GE Healthcare

MUSE™ Cardiology Information System

Advanced Security Guide

Software Version 8.0

2034539-048 A

MUSE Cardiology Information Systems
English

The information in this manual only applies to MUSE™ Cardiology Information System software version 8. It does not apply to earlier software versions. Due to continuing product innovation, specifications in this manual are subject to change without notice.

The document part number and revision appear at the bottom of each page. The revision identifies the document's update level. The revision history of this document is summarized in the following table.

Revision	**Date**	**Comment**
A	29 March 2011	Initial Release

Contents

1

Introduction

Security Features Overview

The MUSE™ Cardiology Information System (also referred to as the MUSE system) has several security features which, when properly used and configured, can support U.S.A. 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 refer to the following link:

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 GE Healthcare Support Center at 1-800-558-7044.

Regulatory and Safety Information

This section provides information about the safe use and regulatory compliance of this device. Familiarize yourself with this information and read and understand all instructions before attempting to use this device. The system software is considered medical software. As such, it was designed and manufactured to the appropriate medical regulations and controls. Any exceptions are noted in the Compliance Information - Exceptions section.

NOTE:

Disregarding the safety information provided is considered abnormal use of this device and could result in injury, loss of data, and void any existing product warranties.

Safety Conventions

A **Hazard** is a source of potential injury to a person, property, or the product.

This manual uses the terms DANGER, WARNING, and CAUTION to point out hazards and to designate a degree or level of seriousness. Familiarize yourself with the following definitions and their significance.

Definitions of Safety Conventions

Safety Convention	Definition
DANGER	Indicates an imminent hazard, which, if not avoided, will result in death or serious injury.
WARNING	Indicates a potential hazard or unsafe practice, which, if not avoided, could result in death or serious injury.
CAUTION	Indicates a potential hazard or unsafe practice, which, if not avoided, could result in minor personal injury or product/property damage.

Safety Hazards

WARNING:

INCORRECT TREATMENT: Some of the communications protocols used in this product (CSI and DCP) do not provide encryption or authentication at this time. These protocols are used to send clinical data to the MUSE system from ECG carts and other clinical devices.

You should take appropriate steps to secure the privacy of communications on your network when using this product.

Document Conventions

This manual uses the following conventions.

Typographical Conventions

Convention	Description
Bold Text	Indicates keys on the keyboard, text to enter, or hardware items such as buttons or switches on the equipment.
Italicized-Bold Text	Indicates software terms that identify menu items, buttons or options in various windows.
CTRL+ESC	Indicates a keyboard operation. A plus (+) sign between the names of two keys indicates that while holding the first key, you should press and release the second key. For example, Press **CTRL+ESC** means to press and hold the **CTRL** key and then press and release the **ESC** key.

Convention	Description
<space>	Indicates that you must press the spacebar. When instructions are given for typing a precise text string with one or more spaces, the point where you must press the spacebar is indicated as: **<space>**. This ensures that the correct number of spaces are inserted in the correct positions within the literal text string. The purpose of the < > brackets is to distinguish the command from the literal text within the string.
Enter	Indicates that you must press the **Enter** or **Return** key on the keyboard. Do not type ***Enter***.
>	The greater than symbol, or right angle bracket, is a concise method to indicate a sequence of menu selections. For example, the statement “From the main menu, select ***System*** > ***Setup*** > ***Options*** to open the ***Option Activation*** window” replaces the following: 1. From the main menu, select ***System*** to open the ***System*** menu. 2. From the ***System*** menu, select ***Setup*** to open the ***Setup*** menu. 3. From the ***Setup*** menu, select ***Options*** to open the ***Option Activation*** window.

Illustrations

All illustrations in the manual are provided as examples only. Depending on system configuration, screens that appear in the manual may differ from the screens as they appear on your system.

All patient names and data are fictitious. Any similarity to actual persons is coincidental.

Notes

Notes provide application tips or additional information that, while useful, are not essential to the correct operation of the product. They are called out from the body text through a flag word and indentation, as follows:

NOTE:

> The tip or additional information appears indented below the **NOTE** flag word.

2

MUSE Security Features

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 that 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.	❐
	User Authentication	Windows Authentication	Windows Users should be mapped to MUSE Users.	❐
			Allow Only Windows Authentication option is installed[1]	
	Unattended Workstation Security	Logout or Lockout Screen Savers	All workstations are configured to use ***Logout Screen Saver*** or ***Lockout Screen Saver***.	❐

[1] Enabling this feature requires the assistance of the GE Healthcare Support Center. Please dial 1-800-558-7044 to request assistance with activating this feature.

FDA Requirement	MUSE Feature	Configuration	Recommended	Solution
Accounting & Tracking	Windows Event Log	Audit Policy	The Windows utility "Audit Policy" is set on the MUSE server and all workstations to log certain events.	□
	Audit Trails	Editor Security	Enable the ***Change Log***.	□
	Secure Configuration	Remote Query	The ***Remote Query*** feature is disabled.	□
		User Entered Destination	The ***User Entered Destination*** feature is disabled.	□
Web Encryption & Logging	MUSE Web	SSL Encryption	The MUSE file server is set to use SSL to force 128-bit encryption.	□
		SSL Logging	The MUSE file server is set to use IIS to log MUSE Web activities.	□
Data Integrity	Anti Virus	Anti Virus Software Configuration	Virus protection software is installed and properly configured on the MUSE file server and all workstations.	□

MUSE Features that Require Policies/Procedures

The following MUSE features require policies and procedures to achieve security compliance.

