AVImark contains a security feature that allows the hospital administrator to control the use of the different capabilities of the system in a very flexible way. The security feature is designed in such a way as to not affect the use of AVImark, except when a user attempts to do something that they are not authorized to do. This fact makes the security feature transparent to the user. The only extra action required by the user is that they log on when they first start AVImark. If you choose not to make use of the new security feature, all you will need to do is enter your list of doctors and other staff, and the security feature will be completely invisible to you. Likewise, you can choose to protect just a few functions in AVImark and those functions that you have not protected will be automatically available to everyone.

In this chapter you will learn how to:

“Identify and Add AVImark Users” on page 1
“Add Categories and Employees” on page 2
“Change User Information” on page 5
“Change Passwords” on page 5
“Specify Doctor Sequence and Location” on page 6
“Authorize User Functions” on page 6
“Specify Security for other User Groups” on page 8
“Print the User and Security Report” on page 8
“On-going Security Administration” on page 8
“Log on to AVImark” on page 9
“AVImark Compliance with FACTA Red Flag Rules” on page 9

Identify and Add AVImark Users

Whether or not you choose to use the AVImark security feature to control the activities of your staff, they will still need to be identified. Information should be recorded for each provider such as ID, names, license numbers (printed on the rabies certificate), and a staff sequence number which will determine the order doctors appear in the Doctors drop-down menu and on the Appointment Calendar.

- On the CID, open the Work with menu. Click Users and Security to display the Security Maintenance window.

![Security Maintenance Window](image-url)
Chapter 21: Security Administration

Add Categories and Employees

Once the appropriate staff members have been added to the Hospital Administrators Category, you may add other categories, and then other employees as required.

Add a new category

- Point in the **Category** section of the Security Maintenance window.
- Right-click and from the shortcut menu click **New** to display the New User Category window.

![New User Category Window]

- In the **Category** field, type the name for this category.
- Use the TAB key to move to the **Auto-logoff** field. Click the **Up** and/or **Down** arrow to specify the number of minutes to wait (if the user does not touch the keyboard or mouse) before automatically logging the user out of AVImark.
- Click **OK**.

Add new employees

- Click the **Category** you wish to add the new user to.
- Point in the **User for** section. Right-click and from the shortcut menu click **New** to display the New User window.

![Change User Window]
• Enter the appropriate information for the employee and click **OK**.

**Category**
This menu allows you to change the category in which to include this user. AVImark automatically enters the Category name depending on the Category you have selected when adding new staff.

• If appropriate, click the **Category** drop-down and select a category.

**First**
• Type the user’s first name.

**Last**
• Type the user’s last name, including ending titles such as DVM, VMD, etc.

**ID**
• Type the user’s initials or other ID; up to three characters.

**Password**
When entering a password, choose 3 to 5 characters using any combination of letters and numbers. Do not use spaces and/or punctuation marks. You will notice that when you open this window asterisks automatically appear. Whether or not the user has been assigned a password these asterisks will appear for security reasons. If you do not intend to use the AVImark security feature at this time, leave this field blank.

• Type an appropriate password.

**Cell Phone**
• If appropriate type the user’s cell phone number.

**Type**
This field is used by VetCor® veterinary hospitals to indicate the type user.

• Click the **Type** drop-down and select the **Type** user.

**E-mail**
This option allows reply e-mails that are received back from customers to be sent directly to a specified user.

• Enter the employees current e-mail address.

**Report**
This feature allows the user to enter a different name, other than the one entered in Users and Security. This Report name will be shown when printing an Invoice.

• If appropriate, type a **Report** name.

**Inactive**
AVImark allows you to mark an employee as inactive, causing them to be removed from the Doctor drop-down list, and from the Appointment Calendar. This may be especially useful in the event you wish to keep a user’s Time Card history for future reference.

• If appropriate, check the **Inactive** box.
User is a Doctor
When adding a new doctor to Users and Security, you will want to select this option. In doing so, the Sequence, DEA, License, and User Appears on Appointment Calendar fields are activated, allowing you to select and enter information.

- If appropriate, check the User is a Doctor box.

AVImark provides controlled substances reports to meet the requirements for specific states. The doctor’s DEA number will need to be entered for the use of these reports.

- If appropriate, type the doctor’s DEA number.

License
This field allows you to enter the doctor’s rabies license number.

- If appropriate, type the doctor’s License number.

User Appears on Appointment Calendar
This feature allows you to have a user appear on the Appointment Calendar.

- If appropriate, check the User Appears on Appointment Calendar box.

Appointment Color
AVImark allows you to assign a color for each doctor’s appointments on the calendar. You may select from a list of basic colors, or you may choose to create and add a custom color.

