GE Healthcare

MUSE CV™ Information System

Software Version 005E

Advanced Security Guide

2020285-023 Revision C

NOTE: The information in this manual only applies to MUSE™ cardiology information system software version 005E. It does not apply to earlier software versions. Due to continuing product innovation, specifications in this manual are subject to change without notice.

Contents

Appendices

For your notes

Introduction

The MUSE system has several security features which, when properly used and configured, can support USA facilities in complying with the Health Insurance Portability and Accountability Act (HIPAA) Security and Electronic Signature Standards. These new security standards were designed to protect patient's health information from improper access, alteration, and loss when it is maintained or transmitted electronically.

For more information on the HIPAA Security and Electronic Signature Standards link to:

http://ge.com/hipaa

Compliance with the HIPAA Security and Electronic Signature Standards cannot be attained solely through the use of the security features on the MUSE system. Sites which use the MUSE system to maintain and transmit patient health information must use the security features in conjunction with a security plan which provides for the user training and secure physical access to patient health information.

This document is provided to describe how to properly set up and use the security features on the MUSE system. The responsibility of developing the security plan for user training and secure physical access to patient health lies with the end user.

If you have any questions or need assistance with any of these security setups, call the Jupiter On-Line Center at 1-800-558-7044.

Revision History

Each page of the document has the document part number followed by a revision letter at the bottom of the page. This letter identifies the document's update level. The revision history of this document is summarized in the table below.

Table 1. Revision History, PN 2020285-023

Revision	Date	Comment
A	15 April 2004	Initial release of manual.
B	21 July 2004	Document edited per feedback from 5E pilot installations.
C	7 February 2008	Document edited for software version v5E.14 release. Removed "Low Level Security" from "Access Control Security" section (SRS_2139).

Notes for Windows 2000 and Windows XP

The MUSE software uses the WIN.INI file to store miscellaneous run-time information . If the current user does not have write permissions to the WIN.INI file, the MUSE software will not run as expected.

By default, Windows 2000 and Windows XP do not provide write permissions to the WIN.INI file for the “Everyone” group.

The following is suggested as a workaround on systems running Windows 2000 or Windows XP:

The system administrator must give the “Everyone” or “[DomainName]\MUSE Users” group change permissions to the **WIN.INI** file. This can be accomplished through the file *Properties* dialog in *Windows Explorer.*

Checklist for MUSE Security Features

When setting up security on the MUSE system, use the following checklist as a reminder of security features available on the system which address both HIPAA and FDA 21 CFR Part 11 requirements. Shaded features are not required for 21 CFR Part 11 compliance but are considered good security practices.

FDA Requirement	MUSE Feature	Configuration	Recommended	Solution
Authentication & Authorization	Access Control Security	MUSE Users' Password	MUSEAdmin, MUSEBkgnd, and MUSE Users' passwords should adhere to facility's best practice or policy.	❒
		MUSERss User	Users should be familiar with how to enable and disable the MUSERss user.	❒
			Configure pcAnywhere *Callers* list to MUSERss only	❒
		pcAnywhere Encryption	pcAnywhere is set to use 128-bit key "Symmetric" encryption level. (Upgrades only)	❒
		pcAnywhere Audit Trails	pcAnywhere's "Event Logging" is set to log activities. (Upgrades only)	❒
	User Authentication	NT Authentication	NT Users should be mapped to MUSE Users.	❒
			"Allow Only NT Authentication" option is installed*	❒
		Logout or Lockout Screen Savers	All workstations are configured to use "Logout Screen Saver" or "Lockout Screen Saver."	❒
Accounting & Tracking	NT Event Log	Audit Policy	The NT utility "Audit Policy" is set on MUSE Sever and all workstations to log certain events.	❒
	Audit Trails	Editor Security	Enable the Change Log	❒
	Secure Configuration	Remote Query	'Remote Query' feature is disabled.	❒
		Temporary Device	'Temporary Device' feature is disabled.	❒
Web Encryption & Logging	MUSE Web	SSL Encryption	MUSE file server is set to use SSL to force 128-bit encryption. (See 2003934-001)	❒
		SSL Logging	MUSE file server is set to use IIS to log MUSE Web activities.	❒
		Browser	All browsers that access MUSE Web are updated to use "High Encryption Pack" (128-bit encryption.)	❒
	Anti Virus	Anti Virus Software Configuration	Anti-virus software is installed and properly configured on MUSE file server and all workstations.	❒

* Enabling of this feature requires the assistance of the Jupiter On-Line Support Center. Please dial 1-800-558-7044 to request assistance with activating this feature.

MUSE Features Which Require Policies/Procedures

The table below contains MUSE features that will require policies and procedures development to achieve security compliance.

Policies and Procedures Required for HIPAA & FDA Security Compliance	
MUSE Feature	Policy/Procedure
HL7 Device	❒
COMPUTER Device	❒
MUSE API	❒
Buffer Server	❒
SDLC	❒

Policies and Procedures Required for FDA Security Compliance	
Feature	Policy/Procedure
Require Technicians to enter ID Number at cart when taking the ECG	❒

Access Control Security

The MUSE system has two default users, MUSEAdmin and MUSEBkgnd. This section describes how to change the passwords of these default users to increase the level of access control security on your system.

You can configure your MUSE system to one of two levels of security. Decide what level of security you want for your MUSE system after reading and understanding the information in this section. Determine how the security features available on the MUSE system will work best in combination with your policies and procedures to help you achieve HIPAA compilance.

Mid Level Security

The following table describes how to set up your MUSE system for mid level system access control security.

User Name	Password
MUSEAdmin	Change password as described in "Changing the MUSE Accounts Passwords" on page 7 and tell GE Healthcare Tech Support the new password. (Call 1-800-558-7044)
MUSEBkgnd	Change password as described in "Changing the MUSE Accounts Passwords" on page 7 and tell GE Healthcare Tech Support the new password. (Call 1-800-558-7044)

NOTE: GE Tech Support uses the MUSEAdmin user name and password to log into MUSE systems remotely.

High Level Security

The following table describes how to set up your MUSE system for high level system security.

Name	Password
MUSEAdmin	Change password as described in "Changing the MUSE Accounts Passwords" on page 7 and DO NOT SHARE THE PASSWORD with GE Healthcare Tech Support.
MUSEBkgnd	Change password as described in "Changing the MUSE Accounts Passwords" on page 7 and DO NOT SHARE THE PASSWORD with GE Healthcare Tech Support.

NOTE: Not sharing these passwords with GE Healthcare Tech Support may result in delays if remote service support is needed.

Changing MUSE Service Accounts

The MUSE service accounts are integral to the correct operation of the MUSE system. The following table identifies the default accounts:

Default Account	Description
MUSEAdmin	MUSE administrator account. Used by the MUSE application to perform functions critical to the system operation. Also used by MUSE Tech Support to help troubleshoot and maintain the system.
MUSEBkgnd	MUSE background account. Used to run the MUSE services.

Changing the MUSE Accounts Passwords

1. Login to the Windows server as the user that you want to change the password for.
2. Press **Ctrl** + **Alt** + **Delete**.
3. Choose *Change Password...* from the *Windows Security* dialog.
4. Enter the current password into the *Old Password* field.
5. Enter the new password into the *New Password* field.
6. Enter the new password again into the *Confirm New Password* field.
7. Click *OK*.
8. When the message *Your password has been changed* appears, click *OK*.

NOTE

If the MUSE server, HIS Interface, and MUSE clients are all using the same Windows domain MUSEBkgnd account to start services, the previous steps need to only be performed once. If using local Windows accounts (not recommended), the password will have to be changed on each computer where the account exists.

What you do afterwards depends on which passwords you changed:

- If you changed the password for the MUSE administrative account, you are done.
- If you changed the password for the MUSE background account, you need to re-install the MUSE services. Continue to "Re-Installing the MUSE Services" on page 8.

Re-Installing the MUSE Services

Windows stores the Windows account name and password of the MUSE background account with any service registration associated with that account. Therefore, if you change the Windows account name or password, you also need to re-install the MUSE services so they can be re-registered with the new Windows account and password.

1. Open a *Command Prompt* window on the MUSE file server.
2. Type the following command and press **Enter**.

   cvsinst domain\account password d:\vol000\system\sysinf\services.asc

3. When you receive a message stating that the services have been re-installed, close the *Command Prompt* window and restart the **CV_SCM** service.
4. If there is a HIS Interface, repeat steps 1-3 on the HIS Interface.
5. If there are any MUSE clients with modems defined on them, the modem services will have to be reinstalled on them. Refer to 2002783-012 for instructions on installing modem services.
6. Determine whether the MACCRA service is installed and running and do one of the following.
   - If the MACCRA service is not installed, you are done changing the MUSE account password.
   - If the MACCRA service is installed, continue to "Changing the MACCRA Service" on page 8.

Changing the MACCRA Service

The MACCRA service is used by several MUSE options, such as MUSE Web and CV Web. If you change the MUSE background account name or password, use the following procedure to modify the MACCRA service.

1. In the services list, locate the MACCRA service and open its *Properties*.
2. On the *MACCRA Properties* window, select the *Log On* tab.
3. Make sure the *This account* option is selected.
4. Enter the Windows domain and account name of the MUSE background account in the *This account* field.
5. Enter the account's password in both the *Password* and *Confirm Password* fields.
6. Click *OK*.
7. Restart the service for the changes to take effect.

User Authentication

NT Authentication vs. MUSE Authentication

The MUSE system has supported NT Authentication since it's first release on the Microsoft Windows NT platform with Version 005A. Using NT Authentication on a MUSE workstation not only eliminates a second logon using MUSE Authentication, but also supports a higher level of security as is recommended to meet HIPAA compliance standards.

Since many facilities have yet to configure their MUSE system users as NT users, the MUSE 005E system will continue to support MUSE Authentication* logon. In MUSE 005E, as in previous Version 005 releases, NT workstation nodes can be configured to use either NT Authentication or MUSE Authentication. Some facilities still use MUSE Authorization on all MUSE nodes, but some have switched to using NT Authentication on at least some nodes, if not all. The transition to NT Authentication on all nodes (i.e. pure NT Authentication mode) requires that all MUSE users are assigned NT user names and passwords, and that their NT user names are mapped to their respective MUSE user names. See "MUSE Information System Operator's Manual" for details. The scope of the NT users setup is tied to the number of MUSE users, and for some larger facilities, the transition from MUSE to NT Authentication may occur over a period of time. When all NT users setup is complete, the MUSE system can be configured to force NT Authentication.