Policies and Procedures Required for HIPAA & 21 CFR Part II Security Compliance	
MUSE Feature	**Why a Policy/Procedure is Needed**
HL7 Device	Patient Data leaving the system, thus, no longer change logging or protecting access of records.
Folder, FTP Folder, Email	Patient Data leaving the system, thus, no longer change logging or protecting access of records.
MUSE API	Data is leaving the system and may not be under any security control.
Fax	Faxed information can be viewed by anyone, thus a policy should be in place regarding cover pages, and confidentiality of patient information. Work with your legal department in developing these policies/procedures.

Policies and Procedures Required for HIPAA & 21 CFR Part II Security Compliance	
Remote Query	Data is leaving the system and may not be under any security control.
Allowing users to enter destination	Data is leaving the system and may not be under any security control.

Policies and Procedures Required for 21 CFR Part II Security Compliance	
Feature	**Why a Policy/Procedure is Needed**
Acquiring ECGs requires Technicians to enter ID Number at cart	Data leaves the system and not under any security control

Access Control Security

The MUSE system requires two Windows user accounts:

- MuseAdmin – used by GE Healthcare service personnel to access and work on the system
- MuseBkgnd – used by the MUSE system to run background Windows Services

Account names and passwords for the MUSEAdmin and MUSEBkgnd Windows user accounts are managed through Windows like any other Windows user account. Both accounts should have passwords that are set to never expire. If the passwords change, GE Healthcare service personnel may not be able to log into the system to provide support, and the background services will fail to start, causing the MUSE system to stop functioning. All other users of the MUSE system can use their normal Windows user credentials to access the MUSE system. Inside the MUSE application, the users are setup with their domain\user account information. No password information is required when configuring a MUSE user. The user passwords can be controlled or changed through Windows as required.

The following sections describes these accounts, how they are used, and the system requirements. These requirements are met by following the instructions in the *MUSE Cardiology Information System Installation Manual*.

MUSE Administrator Account

The MuseAdmin account is used by GE Healthcare service personnel to log into the MUSE system to perform initial setup and configuration, and to provide ongoing service and support.

This account must meet the following requirements:

- Needs to be a member of the Windows Administrators Group on the MUSE file server.
- Must be assigned a system administrator role in SQL server. For instructions on adding a system administrator role in SQL server, see the *MUSE Cardiology Information System Installation Manual*.
- Should be a domain account whenever possible. As an alternative, it can be an account local to the MUSE file server.

- Both the account name and password for the MUSEAdmin account can be determined by the customer, but must be shared with GE Healthcare service personnel so that they can use that account when they work on the MUSE system. For instructions on changing the account name and password, see the *MUSE Cardiology Information System Service Manual*.
- The customer should not use this account for any purpose and should instead create an account for each individual user using the system.

MUSE Background Account

The MuseBkgnd account is used to start the MUSE related background services on the MUSE file server. This account needs to meet the following requirements:

- Needs to be a member of the Windows Administrators Group on the MUSE file server.
- Must be assigned a system administrator role in SQL server. For instructions on adding a system administrator role in SQL server, see the *MUSE Cardiology Information System Installation Manual*.
- Must not be subject to any policies that would not allow the account the “Log on As Service” right, since that right is a requirement for the account to be able to start the MUSE related background services.
- Should be a domain account whenever possible. As an alternative, it can be an account local to the MUSE file server.
- Both the account name and password for the MUSEAdmin account can be determined by the customer, but must be shared with GE Healthcare service personnel so that they can use that account when they work on the MUSE system. For instructions on changing the account name and password, see the *MUSE Cardiology Information System Service Manual*.
- The customer should not use this account for any purpose and should instead create an account for each individual user using the system.

Changing the Default System Accounts

Customers using Windows authentication may choose to change the Windows account names, account passwords, or both to address security issues or to comply with changes in network standards at any time (see “Windows Authentication vs. MUSE Authentication” on page 13). The name and password changes are made using the ***Local Users and Groups*** function of the ***Administrative Tools*** on the MUSE file server. In addition, several command line utilities must be run to ensure that the changes are reflected in the MUSE system.

Customers using MUSE authentication, may choose to change the passwords for the default accounts at any time (see “Windows Authentication vs. MUSE Authentication” on page 13). They cannot, however, change the account names. The password changes are made using the standard ***MUSE User Setup*** function.

For detailed instructions on changing the Windows account names, the Windows account passwords, or the MUSE account passwords, refer to the *MUSE™ Cardiology Information System Service Manual*.

3

User Authentication

MUSE provides two types of user authentication:

- Windows Authentication
- MUSE Authentication

Windows Authentication vs. MUSE Authentication

Using Windows 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.