- Click the Appointment Color drop-down and then select the desired color or click Custom Color to display the Color window.
- Select the desired color from the Custom colors section and click OK.

Group
Each user that is displayed on the Appointment Calendar can be assigned a unique Appointment Group. Once users are assigned an Appointment Group, these users can be displayed according to the group in which they are included. Appointment Groups can be defined from this window by clicking the New button and entering a new code and description or from the new Appointment Groups table within System Tables.

- If applicable, use the Group drop-down list and select the correct Group.

Clocks In
This function allows you to track hours and activity with the AVImark Time Clock feature. For those staff members using the Time Clock check this option. This option must also be checked for those administrators who wish to view or change entries in an employees Time Card.

- If appropriate, check the Clocks In box.

Period Start
AVImark allows you to select the beginning date the user’s Time Card will default to.

- Click the Period Start drop-down calendar.
- Select the date you wish the Time Card to default to.

Track Overtime by Day
AVImark allows you to track an employee’s overtime by day.

- If appropriate, check the Track Overtime by Day box.
• Using the **Daily Hours** field, enter the number of hours the user works before overtime is tracked.

**Client Account Access**

You may prevent an employee from having access to add, change, or remove certain information. By adding the AVImark client account number of the employee to the Account field, you may select the access type you would like to grant that employee. **View only** will allow the user to open their account with a Read only access. **Add patient** allows the employee to add, change, or remove patient information. **Add history** gives access to adding, changing, or removing Medical History as well as patient information. **Full Access** will give the employee full access to their account. Selecting either **Add Patients**, or **Add History**, will prevent the employee from adding, changing, and removing Accounting entries.

- If appropriate, click the **Browse** button to display the Client Selection window.
- Type the employee’s name in the **Client** field and click **Continue**.
- Click the **Access Type** drop-down and select the access type you wish to grant.

**Completing the Setup**

- Click **OK** to add and save the new user information. After selecting OK, you will notice a User Sites window will appear. This will allow you to select the site where this user typically works. This is applicable for clinics with multiple sites.
- In this window choose right-click **New**.
- From the **Site** drop-down list select the appropriate Site and click **OK**.
- Click **Done** once the appropriate information has been entered.
- Another New User window will open allowing you to enter another staff member. You can do that at this time or click **Cancel** to close the New User window.

**Change User Information**

AVImark allows you to change information for any user within Users and Security.

- From the **User for** section, double-click on the correct name to display the Change User window.
- Change any necessary information. Use the TAB key or simply click to move from one field to another.
- Click **Done** to record any changes.

**Change Passwords**

Passwords may be changed from the AVImark Logon window at anytime. AVImark does not force a user to change their password. However, it is recommended to do so periodically.

- On the CID, press **F12** to display the AVImark Logon window.

![Logon Window]

- Enter the current Password. Use the TAB key to move to the **New password** field.
- Enter the New password and click **Logon**.
Specify Doctor Sequence and Location

Specifying Site Location for User
When AVImark data is being shared by multiple hospitals you can specify the site or location this user normally works.

- From the Security Maintenance window highlight the user and from the right-click menu select Locations.
- Click the Site drop-down and select the appropriate site.
- Click Ok once the appropriate information has been entered.

If the user works at multiple locations follow the above steps to add another location for the user.

Doctor Sequence
Once you have selected the option, User is a Doctor, AVImark will automatically enter the sequence number of how the doctor will appear in the Doctor drop-down list throughout AVImark. The sequence is set by the order in which the doctor was entered into Users and Security. Once the new doctor information has been added and saved, you may change this sequence number if you wish.

- From the Security Maintenance window highlight the appropriate doctor.
- From the right-click menu select Sequence, Doctors.
- Highlight the doctors name and use the green up and down arrows to move the user in the desired sequence. You can also drag-and-drop the user in the desired sequence.

Appointment Sequence
Selecting the option, User Appears on Appointment Calendar automatically assigns an Appointment Sequence number. As with the Sequence number, the Appointment Sequence is set by the order in which the user has been entered into Users and Security. You may change the Appointment Sequence once the new user information has been entered and saved.

- From the Security Maintenance window highlight the appropriate doctor.
- From the right-click menu select Sequence, Appointments.
- Highlight the doctors name and use the green up and down arrows to move the user in the desired sequence. You can also drag-and-drop the user in the desired sequence.

Authorize User Functions
Included with AVImark is a list of functions that can be protected. The use of these functions can be controlled through the use of the security feature. As you select the different Categories, you will notice the different functions associated with that category. You will want to identify what AVImark functions are to be protected, and which users are authorized to use these functions.