Force NT Authentication

The MUSE system supports a new feature which forces NT Authentication.

NOTE TO SERVICE:
The Options Installer refers to this feature as "Allow Only NT Authentication."

This feature is disabled by default and should only be enabled when your MUSE system is ready for pure NT Authentication mode as described above. (The "Checklist for MUSE Security Features" on page 4 also documents the prerequisites for turning on this feature.) This new feature forces all MUSE workstations to use NT Authentication, regardless of their original authentication setting. Once this feature is enabled, MUSE Authentication is disabled across the entire MUSE system.

To enable this new feature on the MUSE system, contact the Jupiter On-Line Support Center at 1-800-558-7044. There is no additional charge for enabling this feature.

* "MUSE Authentication" refers to logon via the MUSE *Authorization* window.

Unattended Workstation Security

There are two options available to you for setting up logout/lockout security on workstations which are left unattended for a specified amount of time. The two options are:

1. Logout. When workstation is inactive (no mouse or keyboard input) for the specified amount of time, the current user is logged off Windows NT and the MUSE session is ended.
2. Lockout. When workstation is inactive for the specified amount of time, the screen saver selected in the *Control Panel* is activated.

The table below summarizes these two options for unattended workstation security. Be sure you understand how each option impacts the user before choosing one of these options. Inform all system users about how the unattended workstation security option affects their use of the system.

Table 2. Differences Between the Two Options for Unattended Workstation Security

Item	Logout Screen Saver WINEXIT	Lockout Screen Saver Logon with Password Protected
Access will be terminated after predetermined time of inactivity	Yes	Yes
Require authentication to log back into system	Yes	Yes
Workstation is locked	No	Yes
Users can unlock workstation	N/A	■ Last user ■ Administrator
MUSE application exit	Yes	■ No, if Last user unlocks the workstation ■ Yes, if Administrator unlocks the workstation
Lose unsaved changes	Yes	■ No, if Last user unlocks the workstation ■ Yes, if Administrator unlocks the workstation
* Possibility of locking record that was being edited when screen saver took control.	Yes	■ No, if Last user unlocks the workstation ■ Yes, if Administrator unlocks the workstation

* If a record is locked, a message will be displayed indicating the record is being used by another workstation. The message will display the Node ID of the workstation that has locked the record. To unlock the record, any user can logon the workstation which has locked the record and start MUSE application.

Once you have selected an unattended workstation security option, proceed with the setup.

- To set up the Logout Screen Saver (winexit), go to "Logout Screen Saver" on pages 11 through 15.
- To set up the Lockout Screen Saver (Logon with Password Protected). go to "Lockout Screen Saver" on page 16.

Logout Screen Saver

The MUSE system includes the winexit.scr application which, when properly configured, will logout the current user after the specified amount of time of inactivity, displaying the Windows logon for the next user. This feature can be used to provide additional security for unattended workstations on the MUSE system.

Giving Non-Administrators Permission to Use WINEXIT Screen Saver

In order for non-administrators to be able to use the WINEXIT screen saver, the administrator must add *Set Value* and *Create Subkey* permissions for the group *Everyone* on the following registry key:

HKEY_Local_Machine\Software\Microsoft\Windows NT\CurrentVersion\IniFileMappings\Control.ini

Windows 2000 Workstations

Repeat the following steps at each workstation running Windows 2000.

1. Log onto the workstation as administrator.
2. Click *Start* → *Run...* .
3. Type **REGEDT32.EXE** and click *OK*.
4. Open the following key:

   HKEY_Local_Machine\Software\Microsoft\Windows NT\CurrentVersion\IniFileMappings\Control.ini

5. Click *Security* → *Permissions...* .

6. Click *Advanced*.
7. Under *Name*, select *Users* and click *View/Edit*.
8. Click to select the *Set Value* and *Create Subkey* checkboxes.
9. Click *OK* twice to save your changes.
10. Select *Registry* → *Exit* to exit the *Registry Editor*.
11. Restart the workstation.

Windows XP Workstations

Repeat the following steps at each workstation running Windows XP.

1. Log onto the workstation as administrator.
2. Click *Start* → *Run...* .
3. Type **REGEDT32.EXE** and click *OK*.
4. Right-click the following key:

   HKEY_Local_Machine\Software\Microsoft\Windows NT\CurrentVersion\IniFileMappings\Control.ini

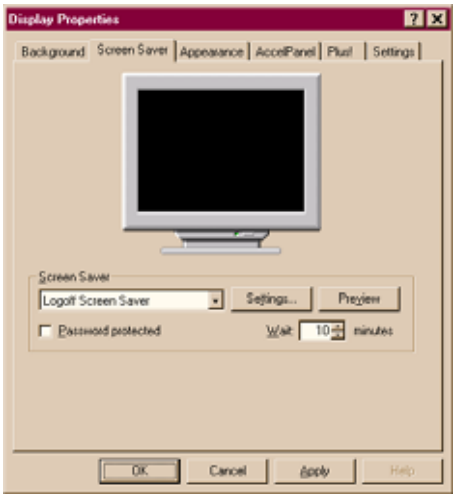
5. Click *Permissions...* from the pop up menu.
6. Click *Advanced*.
7. Highlight *Users* under the *Name* column in the *Permissions Entries* frame.
8. Click the *Edit* button.
9. Check the *Allow* boxes for *Set Value* and for *Create Subkey*.
10. Click *OK*.
11. Click *OK*.
12. Click *OK*.
13. Close the Registry.
14. Restart the workstation.

Existing Windows Users

Any users who are already setup as Windows Users, must log onto each workstation and select the *Logoff Screen Saver* in the *Control Panel*.

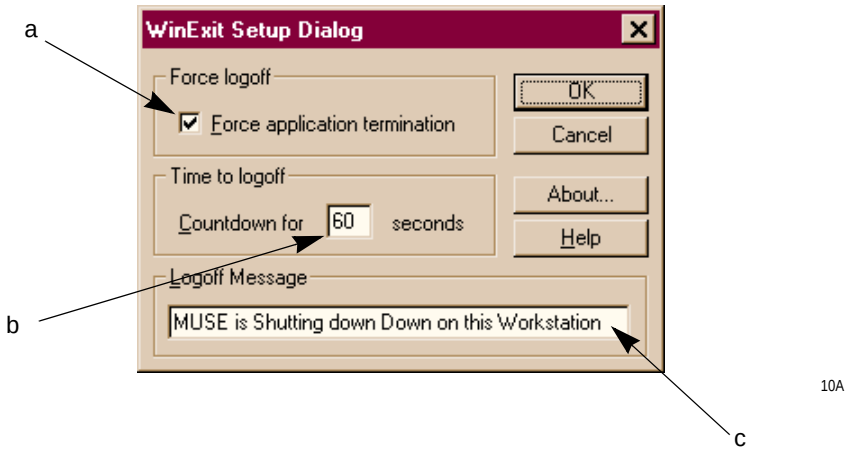
1. Log into Windows using your Windows username and password.
2. Select *Start* → *Programs* → *Command Prompt*.
3. Type the following in the *Command Prompt* window to copy the **winexit.scr** file the the **system32** directory:
   - For Windows 2000 and Windows XP workstations:

     copy [**Space**] **c:\mei\w2kexit.scr** [**Space**] **%SystemRoot%\system32\winexit.scr** and press **Enter**
4. Select *Start* → *Settings* → *Control Panel* → *Display* → *Screen Saver*.
5. Select *Logoff Screen Saver* in the *Screen Saver* list.



9A

6. Select the desired time in the *Wait* list.
7. Click the *Settings...* button.
   a. Select *Force application termination*.
   b. Set **60** seconds for countdown to application termination.
   c. Type **MUSE is Shutting down on this Workstation** in the *Logoff Message* field.



8. Click *OK* to save your settings in the *WinExit Setup Dialog* window.
9. Click *Apply* in the *Display Properties* window.
10. Click *OK* in the *Display Properties* window.
11. Press **Ctrl** + **Alt** + **Delete** and click *Logoff...* button.
12. Click *OK* when the prompted that *This will end your Windows Session*.
13. Each user must repeat steps 1 through 10 on each on each workstation.

New Windows Users

The following procedure, will ensure that all new users added to the Windows User list in the future will automatically be set up with the logoff screen saver. These steps must be repeated at each workstation.

1. Log on as an Administrator.
2. Select *Start* → *Programs* → *Command Prompt*.
3. Type the following in the *Command Prompt* window to copy the **winexit.scr** file the the **system32** directory:
   - For Windows 2000 and Windows XP workstations:
     copy [**Space**] **c:\mei\w2kexit.scr** [**Space**] **%SystemRoot%\system32\winexit.scr** and press **Enter**

4. With the *Command Prompt* window still open, make a backup copy of the **Ntuser.dat** file by typing the following:
   - Windows 2000 or Windows XP Workstations:

     echo [**Space**] **F** [**Space**] **|** [**Space**] **xcopy** [**Space**] **/h** [**Space**] **"C:\documents and settings\default** [**Space**] **user\ntuser.dat"** [**Space**] **"C:\documents and settings\default** [**Space**] **user\ntuserbak.dat"** and press **Enter**
5. Close the *Command Prompt* window.
6. Click *Start* → *Run...* .
7. Type **regedt32.exe** and click *OK*.
8. Click the *HKEY_USERS on Local Machine* window.
9. Click the *HKEY_USERS* registry key, and then click *Registry*.
10. Then *Load Hive...* from the menu.
11. Click the Ntuser.dat file that is located in the following path:
    - Windows 2000 or Windows XP Workstations:

      Documents and Settings\Default User\Ntuser.dat
12. Enter **temp_defaultuser** in the *Key Name* dialog box that is displayed and click *OK*.
13. Double-click and expand *temp_defaultuser*.
14. Double-click and expand *Control Panel*.
15. Add a key:
    - Select *Edit* → *Add Key* (Windows 2000)
    - Select *Edit* → *New* → *Key* (Windows XP)
16. Enter **Screen Saver.Logoff** in the *Key Name* field and click *OK* (if applicable). A class value is not required.
17. Click *Desktop* (under *temp_defaultuser /Control Panel*).
18. In the right window, change the value in *ScreenSaveActive* to **1**.
19. Change the value in *ScreenSaverIsSecure* to zero (0).