MUSE authentication is most commonly used on a client workstation that is shared by multiple users, and where those users do not want to log out of Windows and log back in to run the MUSE application and be recognized as a different user. Each person that runs the MUSE application on the shared workstation can log into MUSE with their own user name and password. To help meet HIPAA compliance, policies and procedures will need to be in place when using MUSE authentication.

Using Windows authentication, users are not required to log into the MUSE application separately. When the MUSE application is launched, MUSE will automatically log them in as the proper user, based on the user that is logged into Windows on that computer. Windows authentication supports a higher level of security as recommended to meet HIPAA compliance standards.

Allowing MUSE Authentication

By default, the system allows either MUSE or Windows authentication. To disable MUSE authentication on the system so that Windows authentication can be used, contact the GE Healthcare Support Center at 1-800-558-7044, or contact your regional support center if you are outside the United States.

If MUSE authentication is allowed, it can be enabled at individual workstations by adding the following switch to the shortcut that is used to launch MUSE: ***-museauthenticate***.

If MUSE authentication is disabled and a user tries to log in using MUSE authentication, a message will appear stating MUSE authentication is not enabled.

If a user is logged into the MUSE system using their correct Windows authentication, an error message appears, but they will be allowed into the system.

If a user is logged into the MUSE system as a different user, and logs in using MUSE authentication, an error message appears and they will not be allowed into the system.

Unattended Workstation Security

Two options are available for setting up logout/lockout security on workstations that are left unattended for a specified amount of time:

- **Logout** — When a workstation is inactive (no mouse or keyboard input) for a specified amount of time, the current user will be logged off Windows, and the MUSE session will end.
- **Lockout** — When a workstation is inactive for a specified amount of time, the screen saver selected in the ***Control Panel*** is activated.

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

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 a predetermined time of inactivity	Yes	Yes
Requires authentication to log back into the MUSE system	Yes	Yes
The workstation is locked	No	Yes
Users can unlock workstation	N/A	• Last user • Administrator
The MUSE application exits	Yes	• No, if the last user unlocks the workstation • Yes, if the Administrator unlocks the workstation

Differences between the Two Options for Unattended Workstation Security		
Item	**Logout Screen Saver WINEXIT**	**Lockout Screen Saver Logon with Password Protected**
Lose unsaved changes	Yes	• No, if the last user unlocks the workstation • Yes, if the Administrator unlocks the workstation
Possibility of locking a record that was being edited when the screen saver took control. [2].	Yes	• No, if the last user unlocks the workstation • Yes, if the Administrator unlocks the workstation

Setting Up Security for an Unattended Workstation

There are two ways you can set up security for an unattended workstation.

- WINEXIT can be used if you are running Windows XP.
- Setting up a scheduled task can be used no matter which Windows version you are using.

Configuring the Winexit.scr Screensaver for Windows XP

If you are running Windows XP, the Winexit.scr screensaver forces the user to quit programs and log off after a set period of inactivity. To install the winexit screensaver on a typical Windows XP system, use the following instructions or the instructions found at http://support.microsoft.com/kb/314999 .

1. Download the file from the Windows 2003 Resource Kit at http://www.microsoft.com/downloads/en/details.aspx?FamilyID=9D467A69-57FF-4AE7-96EE-B18C4790CFFD&=en , or use ***Windows Explorer*** to locate the **Winexit.scr** file in the Windows 2000 Resource Kit folder on your hard drive.
2. Right-click the ***Winexit.scr*** file, and then click ***Install***.

   The ***Display Properties*** dialog box opens with the ***Screen Saver*** tab active. and the ***Logoff Screen Saver*** entry is automatically selected.
3. Click ***Settings***.
4. Select the ***Force application termination*** check box to force programs to quit.
5. In the ***Countdown for n seconds*** box, type the number of seconds the ***logoff dialog*** box will appear before the user is logged off.
6. In the ***Logoff Message*** box, type the message that appears during the logoff countdown.
7. Click ***OK***.
8. In the ***Display Properties*** dialog box, click ***Preview***.

[2] 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, a user with sufficient privileges can log on the workstation which has locked the record and start the MUSE application.

9. Review the ***Auto Logoff*** dialog box.

   It displays the logoff message and the countdown timer.

10. Click ***Cancel***.

11. Click ***OK*** to save the settings.

Alternative to WINEXIT

The other way to log off users after inactivity is to use the pssshutdown.exe program from sysinternals. This program will log out the currently logged in user on the system where it is installed. You can use the system scheduler to run this task after the system has been idle.

1. Log onto http://technet.microsoft.com/en-us/sysinternals/bb897541.aspx for instructions and download the ***sysinternals psshutdown.exe*** command.

2. Place the file into the ***C:\windows*** folder.

3. Schedule a task as the local administrator using ***c:\windows\psshutdown.exe -o -f***.

4. Under the ***Schedule tab > Schedule Task***, select ***When idle*** .

5. In the field ***When the computer has been idle for***, enter the number of minutes before automatic shutdown.

6. Under the ***Settings*** tab, leave the 72 hours at the top as is. Select ***Only start the task if the computer has been idle for at least:***, and enter the number of minutes that the computer can be idle.

