & R3)

**Staff access** – Within Divisional Security, grant either **Partial** or **Full** cross divisional access.

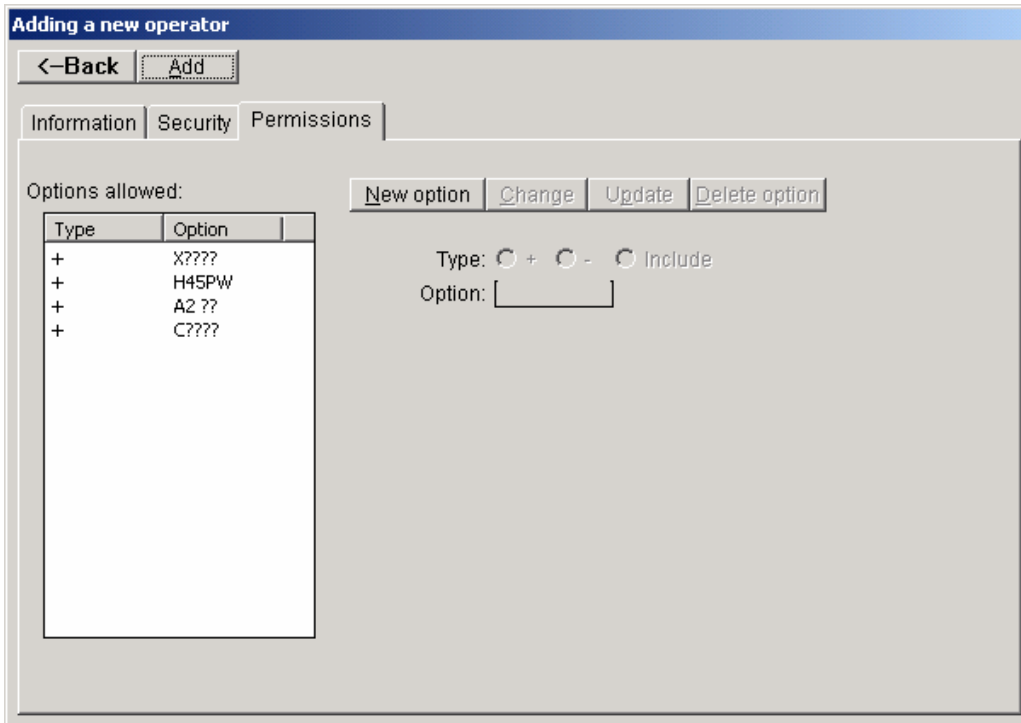
**Partial** restricts the user within his/her assigned division to client and programs that belong to his/her division.

**Full** expands the view of clients to include clients' program enrollments external to the user's divisions for any client within his/her division.

# The IMA Desktop Implementation Guide

## Privacy and Access

---



Add Operator Permissions tab

---

**Tip:** To save time use the 'Copy Operator' option. It is likely that many of the users will have similar roles in the agency. Save a lot of time by first creating one typical user of each kind, stamp out the rest with this feature and make individual changes to fine tune.

---

Use the list option to print out the user list as part of the permanent system documentation records.

When this process has been completed, refer to the user list above and run the UNIX program H46-NU to enter the UNIX ID and password for all the users. These are the same as have been entered in IMA Operator Maintenance. This completes the setup of user access. Now the system users can log in, unlock the portal that awaits them, and learn to take full advantage of their IMA Desktop.