    NOTE

    By default, this value is already zero (0).
20. Change the value in *ScreenSaveTimeOut* to desired time. (This value is in seconds.)
21. Change the value in *Scrnsave.exe* to **%SystemRoot%\system32\winexit.scr**
22. Click the *temp_defaultuser hive*
23. Unload the hive:
    - Click *Registry* → *Unload Hive* and click *Yes* to the warning (Windows 2000)
    - Click *File* → *Unload Hive* and click *Yes* to the warning (Windows XP)

    The changes will be saved in:
    Documents and Settings\Default User\ntuser.dat

Lockout Screen Saver

An alternative way of setting up system security is to set up individual users' screen savers with the "Password Protected" option enabled.

Existing Windows Users

The steps below apply only to setting up password protection for existing NT users' screen savers.

1. Log on with the name and password of the user you are setting up.
2. Select *Start* → *Settings* → *Control Panel*.
3. Double-click *Display*.
4. Click the *Screen Saver* tab.
5. Select *Password protected* checkbox.
6. Click *Apply*.
7. Click *OK*.
8. Close the *Control Panel*.

New Windows Users

The following procedure, will ensure that all new users added to the Windows User list in the future will automatically be set up with the lock out Password Protect screen saver. These steps must be repeated by the Administrator at each workstation.

1. Log on as an Administrator.
2. Select *Start* → *Programs* → *Command Prompt*.

3. Make a backup copy of the **Ntuser.dat** file by typing the following:
   - For Windows NT workstations:
     copy [**Space**] **"c:\winnt\profiles\default** [**Space**] **user\ntuser.dat"** [**Space**] **"c:\winnt\profiles\default** [**Space**] **user\ntuserbak.dat"** and press **Enter**
   - For Windows 2000 or Windows XP workstations:
     echo [**Space**] **F** [**Space**] **|** [**Space**] **xcopy** [**Space**] **/h** [**Space**] **"c:\documents** [**Space**] **and** [**Space**] **settings\default** [**Space**] **user\ntuserbak.dat"** and press **Enter**
4. Close the *Command Prompt* window.
5. Click *Start* → *Run...* .
6. Type **regedt32.exe** and click *OK*.
7. Click the *HKEY_USERS on Local Machine* window.
8. Click the *HKEY_USERS* registry key, and then click *Registry*.
9. Then *Load Hive...* from the menu.
10. Click the *Ntuser.dat* file that is located in the following path:
    - *Winnt\Profiles\Default User\Ntuser.dat* (Windows NT)
    - *Documents and Settings\Default User\Ntuser.dat* (Windows 2000 & XP)
11. Enter **temp_defaultuser** in the *Key Name* dialog box that is displayed and click *OK*.
12. Double-click and expand *temp_defaultuser*.
13. Double-click and expand *Control Panel*.
14. Select *Edit* → *Add Key*.
15. Enter **Screen Saver.Logoff** *Key Name* field and click *OK*. (A class value is not required.)
16. Click *Desktop* (under *temp_defaultuser /Control Panel*).
17. In the right window, change the value in *ScreenSaveActive* to **1**.
18. Change the value in *ScreenSaverIsSecure* to **1**.

    NOTE
    By default, this value is zero (0).
19. Change the value in *ScreenSaveTimeOut* to desired time. (This value is in seconds.)
20. Change the value in *Scrnsave.exe* to **c:\winnt\system32\logon.scr**
21. Click the *temp_defaultuser hive*
22. Click *Registry* → *Unload Hive*.

    The changes will be saved in:
    Winnt\Profiles\Default User\ntuser.dat (Windows NT)

    documents and settings\Default User\ntuser.dat
    (Windows 2000 or Windows XP)

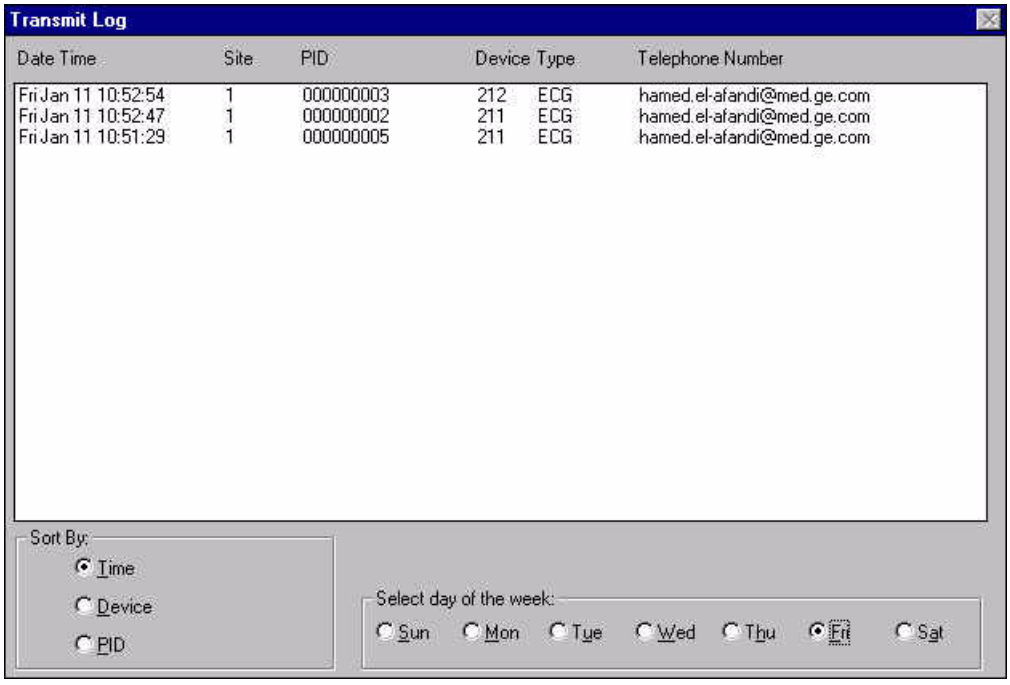
Accounting/Logging

Transmit Log & Status Viewer (Outbound Events)

The MUSE system logs the following outbound events:

Network Printing to Postscript and PCL printers
Fax
CSI
email messaging
MEI Thermal
MUSE Word Report
Floppy Disk Acquisition

These outbound events can be viewed in *System Status* → *Transmit Log*.



MD1350-131A

Each record in the *Transmit Log* will contain the following fields.

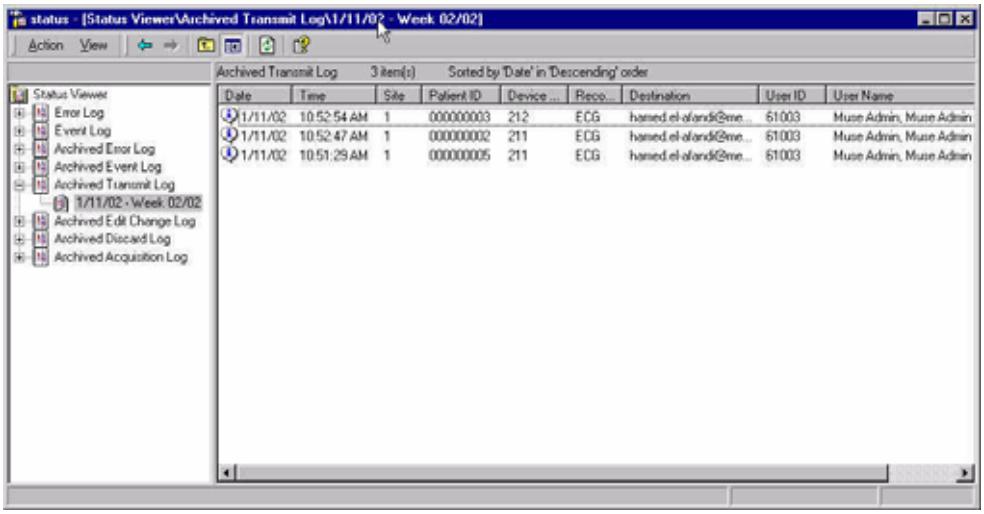
Patient ID
Patient Name
Acquisition Date/Time
Order Number
Task
Station
Spool File Name
Output File

Destination Field (Device)
Logged User ID
Logged User Name
Date/time of transmission

NOTE

The MUSE system does not log HL7 and computer events. Policies and procedures must be established to track the HL7 and computer device events.

The outbound events can also be viewed with the MUSE Status Viewer. At the file server from the Windows NT desktop, select *Start* → *Programs* → *MUSE CV Information* → *Status Viewer*.



MD1350-132A

Change Log

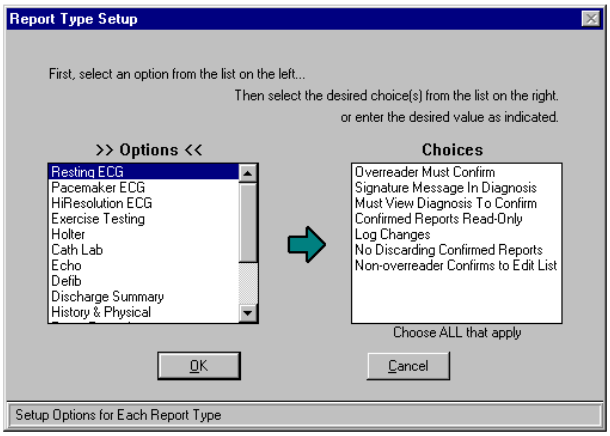
NOTE

Prior to version 005D software this selection logged changes to confirmed reports only. With version 005D software, changes to both confirmed as well as unconfirmed reports are logged.

Setting Up a Change Log

The MUSE system can be configured to log any changes made to a patient report. The feature bit must be turned on as follows:

1. Select *System* → *System Setup* → *Options* → *Report Type Options*.



11A

2. Click on a data type in the *Options* list and select *Log Changes* in the *Choices* list.
3. Repeat step 2 for each data type.

Viewing and Printing a Change Log

1. The *Change Log* can be viewed from within a patient report by selecting *Test Data* → *Change Log*.
2. To print the *Change Log*, click *Print* in the *Change Log* window.