7. Leave ***if the computer has not been idle that long, retry for up to:*** at zero.

8. Leave all other boxes beyond this point empty.

9. Exit the screen.

4

Accounting/Logging

Print Log

Outbound events refer to data that is sent out of the MUSE system, such as patient tests, reports, sending out lists for printing, and so on.

The system logs the following outbound events:

- Printing to Postscript and PCL printers
- Fax
- CSI
- Email
- HL7
- Folder
- FTP Folder

These outbound events can be viewed in the ***Print Log***. To open the ***Print Log***, select ***Status*** > ***Print Log***.

Refer to the *MUSE Cardiology Information Systems Operator Manual* for instructions on configuring the ***Print Log***.

Change Log

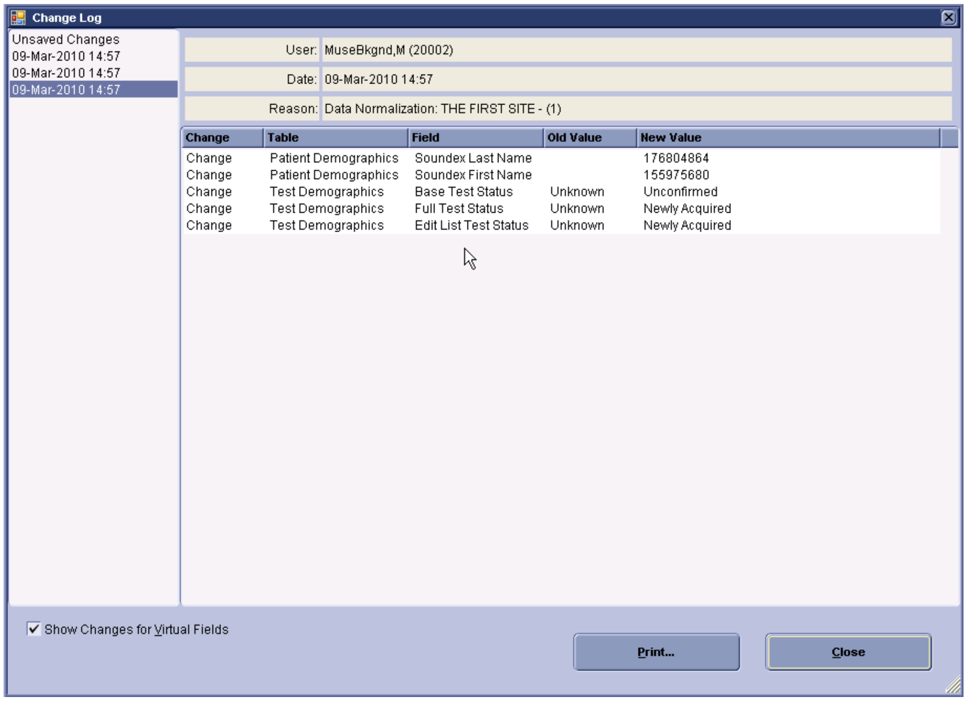
The ***Change Log*** tracks changes to patient data and may facilitate finding a test that had incorrect data entered on the device and has since been corrected in the MUSE system.

The Change Log function must be activated within ***System > Setup > Sites > Test Type Settings***. All changes made to a record appear in the ***Change Log***. This includes changes to patient demographics, test measurements, and diagnostic statements within the interpretive window.

NOTE:
You cannot view the ***Change Log*** at the Serial Comparison layout.

1. At the ***Edit list***, open a patient test.
2. Select the ***Clerical*** tab.

3. Click the ***Change Log*** button to open the ***Change Log*** window.



Unsaved Changes
09-Mar-2010 14:57
09-Mar-2010 14:57
09-Mar-2010 14:57

User: MuseBkgnd,M (20002)

Date: 09-Mar-2010 14:57

Reason: Data Normalization: THE FIRST SITE - (1)

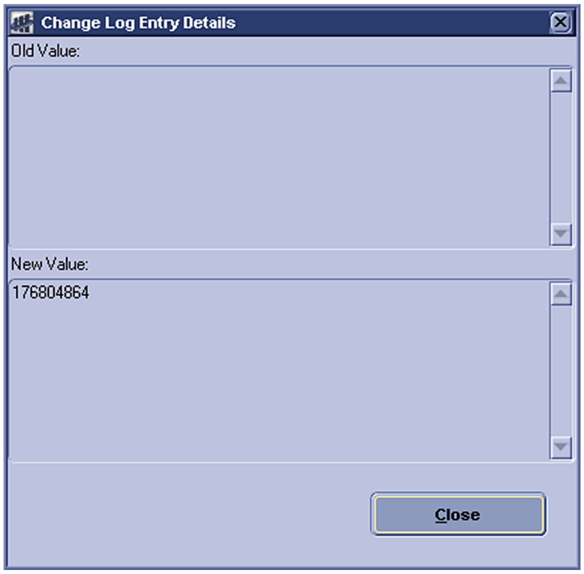
Change	Table	Field	Old Value	New Value
Change	Patient Demographics	Soundex Last Name		176804864
Change	Patient Demographics	Soundex First Name		155975680
Change	Test Demographics	Base Test Status	Unknown	Unconfirmed
Change	Test Demographics	Full Test Status	Unknown	Newly Acquired
Change	Test Demographics	Edit List Test Status	Unknown	Newly Acquired

☑ Show Changes for Virtual Fields

Each time you make a change to a patient test (including changes made at the HIS), the changes are recorded. After a test is updated or saved in the database, the changes are saved by date.

