CA eHealth Suite
Version 5.7 SP9
Security Target

Version 2.4
January 27, 2009

Prepared for:
CA, Inc.
100 Staples Drive
Framingham, MA 01702

Prepared by:
Booz Allen Hamilton
Common Criteria Testing Laboratory
900 Elkridge Landing Road, Suite 100
Linthicum, MD 21090-2950

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1 Security Target Introduction

This chapter presents the Security Target (ST) identification information and an overview. An ST contains the Information Technology (IT) security requirements of an identified Target of Evaluation (TOE) and specifies the functional and assurance security measures offered by the TOE.

1.1 Security Target, TOE and CC Identification

This section provides information needed to identify and control this ST and its Target of Evaluation. This ST targets Evaluation Assurance Level 2 (EAL2).

ST Title: CA eHealth Suite Version 5.7 SP9 Security Target
ST Version: 2.4
ST Publication Date: January 27, 2009
ST Author: Booz Allen Hamilton
TOE Identification: CA eHealth Suite Version 5.7 SP9
CC Identification: Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005

Note: All applicable NIAP and International interpretations have been applied in this ST.

ST Evaluator: Booz Allen Hamilton
Keywords: Network Analysis, Network Topology Management, Network Performance Management, TOE Overview, System and Application Management, Application Performance Management, End-to-End Infrastructure Management.

The TOE is the CA eHealth Suite Version 5.7 SP9 software which is a System, Application and Network Analysis and Reporting system developed by CA. The product consists of one server component with two other integrated functional components as follows:

- An eHealth Server for enterprise infrastructure analysis (TOE)
- Oracle 9i Database for storage of system and report critical information (IT Environment)
- Apache Web Server for user web and GUI interface (TOE)

The eHealth Suite is used to acquire, warehouse, analyze, display, and report on data from various nodes across a network. This ensures that client networks are online and functional. The eHealth Suite delivers performance and availability management across heterogeneous IT environments. The eHealth Suite also allows users to manage multiple IT platforms and architectures, manage network services, and achieve performance management.

Note that Concord Communications was wholly acquired by CA, Inc., hereafter referred to as CA, on June 7, 2005. Any references to Concord Communications in this document or other referenced documents were made prior to the acquisition and should be assumed to refer to CA in all cases.

1.2 Conformance Claims

This ST is CC Part 2 extended and is CC Part 3 conformant for EAL2.
This ST does not claim Protection Profile conformance.

1.3 Conventions, Terminology and Acronyms

This section identifies the formatting conventions. It also defines the terminology and meanings of acronyms used throughout this ST.

1.3.1 Conventions

This section describes the conventions used to denote Common Criteria (CC) operations on security functional and assurance components. The operations performed on these components adhere to the following conventions:

1 Iteration: Allows a component to be used more than once with varying operations. In this ST, a number in parenthesis appended to a component indicates iteration. The parenthetical is also append to the component tag. For example, FMT_MOF.1 Management of security functions behaviour (1) and FMT_MOF.1 Management of security functions behaviour (2) indicate that the ST includes two iterations of the FMT_MOF.1 component, FMT_MOF.1(1) and FMT_MOF.1(2).

2 Assignment: Allows the specification of an identified parameter. Assignments are indicated using italicised text and are surrounded by brackets (e.g., [*assignment*]).

3 Selection: Allows the specification of one or more elements from a list. Selections are indicated using bold italicised text and are surrounded by brackets (e.g., [***selection***]).

4 Refinement: Allows the addition of details. Refinements are indicated using bold text for additions to the requirements (e.g., **refinement**). In addition, refinements based upon CCIMB interpretations are indicated in red italicised text for additions, and strikethrough red italicised text for deletions (e.g., *text added* ~~*text removed*~~).

1.3.2 Terminology

The following user types are specific to this ST:

eHealth System Administrator: The eHealth System Administrator is empowered to configure the eHealth Suite, monitor deployment, user accounts and settings, and reporting options within the software. The eHealth System Administrator is assigned when the eHealth Server is initially installed and set up.

End Users: Refer to the individuals for whom web accounts have been set up on the eHealth Suite by the eHealth System Administrator. These users can view network node system settings, generate reports, and view other settings dependent upon the privileges assigned to them by the eHealth System Administrator.

1.3.3 Acronyms

The following acronyms are used in this ST:

API – Application Programming Interface
CC – Common Criteria
CCIMB – Common Criteria Interpretations Management Board
CGI – Common Gateway Interface
DB - Database
EAL – Evaluation Assurance Level
GUI – Graphical User Interface
SNMP – Simple Network Management Protocol
ST – Security Target
TOE – Target of Evaluation
TSF – TOE Security Function
UI – User Interface

1.4 eHealth Suite Version 5.7 SP9 Functional Summary

This section provides a summary of the functionality of the eHealth Suite.