Hospital Administrators
Authorize the hospital administrator to perform only those functions which you want to prevent other categories of users from performing. By authorizing the function, Administer AVImark (System-wide Authority) to the hospital administrator, this will grant full authority to all functions in AVImark in one step.

- On the Security Maintenance window, click Hospital Administrator.
- Point in the Authorized Functions section. Right-click and from the shortcut menu click Choose to display the User Functions window.
Chapter 21: Security Administration

- From the Category section, click System Administration.
- From the AVImark functions for System Administration section, point to ADM01, Administer AVImark (System-wide Authority).
- Right-click and from the shortcut menu, click Select to copy the function into the Selected area.
- Continue selecting the other functions you wish to prevent other user groups from performing.
- After the appropriate functions have been copied to the Selected area, click Done.

Remove authority

Once functions have been authorized to a user group and you find it necessary to remove one or more of these functions, you may choose to do so a couple different ways.

- On the Security Maintenance window, click the Category name you wish to remove a function from.
- From the Authorized Functions section, point to the function you wish to remove. Right-click and from the shortcut menu, click Remove.
- You will need to click Yes to confirm.
  
  OR
  
- From the User Functions window, click the Category name for which functions had been authorized.

In the AVImark functions for section, functions which have been authorized to a user group will be indicated by a check mark in the Authorized column.

- In the AVImark function for section, point to the authorized function that you wish to remove.
- Right-click and from the shortcut menu, click Authorized Categories to display the Authorized to User Categories window.
Point to the appropriate **User Category** name. Right-click and from the shortcut menu, click **Remove**.

You will need to click **Yes** to confirm.

Click **Done** when finished removing the function from the appropriate user groups.

Specify Security for other User Groups

Use the discussion above to establish authority for other groups of users, if appropriate. Understand that with the functions you secured to the Hospital Administrator group, those functions are automatically off limits to other user groups, unless you authorize them as well. For those functions you have secured, you will need to decide if there are other groups of users which you want to authorize any of these same functions. Do not make the mistake of thinking you have to authorize everyone to all the functions they can perform. For any given function, if you don’t secure it as Hospital Administrator, everyone will be able to use it. When a user does not have the authority to perform certain functions or make desired changes, the window will be displayed as VIEW ONLY, and the fields within this window will be locked, preventing any change from being made. If the user attempts to click Done on a window that displays the VIEW ONLY message, they will be prompted with an unauthorized message.

Print the Users and Security Report

AVImark gives you the ability to print, e-mail, save and/or export a report containing a list of users, user groups, and secured functions for specific user groups.

Print the report

- On the **Security Maintenance** window, open the **File** menu. Click **Print** to display the Print Users window.
- Click the **Category** drop-down and select a **Category** or select **(All Categories)**.
- Click the **Print** drop-down and select the printer to print to.
- Click **Print** or click **Preview** to view the report on-screen.

On-going Security Administration

Once your users have been identified and authorized to the correct functions, the security feature more or less takes care of itself. As new employees join your staff or leave the hospital, you will simply add them to the appropriate user group or mark them as Inactive. As you become more comfortable with the security feature and the functions that you can protect, it is likely that you will gradually fine tune the security on your system to a more restrictive, yet workable level.
Log On to AVImark

From this point on, you are using the security feature. This implies several things, including the fact that you will be prompted for a password each time you start AVImark. AVImark will automatically allow or disallow the user to perform protected functions, based on what you have specified. From the Windows desktop, start AVImark in the normal manner. The logon window will appear in the center of the screen requesting you to enter your password. Enter your password and then click Logon.

AVImark Compliance with FACTA Red Flags Rule

AVImark includes security features that will aid in hospitals efforts to be compliant with the new Fair and Accurate Credit Transactions Act (FACTA) Red Flags Rule. The Red Flags Rule sets out how certain businesses must develop, implement and administer Identity Theft Prevention Programs.

AVImark security must be in place to protect and secure client privacy. To begin using security in these areas you must give access to one user group that has authority to perform the task. These new security functions apply to fields in the Client Area that store personal client information.

Having the following functions secured will safeguard customer information from being viewed on the main screen of the CID, from being accessed when the Change Client window is open and from being accessed from Information Search reports or utility program reports that contain this information. It is our recommendation that each function be secured only to the hospital administrator group.

- CLT12 – Change Client Drivers License
- CLT13 – Change Client SSN

Unauthorized user groups will not be allowed to view or enter information in the SSN or DL fields in a New or Change Client window.

These security functions also protect the following areas:
- The third-party reports generated by CareCredit, ASAP and Kasper
- The SSN and Drivers License fields will be protected from printing on the Information Search
- The information in the SSN and Drivers License fields will not be viewable in the Enter Payment and Invoice windows.