4. To view the change log details, double-click on a changed item to expand it.

   The ***Change Log Entry Details*** window opens.



Old Value:

New Value:
176804864

This window is helpful when displaying long fields such as the diagnosis.

5. To print the ***Change Log***:
    a. Click the ***Print*** button

       The ***Select Device and Formatting Options*** window opens.
    b. Make the appropriate choices and click ***OK*** to print the log.
6. To enable the display of supplemental test fields that are generated and maintained by the MUSE system, select the ***Show Changes for Virtual Fields*** check box. Examples of some of these fields are: ***Edit Time***, ***Edit Date*** and identification codes that uniquely identify the patient to the MUSE system.
7. Click ***Close*** when finished to exit the ***Change Log***.

Edit Change Log

The ***Edit Change Log*** is a list of changes made to a test's patient ID, name (first and last), location, date and time. The log exists to facilitate finding a test that had incorrect data entered on the device and was corrected in the system.

Process Log

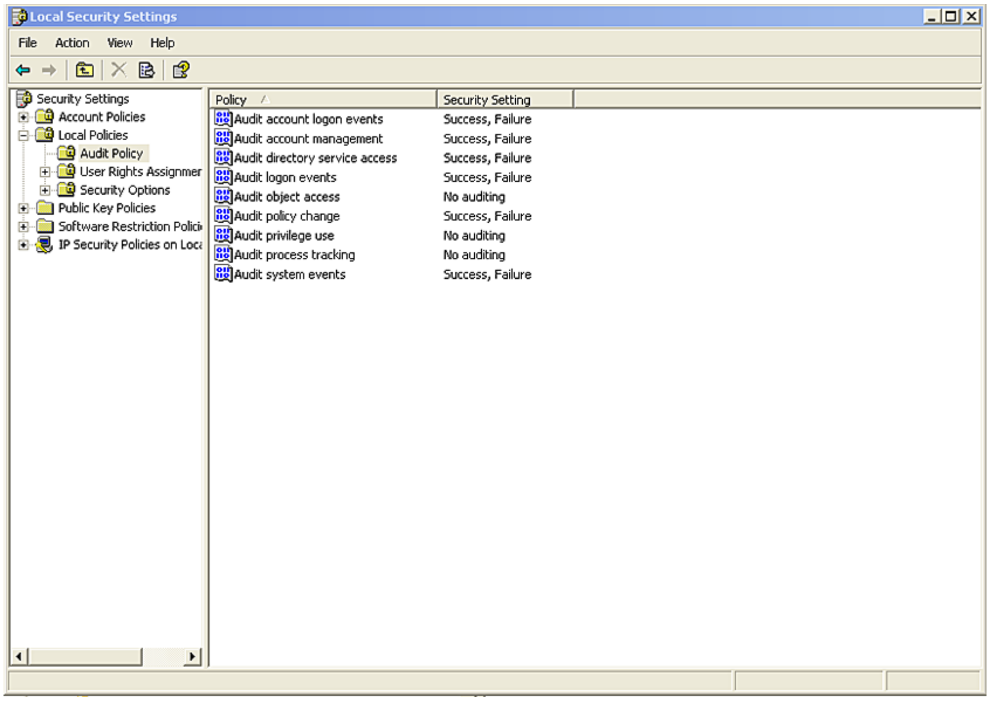
The ***Process Log*** is a list of all of the processes the system ran. This log includes processes currently running and those that terminated successfully. You can identify current processes because they do not have an end time. Processes with an old start time and no end time have most likely failed and can be investigated for issues.

Logging System Security Events

The MUSE application server and workstations should be configured to log Windows security events to the ***Windows Viewer***. At each file server and workstation, repeat the following steps to set up this audit.

1. Click ***Start*** > ***Programs*** > ***Administrative Tools*** > ***Local Security Policy***.

   The ***Local Security Settings*** window opens.



Policy	Security Setting
Audit account logon events	Success, Failure
Audit account management	Success, Failure
Audit directory service access	Success, Failure
Audit logon events	Success, Failure
Audit object access	No auditing
Audit policy change	Success, Failure
Audit privilege use	No auditing
Audit process tracking	No auditing
Audit system events	Success, Failure

2. Select ***Local Policies*** > ***Audit Policy***.
3. Click on each event and select the check boxes indicated in the following table.

Event	Success	Failure
Audit account logon events	✓	✓
Audit account management		✓
Audit directory service access		✓
Audit logon events	✓	✓
Audit object access		✓
Audit policy change	✓	✓
Audit privilege use		✓
Audit process tracking		✓
Audit system events	✓	✓

4. Click ***OK*** to save your changes.
5. Close the ***Local Security Settings*** window.

5

MUSE Web

Internet Information Services (IIS) is required on the MUSE Web server. To access the MUSE Web, the user must have their browser configured for 128-bit encryption.