Logging of System Security Events

The MUSE system can be configured to log system security events to the *NT Event Log*. At each file server and workstation, repeat the following steps to set up this audit.

1. Click *Start* → *Programs* → *Administrative Tools* → *User Manager*
2. Select *Policies* → *Audit*.
3. Select the *Audit These Events* option button.
4. Select the checkboxes indicated in the table below.

Event	Success	Failure
Logon and Logoff	✓	✓
File and Object Access		✓
Use of User Rights		✓
User and Group Management		✓
Security Policy Changes	✓	✓
Restart, Shutdown, and System	✓	✓
Process Tracking		✓

5. Click *OK* to save your changes.

Archived Log Files

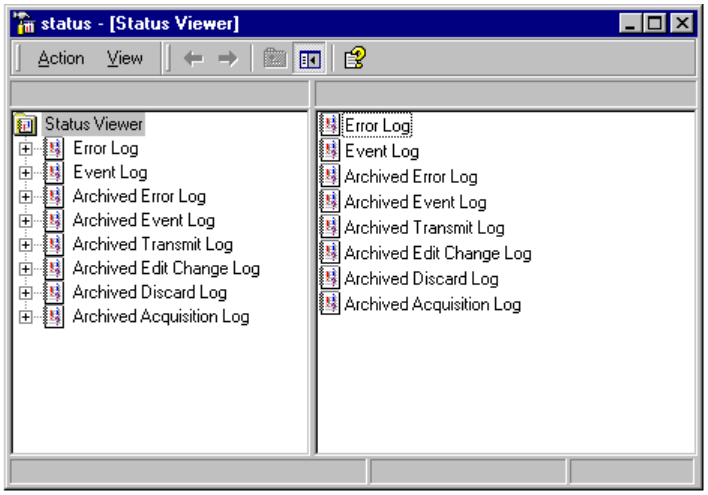
Once a week, the MUSE system automatically archives the following log files.

Log File	Path
Archived Transmission Log	vol000\system\ArchLog\Transmit\Xmityyww.btr
Archived Edit Change Log	vol000\system\ArchLog\EditChg\Echgyyww.btr
Archived Discard Log	vol000\system\ArchLog\Discard\Dscryyww.btr
Archived Error Log	vol000\system\ArchLog\Error\Erryyww.btr
Archived Event Log	vol000\system\ArchLog\Event\Evtyyww.btr
Archived Acquisition Log	vol000\system\ArchLog\Acq\Acqyyww.btr

Where: yy = year
ww = Julian week (Day of year / 7)

These files can be viewed using *Status Viewer* as follows:

1. From the desktop, click *Start* → *Programs* → *MUSE CV Information System* → *Status Viewer*.



12A

NOTE

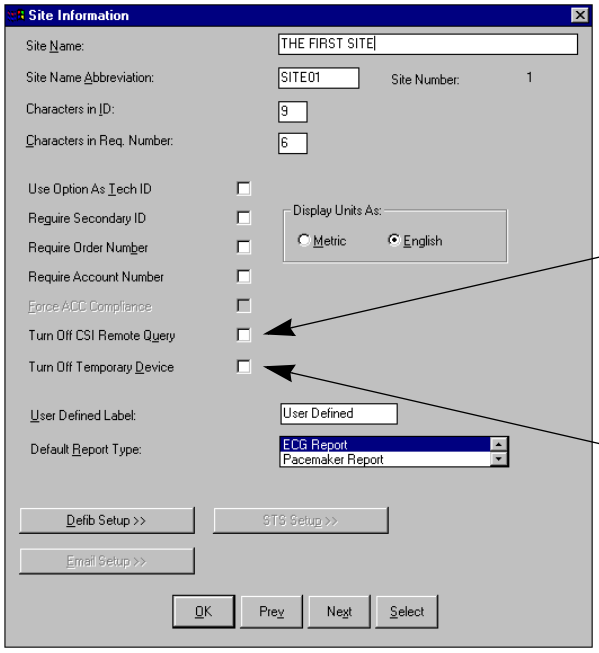
These files are viewable in *Status Viewer* only when they are located in the paths shown above. If you archive these files to another location, they must be copied back to their original locations in order to be viewed with *Status Viewer.*

Disabling Remote Query & Temporary Devices

The MUSE system does not log printing of reports to devices via remote query or to temporary devices. With version 005D software, however, you can disable the sending of patient reports to remote query or to temporary devices to enhance the security of patient reports.

To prevent remote query via CSI modem and/or printing to a temporary device, log into the system as a *System Owner* or *Site Manager* and follow the steps below.

1. Select *System* → *System Setup* → *Select List* → *Sites*.



2. To disable remote query, select the *Turn Off CSI Remote Query* checkbox.
3. To disable printing to temporary devices, select the *Turn Off Temporary Device* checkbox.
4. Click *OK*.
5. Repeat for each site on the system.

MUSE Web

IIS 4.0 Option Pack is installed on the MUSE Web server. In order to access the MUSE Web, the user must have their browser configured for 128-bit encryption.

For detailed procedures, see “MUSE CV Web Server Instruction Guide to Enabling SSL” (PN 2003934-001).

Configure IIS to Log Web Site Activity on MUSE Web

MUSE file server should be configured to enable logging web site activity as follows:

1. Right-click *My Computer* and select *Manage*.
2. Expand *Services & Application* in the list found in the *Tree* list (left panel).
3. Highlight *Internet Information Services*.
4. Right-click on *MUSE CV Web Site* and select *Properties*.
5. Ensure that *Enable Logging* is checked in the *Web Site* tab.
6. For *Active log format*, make sure it is *W3C Extended Log File Format*.
7. Select *Properties...* .
   - Select the *General Properties* tab.
   - Select *Weekly* for *New Log Time Period*
   - Make sure *Log file directory* is **%WinDir%\System32\LogFiles**
   - Select *Extended Properties* tab
   - Add/delete/verify checkmarks to obtain the following *Extended Logging Options*.

✓	*Date*	✓	*URI Query*
✓	*Time*		*Http Status*
✓	*Client IP Address*		*Win32 Status*
✓	*User Name*		*Bytes Sent*
	Service Name		*Bytes Received*
✓	*Server Name*		*Time Taken*
✓	*Server IP*		*Protocol Version*
	Server Port		*User Agent*
✓	*Method*		*Cookie*
			Referrer

   - Click *OK* in this window and in the next.

Setting Up Client Browser for 128-bit Encryption

MUSE Web server will allow only 128-bit encryption accesses. Users will need to update their Internet Explorer (IE) 5.0 or 6.0 to have “High Encryption Pack” installed.

NOTE

The High Encryption Pack can be downloaded from the Microsoft web site.

The steps below describe how to determine the IE encryption level.

1. Start Internet Explorer.
2. Select *Help* → *About Internet Explorer*.
3. If *Cipher Strength* is less than 128-bit, you will need to install *High Encryption Pack*.

Anti-Virus Software

Anti-virus software is a requirement for HIPAA compliance. GE has tested the system with Norton Anti-Virus Corporate Edition and McAfee NetSheild. Either of these two virus protections software applications can be installed on the MUSE system without affecting function or performance.

This anti-virus software is not provided with the MUSE system and it remains the customer's responsibility to acquire and install anti-virus software on their system per the recommendations of the manufacturer of the anti-virus software.

See the MUSE Pre-Installation Manual (PN 2020285-025) for GE's recommended anti-virus software configuration settings. When properly used, anti-virus software can protect the MUSE system from virus infection and the subsequent data corruption which can result from a virus infection. However, if improperly configured, anti-virus software can cause system degradation.

For your notes

A Appendix A – HIPAA Overview

For your notes

HIPAA Introduction

The future of health care in the United States changed on August 2, 1996 when the Health Insurance Portability and Accountability Act (HIPAA) became law. The complex and far-reaching federal legislation significantly affects every person and organization involved in health care. HIPAA rules spell out standards and requirements for protecting the confidentiality, security, and integrity of all health information.

HIPAA Law Overview

The primary goals of HIPAA are quantification of consumer health care rights along with improved privacy and security of medical records. The two main components of HIPAA are Health Care Portability and Administrative Simplification. The Health Care Portability legislation became effective in 1996. The Portability part of HIPAA is well understood and was successfully implemented by the US government and the medical industry in 1996 and 1997. The Portability legislation guarantees the following rights to health care consumers:

- Improved availability and accessibility of health insurance
- Guaranteed right of portability and continuity of health insurance coverage for individuals and groups
- Prohibits discrimination based on health status

HIPAA's Administrative Simplification provision is composed of four parts and involves these health care issues:

- Standardization of electronic transfers of patient health, administrative and financial data
- Privacy and security standards protecting the confidentiality and integrity of health information
- Unique health identifiers for individuals, employers, health plans and health care providers

Each part will eventually produce a variety of rules and standards. Many of the rules and standards are under development. As the rules and standards are finalized and become law they will have different compliance deadlines. The four parts of Administrative Simplification are:

1. Electronic Health Transactions Standards
2. Unique Identifiers
3. Security & Electronic Signature Standards
4. Privacy & Confidentiality Standards

HIPAA's complexity confuses customers. Even the HIPAA name causes confusion. Recently the meaning of the moniker HIPAA changed. Initially HIPAA referred to all parts of the legislation. Current usage narrows HIPAA's meaning to the rules generated from the Administrative Simplification subsection. GE Medical Systems *Information Technologies* follows common usage and unless otherwise noted HIPAA refers to the rules developed from the Administrative Simplification subsection.

The main components of HIPAA and their relationships are presented in Figure 1 below.