1.4.1 eHealth Suite Version 5.7 SP9 Overview

The TOE is the CA' eHealth Suite Version 5.7 SP9 software which is a System, Application and Network Analysis and Reporting system developed by CA . The product consists of one server component (eHealth Suite 5.7 SP9 Server for enterprise infrastructure analysis) with three other integrated functional components as follows:

- Oracle 9i Database for storage of system and report critical information (IT Environment)
- Apache Web Server for user web and GUI interface (TOE)
- eHealth OS, Solaris 2.9, to provide access to resources (e.g., CPU, memory, disk, network) (IT Environment)

The eHealth Suite 5.7 SP9 has three interfaces that require OS authentication to access. The Motif Console, the Custom Variable (CVAR) java application and the command line interface (CLI). These interfaces are used to get the TOE into its operational state.

The eHealth Server is used to acquire, warehouse, analyze, display, and report on data from various nodes across a network. This allows the TOE to provide information to the administrator for verification that client networks are online and functional. The eHealth Suite delivers performance and availability management across heterogeneous IT environments. The eHealth Suite also allows users to manage multiple IT platforms and architectures, and manage network services.

1.4.2 eHealth Suite Version 5.7 SP9 Features

The eHealth Suite collects and analyzes data from all areas of a business infrastructure, including networks, systems, and applications. The eHealth Suite serves as a foundation for management strategies by integrating real-time management of network problems with a historical context of performance. This enables users to identify, detect, and correct problems before end-user service quality is jeopardized.

1.4.2.1 Poller Processes (TOE)

eHealth Poller Processes provide the data collection for monitored devices. Information is collected a variety of different ways through the Poller Processes via the SNMP protocol. The information is then stored by the Poller Processes to the Oracle 9i Database for future use.

1.4.2.2 eHealth Processes (TOE)

eHealth Processes provide an interface to the information stored within the Oracle 9i Database. These processes are used to facilitate interactions with the eHealth Server received from remote workstations through the Apache Web Server component.

1.4.2.3 Oracle 9i Database (IT Environment)

The Oracle 9i Database is utilized to store information that is passed to the eHealth Server from its various sources. Database sizes may vary and are set up upon initial installation and configuration of the TOE. Statistics and other data on the status of the network are stored in the database. The Oracle 9i Database is located on the same machine running the eHealth Server.

1.4.2.4 Apache Web Server (TOE)

The Apache Web Server serves multiple purposes within the eHealth Suite. Primarily it serves as the platform upon which the User Interface (UI) runs. eHealth System Administrators may login to the console and setup End User accounts. User login information is encrypted in a configuration file and is stored and protected by the host Operating System on the eHealth Server. The Apache Web Server facilitates End User access to eHealth reporting functionality to analyze data stored in the Oracle 9i Database. The Apache Web Server acts as the interface with the client machine and creates an instance of a program called nhWeb on the eHealth Server through the utilization of a Common Gateway Interface (CGI) script. The nhWeb invocation then serves as the link between the Apache Web Server and the Oracle 9i Database.

nhWeb, the Web GUI, is the primary means by which users operate the TOE. The other nh commands, such as nhManageUsers, are in turn called by nhWeb using parameters gathered from website input. As a result, the remainder of the nh suite of commands are transparent to the user because they're all indirectly accessed by using nhWeb as an intermediary.

1.5 Security Target Organization

Chapter 1 of this ST provides introductory and identifying information for the CA' eHealth Suite Version 5.7 SP9 software. Chapter 2 describes the TOE and provides some guidance on its use. Chapter 3 provides a security environment description in terms of assumptions, threats and organizational security policies. Chapter 4 identifies the security objectives of the TOE and of the Information Technology (IT) environment. Chapter 5 provides the TOE security functional requirements, the assurance requirements, as well as requirements on the IT environment. Chapter 6 is the TOE Summary Specification, a description of the functions provided by the CA' eHealth Suite Version 5.7 SP9 software to satisfy the security functional and assurance requirements. Chapter 7 provides a rationale for claims of conformance to a registered Protection Profile (PP). Chapter 8 provides a rationale, or pointers to rationale, for objectives, requirements, TOE Summary Specification, and PP claims.

2 TOE Description

This section provides a description of the TOE in its evaluated configuration. This includes identification and descriptions for the components that comprise the TOE.

eHealth discovers and collects data from existing devices, agents, and management systems in an isolated network. It provides real-time monitoring tools and reports for resources on the network. The standard eHealth product includes an integrated database, a console interface that provides scheduling and element grouping capabilities, and a Web interface that allows users to view and run reports and real-time monitoring tools from a Web browser.