For detailed procedures, see the *MUSE Web Server Instruction Guide to Enabling SSL*.

Configuring IIS to Log Web site Activity on MUSE Web

The MUSE application server should be configured to enable logging Web site activity as follows:

1. Right-click ***My Computer*** and select ***Manage***.
2. Expand ***Services & Application*** > ***Internet Application Services*** > ***Websites*** in the list found in the ***Tree*** list (left panel).
3. Right-click on ***MUSE Web site*** and select ***Properties*** in the ***Web site*** tab.
4. Make sure that the ***Enable Logging*** check box is selected in the ***Web site*** tab.
5. For ***Active log format***, make sure it is ***W3C Extended Log File Format***.
6. Select ***Properties.....***.

    a. Select the ***General*** tab.

    b. Select ***Weekly*** for ***New Log Time Period***.

    c. Make sure the ***Log file directory*** is ***%WinDir%\System32\LogFiles***.

    d. Select the ***Advanced*** tab.

    e. Add/delete/verify check marks to obtain the following ***Extended Logging Options***.

        ✓ Date
        ✓ Time
        ✓ Client IP Address
        ✓ User Name
        Service Name
        ✓ Server Name
        ✓ URI Query
        Http Status
        Win32 Status
        Bytes Sent
        Bytes Received
        Time Taken

✓ Server IP

Server Port

✓ Method

Protocol Version

User Agent

Cookie

Referred

f. Click ***OK*** to close the ***Logging Properties*** window.

g. Click ***OK*** to close the ***Web site Properties*** window.

Setting up Client Browser for 128-bit Encryption

The MUSE Web server will only allow 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 following steps 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***.

6

Anti-Virus Software and Security Updates

Anti-Virus Software

GE Healthcare has validated the proper operation of the MUSE system with Norton Anti-Virus Corporate Edition and McAfee NetShield installed. Either of these two virus protection software applications can be installed on the system without affecting function or performance.

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

See the *MUSE Pre-Installation Manual* for additional information on installing anti-virus software on the MUSE system. 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.

Security Updates

A list of viruses that pose a significant threat to GE Healthcare customers' product security is posted on the GE Healthcare Product Security web site.

As new vulnerabilities and potential security issues arise, GE Healthcare makes every effort to quickly identify and notify customers of approved fixes. Time is required for GE Healthcare to identify the vulnerability, test the fix, and run a validation test on the product for safety and functionality. Only after this rigorous process does GE Healthcare release the official patch. While we recognize the urgency to correct these problems, we must ensure that the integrity of the system is not compromised.

After security patches are validated for specific GE Healthcare products, the information is added to the Product Security website. You can download the patch directly from the website of the software manufacturer (Microsoft, and so forth) and apply it to your GE Healthcare product. To check on the latest information regarding validated security patches:

1. Browse to the GE Healthcare Product Security website: http://prodsecdb.gehealthcare.com

   The ***Single Sign On*** (SSO) window opens.

2. Enter your SSO number and password and click ***Log In***..

   If you do not have an SSO number, click the ***Sign Up*** link to obtain one.

3. Use the features on the GE Healthcare ***Product Security Database*** Web site to determine security patches that you can apply to your system.

A

Appendix A — HIPAA Overview

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 U.S. 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
- Prohibition of discrimination based on health status

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

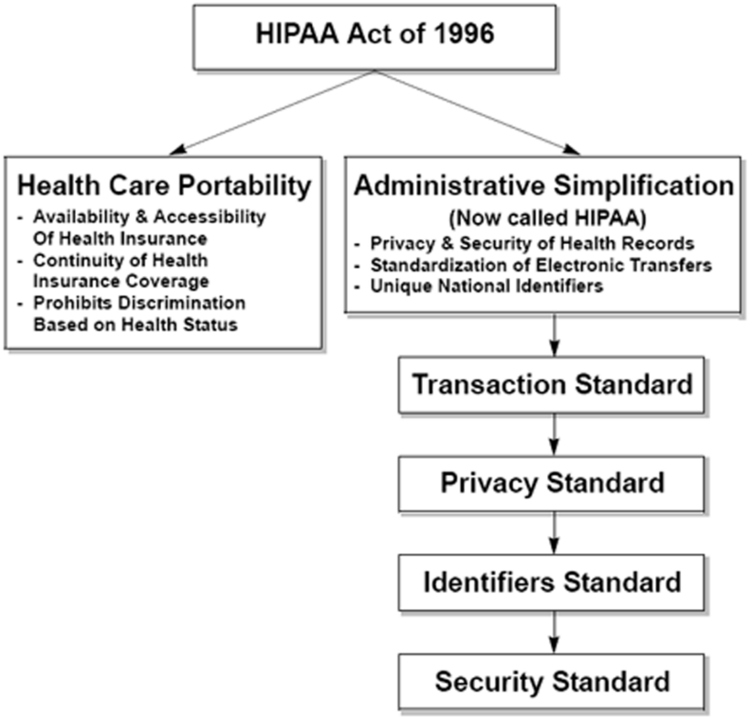
- Standardization of electronic transfers of patient health, administrative, and financial data
- Privacy and security standards protecting the confidentiality and integrity of health information
- Unique health identifiers for individuals, employers, health plans, and health care providers

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:

- Electronic Health Transactions Standards
- Unique Identifiers
- Security & Electronic Signature Standards
- Privacy & Confidentiality Standards

HIPAA's complexity confuses customers. Even the HIPAA name causes confusion. Recently the scope of the term 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 Healthcare 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 the following diagram.