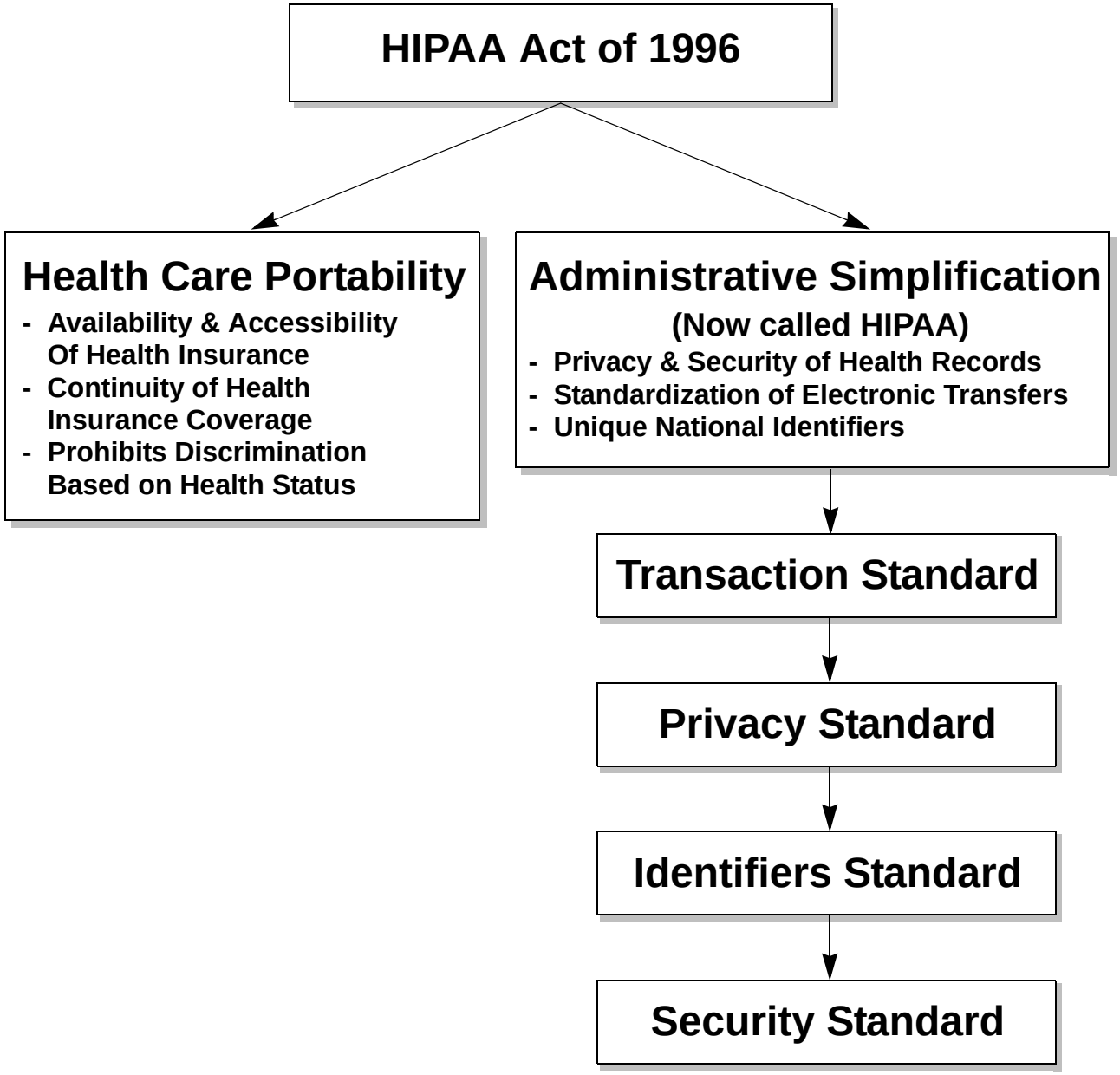


Figure 1. HIPAA Components

The HIPAA component with the greatest impact on GEMS-IT customers is the Privacy Standard. The Privacy Standard is defined in the Administrative Simplification subsection. The Final Version of the Privacy Standard, (Standards for Privacy of Individually Identifiable Health Information, 45 CFR Parts 160 and 164), was published in the Federal Register on December 20, 2000.

The HIPAA implementation and enforcement schedule spans several years. The Privacy Standard becomes enforceable on April 14, 2003. Table 1 summarizes the HHS release status and timetable for the HIPAA rules.

Table 1. HIPAA Rules and Rulemaking Timetable

Standard	Publication Date	Final Ruling	Required Compliance
1. Insurance Portability	Aug 02, 1996	Aug 02, 1996	Jul 01, 1997
2. Electronic Transactions & Code Sets*	May 07, 1998	Aug 17,2000	Oct 16, 2003
3. Privacy & Confidentiality	Nov 03, 1999	Dec 28, 2000	Apr 14, 2003
4. National Provider Identifier	May 7, 1998	Expected 2002	–
5. National Employer Identifier	Jun 16, 1998	Expected 2002	–
6. Security	Aug 12, 1998	Expected 2002	–
7. National Health Plan Identifier	In Development	–	–
8. Claims Enforcement Procedures	In Development	–	–
9. National Individual Identifier **	Withdrawn	–	–

* In January, 2002 the Bush Administration extended the deadline for the 'Electronic Transactions & Code Sets' from Oct 2002 until October 2003.

** Although the HIPAA law called for a unique health identifier for individuals, HHS and Congress indefinitely postponed any effort to develop such a standard. (HHS Fact Sheet, Administrative Simplification, 2001)

Privacy and Confidentiality

The Final Rule for Privacy was published December 28, 2000. Compliance will be required on April 14, 2003 for most covered entities. In general, privacy is about who has the right to access personally identifiable health information. The rule covers all individually identifiable health information in the hands of covered entities, regardless of whether the information is or has been in electronic form. The Privacy standards limit the non-consensual use and release of private health information; give patients new rights to access their medical records and the right to know who else accessed them; restrict most disclosure of health information to the minimum needed for the intended purpose; establish new criminal and civil sanctions for improper use or disclosure; establish new requirements for access to records by researchers and others.

The Privacy and Confidentiality regulations incorporate five basic patient rights related to health care information:

- Consumer Control: The regulation provides consumers with critical new rights to control the release of their medical information
- Boundaries: With few exceptions, an individual's health care information should be used for health purposes only, including treatment and payment.
- Accountability: Under HIPAA, for the first time, there will be specific federal penalties if a patient's right to privacy is violated.
- Public Responsibility: The new standards reflect the need to balance privacy protections with the public responsibility to support such national priorities as protecting public health, conducting medical research, improving the quality of care, and fighting health care fraud and abuse.
- Security: It is the responsibility of organizations that are entrusted with health information to protect it against deliberate or inadvertent misuse or disclosure.

Electronic Health Transactions and Code Sets Standards

Health care organizations routinely store and transmit medical information in electronic format. Electronic medical information is manipulated through a wide variety of encoding schemes and formats. Standard electronic data interchange improves the efficiency of health care delivery. National standards make it easier for health plans, doctors, hospitals and other health care providers to process claims and other transactions. (HHS Fact Sheet, Administrative Simplification, 2001) The government and the medical industry perceive standardized representations of routine medical data as beneficial for all parties involved. The Transactions Standards mandates use of standardized electronic formats developed by ANSI, the American National Standards Institute. The Code Set Standards require use of the most commonly used medical terminology code sets. Final standards for electronic transactions and code sets were released in Aug 2000. The original compliance deadline of October 2002 was extended to October 2003.

The Transactions Standards specify the format and content of the following medical transactions:

- Health claims or equivalent encounter information transfer
- Health claims attachments
- Enrollment and disenrollment actions in a health plan
- Eligibility status in a health plan
- Health care payment and remittance advice
- Health plan premium payments
- First report of injury
- Health claim status
- Referral certification and authorization

The Health organizations must adopt standard code sets for all health transactions. Code sets are alphanumeric identifiers representing medical data. Medical coding systems describe diseases, injuries, and other health problems, as well as causes, symptoms and actions taken. All parties exchanging medical transactions must generate and accept the same coding. Consistent coding reduces mistakes, duplication of effort and costs. HIPAA specifies the following commonly used code sets:

1. International Classification of Diseases, 9th Edition, Clinical Modification, (ICD-9-CM), Vols 1, 2, 3
2. National Drug Codes (NDC)
3. Code on Dental Procedures and Nomenclature,
4. Health Care Financing Administration Common Procedure Coding System (HCPCS)
5. Current Procedural Terminology, Fourth Edition (CPT-4),

The Transactions Standards regulate information related to health insurance status and remittance. GEMS-IT cardiology information system products are clinical systems and rarely (if ever) process the health insurance and remittance information affected by the Transactions Standards. The GE Medical Systems *Information*

Technologies cardiology information system products are not affected by the Transactions Standards.

The Code Set Standards regulate use of clinical medical information. The Code Set Standards may affect GE Medical Systems *Information Technologies* cardiology equipment. The cardiology equipment may need to support input of code set values when test information is acquired.

HIPAA Compliance

HIPAA compliance is achieved through a combination of changes to ‘policy and procedure’ and the purchase of HIPAA enhanced hardware, software, and other technologies. No product can independently confer HIPAA compliance rather the product must fit into a customer specific HIPAA compliance scheme. Technology updates and ‘policy and procedure’ changes are pieced together by customers into a unique and site specific HIPAA compliance solution. The precise mechanisms for achieving HIPAA compliance are left to the covered entities. HIPAA does not mandate specific vendor equipment or mechanisms for achieving compliance. The HIPAA implementers are free to create the systems that enable compliance as they see fit. The HIPAA implementers must decide how much of the compliance will come from new and upgraded technology versus the amount achieved via changing ‘policy and procedure’. HIPAA expects a majority of the compliance can be achieved through ‘policy and procedure’ changes and the remaining compliance achieved via deployment of new and updated technology. The authors of the HIPAA provided guidance concerning policy and procedure in the Federal Register (Dec 28, 2000):

Policy and Procedures

The rule requires that covered entities develop and document policies and procedures with respect to protected health information to establish and maintain compliance with the regulation. Through the standards, requirements, and implementation specifications, we are proposing a framework for developing and documenting privacy policies and procedures rather than adopting a rigid, prescriptive approach to accommodate entities of different sizes, type of activities, and business practices. Small providers will be able to develop more limited policies and procedures under the rule, than will large providers and health plans, based on the volume of protected health information. We also expect that provider and health plan associations will develop model policies and procedures for their members, which will reduce the burden on small businesses.

The myriad of HIPAA compliance solutions presents a difficult challenge to customers. Customers want to stay focused on their primary job of providing quality health care. Customers expect vendors to provide detailed HIPAA guidance tailored to the customer’s unique security needs and health care environment.