HIPAA Act of 1996
Health Care Portability
- Availability & Accessibility Of Health Insurance
- Continuity of Health Insurance Coverage
- Prohibits Discrimination Based on Health Status
Administrative Simplification
(Now called HIPAA)
- Privacy & Security of Health Records
- Standardization of Electronic Transfers
- Unique National Identifiers
Transaction Standard
Privacy Standard
Identifiers Standard
Security Standard

The HIPAA component with the greatest impact on GE Healthcare customers is the Privacy Standard, as 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. The following table summarizes the HHS release status and timetable for the HIPAA rules.

HIPAA Rules and Rulemaking Timetable			
Standard	**Publication Date**	**Final Ruling**	**Required Compliance**
1. Insurance Portability	August 02, 1996	August 02, 1996	July 01, 1997
2. Electronic Transactions & Code Sets[3]	May 07, 1998	August 17,2000	October 16, 2003
3. Privacy & Confidentiality	November 03, 1999	December 28, 2000	April 14, 2003
4. National Provider Identifier	May 7, 1998	Expected 2002	–
5. National Employer Identifier	June 16, 1998	Expected 2002	–
6. Security	August 12, 1998	Expected 2002	–
7. National Health Plan Identifier	In Development	–	–
8. Claims Enforcement Procedures	In Development	–	–
9. National Individual Identifier[4]	Withdrawn	–	–

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; gives 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; establishes new criminal and civil sanctions for improper use or disclosure; establishes new requirements for access to records by researchers and others.

[3] In January, 2002 the Bush Administration extended the deadline for the ‘Electronic Transactions & Code Sets’ from Oct 2002 until October 2003.

[4] 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)

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 the American National Standards Institute (ANSI). 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 August 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:

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

The Transactions Standards regulate information related to health insurance status and remittance. GE Healthcare cardiology products are clinical systems and rarely (if ever) process the health insurance and remittance information affected by the Transactions Standards. The GE Healthcare cardiology 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 Healthcare cardiology equipment. The cardiology equipment may need to support input of code set values when test information is acquired.

B

Appendix B — Summary of MUSE Security

Introduction

The GE Healthcare Product Security web site has the *HIMSS Manufacturer Disclosure Statement for Medical Device Security* or *MDS2* form for different MUSE versions. This form has some of the same answers as those found in this section. See http://prodsecdb.gehealthcare.com/ and log in with your Single Sign On (SSO). If you do not have an SSO, click the ***Sign Up*** link to obtain one.

The following table is based on a MUSE system running version 8 without the MUSE Web option. These tables are in direct response to the need for security features in medical systems. GE Healthcare provides these answers to assist you in discovering your risks and in the creation of your mitigation plan. GE Healthcare provides 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 the 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 Healthcare 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, and so forth.	Unknown
Does the product Capture, Store, or Transmit any Patient identifiable data?	Yes
Identify the architecture that best describes this product:	3 tier application
What Operating System is this product Client based on?	Windows XP
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?	None

Can the product display a customer supplied message on boot up or login?	Yes & No, the application cannot, but Windows can at login
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 interfaces 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)	No
Direct Serial	Yes
Other	No
Does this product have a Database?	Yes, SQL Server 2005
Identify all of the Services/Protocols the product provides:	
Any Direct Network db Access (JDBC, ODBC, SQL, etc)	Yes
DICOM	No
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?	Yes
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 carriers)?	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)	10,000

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?	16 char. max
Identify all of the authentication technologies this product supports	
Windows Domain	Yes
Microsoft Active Directory	Yes
Non-Windows 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?	No
Other	No
None	No
Identify all of the User Account Reports supported:	
List of all user accounts	Yes
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:	
Unprotected Screen Saver	Yes
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	Yes
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	
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 a log?	No
Is there a time synchronization 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 changeable 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?	InSite 2, Antivirus software, Digiboard, IE, MSDE, MDAC, MMC, Disk
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 fail-safe 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)?	Yes
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 log in 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?	Yes
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?	Yes
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 equivalent 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

C

Appendix C — 21 CFR Part 11 Option

Introduction

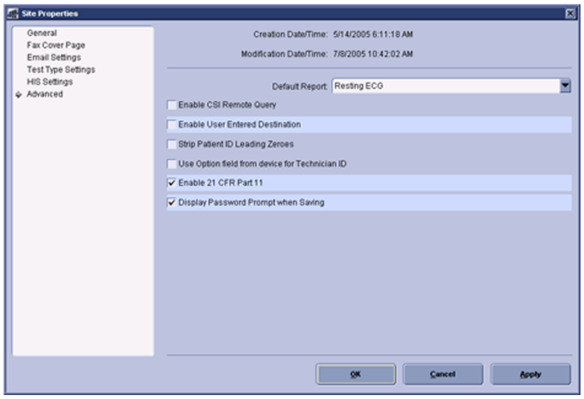
The FDA has issued regulations regarding electronic records and electronic signatures called 21 CFR Part 11. The regulations are required for customers who use the MUSE as a system to support clinical trials. This section describes the 21 CFR part 11 functionality on the MUSE system.