Achieving HIPAA Compliance

Achieving HIPAA compliance is a top-down process of learning, planning and implementing. Health care institutions must become intimately familiar with HIPAA rules. The HIPAA implementer must conduct a self-analysis to determine how HIPAA fits into their unique situation. The HIPAA rules must be broken down into understandable categories and tasks. Many internal stakeholders must be consulted in order to ensure full compliance. Once a plan is in place then the HIPAA-enabling technology is purchased and the 'policy and procedure' documents created. The last stage is integration and deployment of all the HIPAA mechanisms followed by an audit, ensuring compliance. The HIPAA compliance effort requires strong commitment and detailed planning. The American Health Information Management Association (AHIMA) created the HIPAA Privacy Checklist (2001) to guide to HIPAA implementers:

- Get management commitment
- Appoint HIPAA team
- Perform GAP analysis
- Understand current security policy and IT practices
- Perform risk analysis
- Draft required policies, procedures, and consents
- Obtain needed HIPAA-enabling technology
- Deploy 'policy and procedure' and technology
- Audit HIPAA policies, test privacy measures, test security measures

GE Medical Systems *Information Technologies* can advise and add value at each phase of HIPAA implementation.

References

General Electric Medical Systems HIPAA Overview:
http://ge.com/hipaa

Dept. of Health and Human Services, Office of the Secretary, (Dec 28, 2000). Standards for Privacy of Individually Identifiable Health Information, Comments and Rules, 1535 pages, Federal Register 45 CRF Parts 160 through 164, p 82783
http://www.hhs.gov/ocr/fedreg.zip

Dept. of Health and Human Services, Office of the Secretary, (Dec 28, 2000). Standards for Privacy of Individually Identifiable Health Information, Rules only 40 pages, Federal Register 45 CRF Parts 160 through 164, p 82783
http://aspe.os.dhhs.gov/admnsimp/final/PvcTxt01.htm

HHS Fact Sheet: Administrative Simplification Under HIPAA: National Standards For Transactions, Security And Privacy. (May 11, 2001). Retrieved from U.S. Department of Health and Human Services Web site:
http://www.hhs.gov/news/press/2001pres/01fshipaa.html

Quarterly Industry HIPAA Survey Results - Summer 2001. (Aug 6, 2001). Retrieved Aug 10, 2001, from Phoenix Health Systems HIPAAdvisory Web site:
http://www.hipaadvisory.com/action/survey/summer01.htm

HHS FAQ Sheet: The Rule Making Process for Administrative Simplification: What Is Taking So Long? (July 2, 1999)
Retrieved from U.S. Department of Health and Human Services Web site:
http://aspe.os.dhhs.gov/admnsimp/8steps.htm

HIPAA Primer, Retrieved Nov 29, 2001,from Phoenix Health Systems HIPAAdvisory Web site:
http://www.hipaadvisory.com/regs/HIPAAprimer1.htm

HIPAA Privacy Checklist, Retrieved Aug 10, 2001, from the American Health Information Management Association Web site:
http://www.ahima.org/journal/pb/01.06.1.html

Information on Microsoft solutions for the healthcare industry and for a copy of Microsoft's HIPAA Technical White Paper.
http://www.microsoft.com/business/health

How HIPAA-Compliant Can Any Technology Be?

By Roy Rada, M.D., Ph.D.
Department of Information Systems
University of Maryland, Baltimore County

American history has witnessed a myriad of compliance activities; some we might point with pride to, such as the 1906 Pure Food and Drug Act, resulting from Dr. Harvey Wiley's efforts to regulate the content of food. However, the role of government in regulating business in the US has often been accompanied by controversy and debate.

HIPAA has proved to be another battleground for compliance. Without going further into the history, politics, law, or ethics of compliance, let's address the seemingly simple question of whether information technology can be compliant with HIPAA.

How many times have you heard a vendor tout 'my technology is HIPAA compliant'? Some providers and payers are demanding to get HIPAA compliant technology. Claims are commonly made by salespeople that their product is HIPAA compliant. What's the scoop here?

Direct compliance with HIPAA's administrative simplification provisions is not practical because the law itself is too indirect. It calls for rules to be developed and enforced by the executive branch of the federal government. Furthermore, the rules are diverse and cover, at least, transactions, privacy, and in proposed-form security.

Transactions Rule

Might an IT vendor rightfully claim to be compliant with the Transactions Rule? 'Transaction' refers in the HIPAA-context to provider-payer transaction. The Transactions Rule calls for compliance with certain standards, particularly X12 formats. A health care provider might want to use information systems that support message formats to payers that are compliant with X12, and a vendor could claim to provide such X12-compliant forms.

This is not to say that the entity buying the technology would have an instant fix to its 'Transactions' compliance problem. The Transactions Rule goes beyond the X12 formats to specify the codes that have to be used inside the fields of the format. Achieving compliance with some coding requirements may entail changes in behavior. However, technology could enforce the use of Transaction Rule formats and codes and thus support compliance with the HIPAA transaction rule.

Privacy Rule

Privacy calls for changes in the way an entity manipulates information. This is largely an administrative rather than a technical issue. However, a technology can support the options for manipulating information and be a vital support of the entity behavior. The technology should support behavior consistent with the Privacy Rule.

The Privacy Rule calls for information systems that represent and audit workflow. Exactly what the workflow should be is not precisely defined. The approach of the

Privacy Rule is like the ISO (the pre-eminent international standards organization) approach to quality in ISO 9000. ISO 9000 says that an organization should be clear in its goals and work consistently to those goals. ISO 9000 does not say what the organization-specific goals should be, but an organization can be certified as ISO 9000 compliant. To be ISO 9000 compliant an organization must document its objectives and document that its activities take it towards its objectives – nothing more. The Privacy Rule goes beyond ISO 9000 in specifying broadly what some of the privacy objectives are but then asks entities to be quality organizations as respect to those objectives.

Entities must document working towards privacy objectives. Certifying compliance for privacy would require an analysis of the organizational manual and the way the organization implemented its manual. An IT tool should help a health care entity have and follow the appropriate organizational manual but the tool would not make the entity HIPAA compliant.

Security Rule

No security rule has been finalized for HIPAA. Yet, security is the topic that comes closest to what an IT vendor feels is the special turf of the vendor. The typical health care entity may be violating various security mandates, such as transmitting information over the Internet in encrypted form. A vendor can provide tools that encrypt messages before sending them across the Internet.

The proposed security rule gives objectives of secure transmissions, reliable authentication, contingency preparations, and much more. However, the proposed rule gives flexibility to organizations in their choice of ways to achieve the objectives and is neutral about particular technologies. The compliance argument about security is not dissimilar to the argument about privacy: when an organization uses a technology in a certain way to reach a certain objective, then the organization will have behaved in a compliant way as regards that HIPAA security objective.

Overall...

The bottom line is that Administrative Simplification is about Administration, and technology can support that administration – but not replace it. An information technology vendor should help its clients understand what parts of HIPAA compliance are supported by the vendor's technology. But it should not claim that the technology is HIPAA compliant.

B Appendix B – Summary of MUSE Security

For your notes

Introduction

The following table is based on a MUSE CV system with 005D software with no MUSE CV Web option. These tables are in direct response to the need for security features in medical systems. We provide these answers to assist you in discovering your risks and in the creation of your mitigation plan. We provide these answers to the best of our knowledge given the requirements and current state of the product.

This document contains a summary of the Legal Requirements of Health Insurance Portability and Accountability Act (HIPAA). It is not intended as legal advice. Every entity must make its own judgment regarding what will be required to enable it to comply with HIPAA. General Electric Company reserves the right to make changes in specifications and features shown herein, or discontinue the product described at any time without notice or obligation. Contact your GE Representative for the most current information.

Background Information	
Enter any description that helps clarify the security context. The security context would include product options, environmental conditions, intended	Unknown
Does the product Capture, Store, or Transmit any Patient identifiable data?	Yes
Identify the architecture that best describes this product:	Client/Server
What Operating System is this product Client based on?	WIN2003
What Operating System is this product based on (or in the case of client/server products -- what is the server)?	WIN2003
Which GSP Platform does the product utilize?	Unknown
Can the product display a customer supplied message on boot up or login?	No
Does the product provide a training mode that allows for training without corrupting the operational data?	No
Network Presence	
Does this product have a communications/network interface (Not including Remote Service)?	Yes
Identify all of the Communications interface that this product has:	
Ethernet	Yes
Token-Ring	No
ATM	No
RF (802.11, blue tooth, other radio)	No
COTS Modem	Yes
Other Modem (eg SDLC)	Yes
Direct Serial	Yes
Other	No
Does this product have a Database?	Btrieve
Identify all of the Services/Protocols the product provides:	
Any Direct Network db Access (JDBC, ODBC, SQL, etc)	Yes
DICOM	Yes
HL7	Yes
XML	Yes
Hill Top	Yes
Unity	No
AdvantageNET	No
PostScript or PCL printers	Yes
SMTP or MAPI	Yes
FAX	Yes
SNMP	Yes
FTP	Yes
Telnet / X windows	No

Share (NFS, SMB, etc)	Yes
Customer Accessible API?	Yes
Other	No
None	No
Identify the modes of Network Communications of Patient Identifiable Data that is supported using the above protocols:	
Send Patient Identifiable Data to other systems	Yes
Receive Patient Identifiable Data from other systems	Yes
Provide a Query interface that other systems can use to extract Patient Identifiable Data	Yes
Does this product have a Web Server?	No
Transactions, Code Sets, and Identifiers	
Identify all of the Code Sets this product sends or receives:	
non-standard equivalents to X12N Transactions (Billing EDI transactions)?	No
standard X12N Transactions (Billing EDI transactions)?	No
non-standard equivalents to CDT code sets (Dental Services)?	No
standard CDT code sets (Dental Services)?	No
non-standard equivalents to CPT4 code sets (Physician services)?	No
standard CPT4 code sets (Physician services)?	No
non-standard equivalents to ICD9 code sets (Diseases, injuries, etc)?	No
standard ICD9 code sets (Diseases, injuries, etc)?	No
non-standard equivalents to NDC code sets (Drugs and Biotics)?	No
standard NDC code sets (Drugs and Biotics)?	No
non-standard equivalents to HCPCS code sets (other services)?	No
standard HCPCS code sets(other services)?	No
User (soft) configured codes that may be configured to include CDT, CPT4, ICD9, NDC, or HCPCS?	Yes
None of the above	No
Identify all of the identifiers this product supports	
“National Provider Identifier” (USA Unique identifier for all individuals providing healthcare services)?	No
“National Employer Identifier” (USA Unique identifier for all healthcare facilities)?	No
“National Payer Identifier" (USA Unique identifier for all insurance carrier)?	No
None of the above	Yes
User Identification	
Does the product provide for individual identification (accounts) of clinical users (excluding service users)?	Yes
What is the maximum number of accounts (0<zero> ==> theoretically infinite)	1000
Does the product support passwords for authentication of the clinical users?	Yes
Does the product utilize the operating system authentication for clinical users?	Yes
Does the product place constraints on username?	No

Identify all of the authentication technologies this product supports	
NT Domain	Yes
MS Active Directory	No
Non-NT Kerberos	No
NIS / YP	No
CCOW	No
Other	No
None	No
During login does the product inform the user of the last time the system was accessed using that user account?	No
Can the user authentication be augmented by a biometric, token, or other method besides passwords?	Yes
Identify all of the advanced authentication the product supports:	
tokens	Yes
smart cards	Yes
badge readers	No
written signature verification	No
one-time password generators	No
biometric identifiers	No
Certificate identification	No
dial-back modems	No
Other	No
None	No
How does the customer get these advanced authentication methods?	Customer supplied
User Account Maintenance	
Identify all of the information associated with a user account:	
Full Name	Yes
Additional Identifier	Yes
Title	Yes
Department	No
Phone Number	Yes
E-mail Address	Yes
Street Address	No
FAX Number	Yes
Other	No
None	No

Who Can administer user accounts?	Multiple Accounts
Identify all of the User Administrative controls supported	
Audit Log of all account changes	No
Set an account inactive without removing the account?	Yes
Force a logoff of an active user?	No
Automatic de-activation of an account on a specified date or number of days/time?	No
Automatic de-activation of an account after a configured number of days of non-use?	Yes
Other	No
None	No
Identify all of the User Account Reports supported:	
List of all user accounts	No
List of currently active users	Yes
List of all user accounts with last used date/time	No
Other	No
None	No
When an account is marked inactive or deleted does the product disable in real-time any active sessions using that ID?	Yes
Does the product provide a tool for batch management of user accounts?	Yes
Authorizations	
Does the product support multiple levels of access control that can be assigned to user accounts?	Yes
Does the product support multiple levels of access control that can be assigned to groups of user accounts?	Yes
Identify all of the access control rights that can be applied to a user:	
View Patient Identifiable Data on screen	Yes
Print Patient Identifiable Data to paper or film	Yes
Modify Patient Identifiable Data	Yes
Export Patient Identifiable Data to removable digital media	No
Delete	Yes
Identify all the methods by which the access control right are applied:	
Access at database view level	No
Access at file level	No
Access at file system directory level	No
Time-of-Day	No
Weekly Schedule	No
Workstation (location)	No
Other	Yes
None	No

Does product hide functionality that the user does not have rights to (to prevent the user from even knowing a functionality exists)?	Yes
Does the product further restrict access based on patient specific consent?	No
Auto-Logoff	
Identify all of the inactivity Auto Logoff capability supported:	
Screen Saver (screen blanking) with no reAuthentication	No
Password protected Screen Saver (screen blanking)	Yes
Application Logout	No
Application blanking, with re-authentication allowing continuation.	No
Other	No
None	No
Can the administrator override any inactivity screen/application blanking?	Yes
Identify how the inactivity timeout can be configured:	
System Wide	No
Workstation (location)	Yes
Per-User	No
Device to Device Authentication	
Identify all of the entity authentication that is used, when communicating and the remote user is not or can not be authenticated serial number	No
Mac address	No
IP Address	No
AE-Title	No
Process identifier	No
Task identifier	No
Unidirectional PKI certificate challenge (ex: simple SSL)	No
Bidirectional PKI certificate challenge (ex: client and server auth SSL)	No
Other	No
None	Yes
Log All Security Events	
Identify all of the Security Events that can be logged:	
Machine Shutdown	Yes
Machine Boot	Yes
Application start	Yes
Application stop	Yes
Network link/connection failures	Yes
Data Integrity failure	No

Successful User Login	Yes
Failed User Login	Yes
User Logout	Yes
Auto-Logoff	Yes
Forced logoff by administrator	No
A user changed their password	Yes
An admin reset/cleared a users password	Yes
Attempt by a user to access function/data that they do not have access to	No
User/Group account creation	Yes
User/Group account deletion	Yes
User/Group Access rights modification	No
Other	No
None	No
Identify all of the contents of a Security Event log entry:	
Date and Time	Yes
Time to millisecond accuracy	No
Identifier of the User	Yes
Identifier of the device (workstation, IP, or other station identification)	Yes
Event description	Yes
Are these security events tracked in a different log than patient identifiable data related events?	Yes
On failed authentication attempts, is the password attempted entered into the log?	No
Is the log file persistent (NOT automatically overwritten or deleted)?	Not limited
Is access to this log restricted to authorized individuals?	Yes
Can the customer specify the list of events to track?	No
Log All Patient Data Views	
Identify all of the Patient Identifiable Data View events that can be logged:	
Printouts	Yes
Export to files	Yes
Export to removable media	Yes
Faxed	Yes
E-Mailed	Yes
View by browser	Yes
View by client application	No
Retrieved over network protocol (DICOM, XML, API, etc)	No
De-identification	No
Other	No

None	No
Identify all of the contents of a Patient Identifiable Data View log entry:	
Date and Time	Yes
Time to millisecond accuracy	No
Identifier of User	Yes
Identifier of Device (workstation, IP, or other station identification)	Yes
Identifier of the application	No
Identifier of the function within the application	No
Identification of the Patient	Yes
How long the data was displayed	No
Event description	Yes
Is the log file persistent (NOT automatically overwritten or deleted)?	not limited
Is access to this log restricted to authorized individuals?	Yes
Can the customer specify the list of events to track?	No
Log All Patient Data Modifications	
Identify all of the Patient Identifiable Data Modification events that can be logged:	
modification of clinical data prior to a final report (diagnosis, medications, observations, measurements, etc)	Yes
modification or amendments to a final report	Yes
modification of patient demographics	Yes
modification of test date, time, or setup parameters	Yes
modification of diagnosis	Yes
None	No
Identify all of the contents of a Patient Identifiable Data Modification log entry	
Date and Time	Yes
Time to millisecond accuracy	No
Identifier of User	Yes
Identifier of Device (workstation, IP, or other station identification)	Yes
Identifier of the application	No
Identifier of the function within the application	No
Identification of the Patient	Yes
Event description	Yes
Is the log file persistent (NOT automatically overwritten or deleted)?	not limited
Is access to this log restricted to authorized individuals?	Yes
Can the customer specify the list of events to track?	No
Log All Changes to the Configuration	

Identify all of the Configuration Change events that can be logged:	
Change of the system Date and/or Time	No
Installation of patches, maintenance, FMI, hotfix, etc	Yes
IP Address or other network configuration	No
Analysis algorithm parameters	No
Creation, modification, or deletion of output devices/API/interface/AE	No
Creation, modification, or deletion of input devices/API/interface/AE	No
Other	No
None	No
Identify all of the contents of a Configuration Change log entry:	
Date and Time	Yes
Time to millisecond accuracy	No
Identifier of User	No
Identifier of Device (workstation, IP, or other station identification)	No
Identifier of the application	No
Identifier of the function within the application	No
Event description	Yes
Is the log file persistent (NOT automatically overwritten or deleted)?	date limited
Is access to this log restricted to authorized individuals?	Yes
Can the customer specify the list of events to track?	No
Audit Log Viewing	
Is there protection against ALL modification of all log files?	Yes
Is deletion of a log tracked in a different log?	No
Is viewing of a log tracked in a different log?	No
Does the product provide alerts based on automated advanced log analysis?	No
Are the audit trail alerts tracked in an log?	No
Is there a time syncronization function included and documented?	Yes
Audit Log Mining	
Does the product support the use of third-party audit mining packages?	No
Does the product support a mechanism for creating a text based audit log (or are the audit logs already text)?	No
Does the product integrate with CA Unicenter or HP Openview?	No
Does the product provide searching tools for the audit logs?	No
Does the product provide sorting tools for the audit logs?	Yes
Identify all of the Audit Trail Reports that can be created:	
Users accessing records with the same last name as the user	No
Users accessing records with the same address as their address	No

Access to records that have not been accessed in a long time	No
Access to an employee's own patient data	No
Accesses to minor's patient data	No
Accesses to terminated employees patient identifiable data	No
Multiple login attempts with improper authentication	No
All users that have use a specific function	No
All activity of a specific user	No
All accesses to a specific patient	No
All activity from a specific workstation or communications link	No
All login and logout activity within a period of time	No
All login failures	No
All Access control failures	No
All Modifications to security settings	No
All changes to authentication settings	No
All access via remote service interface	No
All changes to the audit trails configuration	No
Other	No
None	Yes
Configuration Lockdown & Security Fixes	
Is this OS configured to meet DOD - C2 Compliance?	No
Have unnecessary services and protocols been turned off?	Yes
Have unnecessary services and protocols been uninstalled?	Yes
Are default passwords documented in any form of manual?	Yes
Are passwords that are not changable used for administrative accounts?	No
Is the SNMP community name set to "public" or "private"?	No
Is there documentation available that describes the services and protocols that are necessary for proper operation of the product?	Yes
Is the customer free to apply any Operating System or tool vendor fixes to the product?	No
Does the M4 release contain all security fixes for the OS, database, or any other third party tools within 6 months of the M4 date?	Yes
For Operating Systems:	
The typical time window between when a patch is available and when it can be applied to a customer system is 6 months	Yes
The typical time window between when a patch is available and when it can be applied to a customer system is 12 months	Yes
The customer can get OS fixes that are no more than 12 months old	Yes
Is this database configured with the minimal services and protocols running?	Yes