This option, when activated, will disable automatic changes to patient data, require entry of a reason for changes to patient data, and allows you to enable a second option to prompt for a password when patient data is changed.

Electronic Signature

21 CFR Part 11 states that users must be prompted for a password on each site when they are not biometrically authenticated. The 21 CFR Part 11 option is available with MUSE software version 7.x software. When this option is enabled, the ***Site Information*** window contains two additional check boxes.

- ***Enable 21 CFR Part 11***
- ***Require Password Prompt when saving***



Creation Date/Time: 5/14/2005 6:11:18 AM

Modification Date/Time: 7/8/2005 10:42:02 AM

Default Report: Resting ECG

□ Enable CSI Remote Query

□ Enable User Entered Destination

□ Strip Patient ID Leading Zeroes

□ Use Option field from device for Technician ID

☑ Enable 21 CFR Part 11

☑ Display Password Prompt when Saving

1. To enable 21 CFR Part 11, at ***System > Setup > Sites > Advanced***, select the ***Enable 21 CFR Part 11*** check box.
2. If biometric authentication is being used for EVERY USER on the site, select the ***Require Password Prompt when Saving*** check box.
3. If the site has some users who use biometric authentication and some users who do not use biometric authentication, select the ***21 CFR Part 11*** check box and leave ***Require Password Prompt when Saving*** unchecked.

   When ***Require Password Prompt when Saving*** is left unchecked in ***Site Setup***, the individual's user setups will be used by the system when a report is saved.

   The following table summarizes how the individual user's ***Require Password Prompt when Saving*** option functions.

User Electronic Signature Summary		
Site Setup Window	**User Setup Window**	**Prompt for Password on each Save?**
21 CFR Part 11 ☑ ***Require Password Prompt when Saving*** □	***Require Password Prompt when Saving*** ☑	Yes, for that user at that site.
21 CFR Part 11 ☑ ***Require Password Prompt when Saving*** □	***Require Password Prompt when Saving*** □	No
21 CFR Part 11 ☑ ***Require Password Prompt when Saving*** ☑	***Require Password Prompt when Saving*** ☑ -or- ***Require Password Prompt when Saving*** □	Yes, for all users at that site.

Other/Related Features

In addition to prompting the user for a password when saving a record, enabling the 21 CFR Part 11 option also affects the following features:

Feature	Description
Patient Data Merge	By default the system merges stored patient data (age, gender, race, height, and weight) when a newly acquired or diagnosis complete test is opened in the editor. If the 21 CFR Part 11 option is enabled, the system will not merge that data when an unconfirmed test is opened.
QTC Calculation	By default, the system recalculates QTC data when it is acquired from the cart. If the 21 CFR Part 11 option is enabled, this data is no longer recalculated upon its acquisition.
User Name Retrieval	By default, the system assigns user names when it acquires IDs that were entered at the card. If the 21 CFR Part 11 option is enabled, the system no longer assigns user names to these IDs.
Electronic Signature Message	The MUSE system will display the 21 CFR Part 11 eSignature Message when the password prompt appears. This message can be modified in ***System > Setup > Sites > Advanced***.
Reason for Change	The MUSE system will prompt the user for a reason for changes when updating or discarding patient data. The reason can be chosen from a list or if ***Other*** is selected, the user can type a reason.
Change Log	This feature logs changes to patient data. Enable the ***Change Log*** at ***System*** > ***Setup*** > ***Sites*** > ***Test Type Settings***, select the ***Log Changes*** check boxes for each test type. See Chapter 4 “Accounting/Logging” on page 17 for instructions on how to view the ***Change Log***.
Signature Message in Diagnosis	The MUSE system can be configured to place a signature message in the diagnosis when the test is confirmed. Enable the signature message at ***System*** > ***Setup*** > ***Sites*** > ***Test Type Settings***, select the ***Signature Message in Diagnosis*** check boxes for the desired test types.

🏭

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 5
D-79111 Freiburg Germany
Tel: +49 761 45 43 -0
Fax: +49 761 45 43 -233

Asia Headquarters
GE Medical Systems
Information Technologies, Inc.
Asia; GE (China) Co., Ltd.
No.1 Huatuo Road
Zhangjiang Hi-tech Park Pudong
Shanghai, People's Republic of China 201203
Tel: +86 21 5257 4650
Fax: +86 21 5208 2008

GE Medical Systems *Information Technologies*, Inc., a General Electric Company, going to market as GE Healthcare.

www.gehealthcare.com