For Databases:	
The typical time window between when a patch is available and when it can be applied to a customer system is 6 months	Yes
The typical time window between when a patch is available and when it can be applied to a customer system is 12 months	Yes
The customer can get database fixes that are no more than 12 months old	Yes
Does the product include other third party tool or application (Backup software, SNMP agent, pcAnywhere, maintenance tool, Microsoft Office, etc)	Yes
For other 3rd party tools:	
The typical time window between when a patch is available and when it can be applied to a customer system is 6 months	Yes
The typical time window between when a patch is available and when it can be applied to a customer system is 12 months	Yes
The customer can get 3rd party tool fixes that are no more than 12 months old	Yes
List any Third Party Applications, Tools, Libraries, Drivers?	IE, MSDE, MDAC, MMC, Diske
AntiVirus	
Are all product releases and maintenance releases scanned for any malicious code (Virus, Worm, Trojan)?	Yes
Identify all of the Malicious Code detection supported:	
Host based Intrusion Detection	No
Norton AntiVirus	Yes
McAfee AntiVirus	Yes
Other Windows AntiVirus	No
Customer supplied AntiVirus software	No
Customer administrated AntiVirus Signature Files	No
Tripwire or other	No
None	No
Integrity Controls on Data	
Does the product utilize transparent end-to-end data integrity controls? (memory parity, tcp checksums, etc)	Yes
Does the product enforce application managed data integrity controls like object checksums?	No
Does the product support PKI based Digital Signatures to maintain data integrity?	No
Does the product enforce required fields during data entry to ensure completeness of records?	Yes
Does the product have a data entry validation mechanism such as double keying of patient identifiable data to ensure accuracy of the data entered?	No
Does the product store rejected transactions with the reason for the rejection?	Yes
Does the product ensure that database updates are done in a failsafe way?	Yes

Is there any Other form of integrity control provided?	No
Backup and Recovery	
How many patient records does this product store or manage?	unlimited
Identify all the ways that the product protects against disasters/failures:	
Export to removable media	No
RAID hard drive	Yes
backup of patient data only (typically to tape)	Yes
backup of full system (typically to tape)	Yes
UPS	Yes
Off site mirroring	No
Near-line storage	No
Other	No
None	No
Backup and Recovery procedures are documented?	Yes
Can the Integrity and completeness of the backup be verified by the operator through the use of offline means?	Yes
Encryption	
Is any form of encryption of patient identifiable data supported (not including the service interface)?	No
De-Identification	
Is there a bulk de-identification functionality that the user can use? (not service interface)	No
Digital Signatures	
Does the product provide for some form of electronic acceptance stamp on Patient Identifiable Data ?	Yes
Does the product provide for a PKI based digital signature?	No
Does the product support DICOM supplement 41 Digital Signature Extensions?	No
Service	
Is there a method that service can use to access the system in the case of an emergency when normal administration is not possible?	Yes
Does the product have at least one login specifically for servicing the equipment?	Yes
Does the product restrict service individuals with multiple levels of access control?	No
Does the product support multiple individual service accounts?	No
Does the product support multiple individual service accounts?	No
Are Service accounts restricted from viewing, or manipulating Patient Data?	No
Are all accesses to Patient Data by service restricted to de-identified data?	No
Are Service actions accounted for in a log file somewhere?	Manually
Are passwords that are not changeable used for Operating System administrative accounts?	No
Are passwords that are not changeable used for service accounts?	No
Are Service default passwords described in details in any form of manual?	No

Is the customer allowed to change the service passwords?	Yes
Does the product support remote service?	pcAnywhere
Does the remote service session require authentication to a service user?	Yes
Can the customer tell that a remote service session is in progress?	Yes
Can the customer, through automatic or manual methods, know which specific service individual is currently remotely logged in?	No
Can the customer see what is happening in an active remote service session?	Yes
Can the customer stop an active remote service session?	Yes
Specify the equivilant encryption strength that a remote service session can operate over?	3DES
Is the product specific GE Remote Service network isolated from the rest of the GE intranet?	No
Are access points to the GE service network protected with an ICSA equivalent firewall?	No
Are remote sessions ever initiated without a Service call being logged by the customer?	No

For your notes

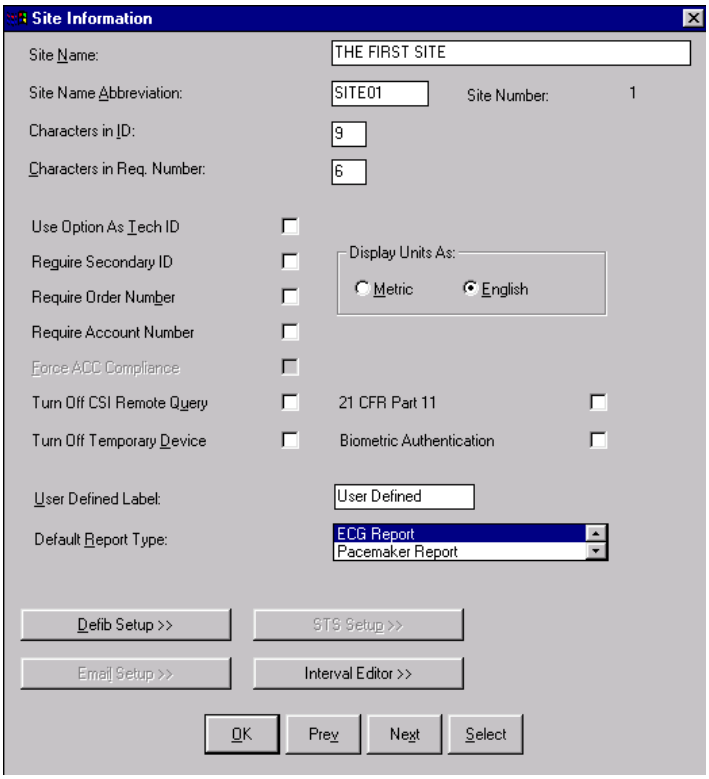
C Appendix C – 21 CFR Part 11 Option

For your notes

Biometric Authentication

The 21 CFR Part 11 option is available with MUSE CV software version 005D.02 software and higher. When this option is enabled, the *Site Information* window contains two additional check boxes.

- *21 CFR Part 11*
- *Biometric Authentication*



14A

1. Use the *Select* button to display the *Site Information* window for the site which must meet the requirements of 21 CFR Part 11.
2. Select the *21 CFR Part 11* check box.

NOTE

This check box is not checked by default. In order to have this option be functional on the site, the check box must be checked.

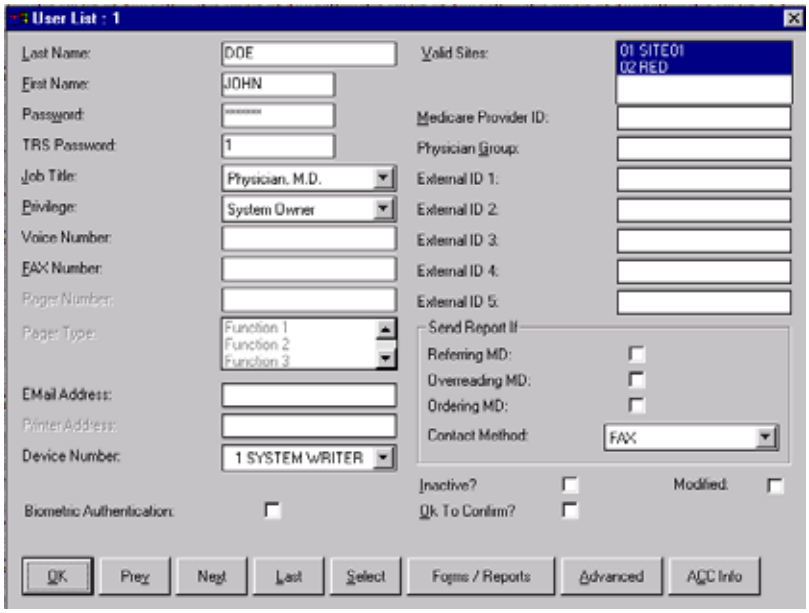
3. If biometric authentication is being used for EVERY USER on the site, check the *Biometric Authentication* check box.

21 CFR Part 11	☑
Biometric Authentication	☑

4. If the site has some users who use biometric authentication and some users who do not use biometric authentication, check *21 CFR Part 11* and leave *Biometric Authentication* unchecked.

21 CFR Part 11	☑
Biometric Authentication	☐

When *Biometric Authentication* is left unchecked in *Site Setup*, individual's User Setups will be used by the system when they confirm reports.



16A

The table below summarizes how the individual user's *Biometric Authentication* option functions.

User *Biometric Authentication* Summary		
Site Setup Window	User Setup Window	Description
21 CFR Part 11 ☑ *Biometric Authentication* ☐	*Biometric Authentication* ☑	Users who have *Biometric Authentication* checked in their *User Setup* window will not be prompted for a password when they confirm reports.
21 CFR Part 11 ☑ *Biometric Authentication* ☐	*Biometric Authentication* ☐	Users who do not have *Biometric Authentication* checked in their *User Setup* window will be prompted for a password EACH TIME they confirm a report.

Other 21 CFR Part 11 Features

Disable Automatic Updates to Report Data

When the 21 CFR Part 11 option is enabled, automatic updates to report data are disabled on the MUSE system. This means that confirmed reports are not updated when new reports for the same patient are confirmed. It also means that the MUSE CV system does not update data entered/acquired at the cart.

- Patient demographic data (age, gender, race, height, and weight) are not updated in confirmed data when new reports for the same patient are confirmed on the system.
- After QTC has been calculated at the cart, the MUSE CV system does not re-calculate QTC upon acquisition of this data.
- When user IDs have been entered at the cart, the MUSE CV system does not assign user names to these IDs upon acquisition of this data.

Logging

When the 21 CFR Part 11 option is enabled, all changes made to patient reports are logged and these log files are archived by the system.

GE Medical Systems
Information Technologies, Inc.
8200 West Tower Avenue
Milwaukee, WI 53223 USA
Tel: + 1 414 355 5000
1 800 558 7044 (US Only)
Fax: + 1 414 355 3790

EC REP
GE Medical Systems
Information Technologies GmbH
Munzinger Straße 3-5
D-79111 Freiburg
Germany
Tel: + 49 761 45 43 - 0
Fax: + 49 761 45 43 - 233

Asia Headquarters
GE Medical Systems
Information Technologies Asia; GE (China) Co., Ltd.
11th Floor, Shanghai MAXDO Center,
8 Xing Yi Road, Hong Qiao Development Zone
Shanghai 200336, People's Republic of China
Tel: + 86 21 5257 4650
Fax: + 86 21 5208 2008

www.gehealthcare.com