The TOE will:

- Run the discover process to find the elements to manage.
- Use discover logs to interpret discover results.
- Manage the configuration information that eHealth stores about managed resources.
- Organize resources into groups to associate related resources for monitoring.
- Generate eHealth reports to obtain information about the recent performance of resources on the network.
- Use eHealth reports and tools to determine the current status of resources and identify changes.
- Provide customized eHealth reporting tools.
- Add and manage scheduled jobs for generating reports, running discover processes, and managing the database.
- Manage the amount of space that the eHealth database uses to ensure that eHealth can continue to collect data and generate reports.
- Monitor eHealth, and determine if critical processes are running or if certain events have occurred on the eHealth system.

2.1 Basic eHealth Concepts

To monitor and manage the performance of networks, systems, and applications, eHealth allows administrators to locate manageable resources, called elements, by discovering them or by importing element information from a provisioning or inventory system.

2.1.1 Elements

An element is a resource that eHealth polls and for which it collects data. eHealth polls two types of elements: statistics elements and conversation elements. Conversation elements contain information collected from Remote Network Monitoring (RMON). RMON v2 is a type of device that collects network management information, including packets sent, bytes sent, packets dropped, statistics by host, by conversations between two sets of addresses, and certain kinds of events that have occurred. A probe is an example of an RMON device. For more information, refer to RFC 2021. Note that TOE is sent information about the data collected from probes in the environment (i.e., second hand) and therefore the analysis of the RFC 2021 implementation is outside the scope of the TOE evaluation.

2.1.2 Discover

Discovery is the process by which real-world entities found on a network are recognized, and for which an element representation is then constructed. During the installation of the TOE, a TOE administrator will enter the IP address range for all the resources he/she desires to poll on the network.

2.1.2.1 Using the Discover Process

During the discover process, eHealth searches for resources with Simple Network Management Protocol (SNMP) agents at Internet Protocol (IP) addresses that TOE administrators specify. Once invoking the discover main program reads a list of user-supplied IP addresses, and first tests each address via a simple PING and SNMP request to ascertain the probable existence of an agent at that address. It then obtains information from the management information base (MIB) of each device and creates elements based on that information. When the TOE administrator saves the discover process results, eHealth stores element information in its database and its poller configuration. Once the initial address range is set by the TOE Administrators the discovery process is complete. After installation the discovery process can be scheduled to run at regular times to update information in the poller configuration. The Poller Configuration information includes a name, IP address, SNMP index numbers, and other information needed to uniquely identify the element, poll it, and report on it.

2.1.2.2 Collecting Data for Elements

After the TOE administrator identifies critical resources and creates elements for them, the TOE must collect management data from them. eHealth collects management data from polling.

2.1.2.3 Using Polling

Polling is the process of collecting statistics on network, system, and application data. The eHealth poller automatically collects data for any element in the eHealth poller configuration. When the TOE discovers an element, eHealth creates an entry for it in the poller configuration. Each entry contains the element name, the configuration information that eHealth obtained, a polling rate, and the eHealth agent type. The polling rate specifies the frequency with which eHealth polls the element. eHealth has several polling rates. The default rate—normal—is typically five minutes. The eHealth agent type classifies the type of element that eHealth discovered. eHealth automatically polls elements at the specified polling rate to collect data and store it in the Oracle 9i database.

2.1.3 Element Editing

Changes to elements are processed via the configuration server process. The configuration server maintains an in-memory image of elements in the system, and updates changes to them based on a complex set of constraints and rules (it is for this reason that an in-memory image must be maintained).

A user's changes to elements are reflected in an element operation file known as a DCI (Database Configuration Information) file. This file is then processed by the configuration server, which resolves changes to the element memory image, and stores the final results in the database.

2.2 eHealth Auditing

Statistics Polling static window messages are stored on the underlying OS in a file called messages.stats.log. On the TOE these files can reach a maximum size of 100 MB. Once the log file reaches the maximum size, eHealth moves it to a backup log file named messagesbackup.bak and overwrites the existing backup log file, if one exists. eHealth then starts a new log file using the default file name. This process is transparent to any users on the TOE; the backup process is engaged automatically and no warning is issued.

2.2.1.1 Comparing Discover Results to the Poller Configuration

eHealth records the results of the discover process in comparison to the existing poller configuration in a log file named discoverinteractive.*date.time*.log. Where data and time are retrieved from the operating system clock. This log itemizes new elements, updates to existing elements, and elements that exist in the poller configuration but that discover did not find. When eHealth compares the discovered results with any existing element definitions in the poller configuration file, it does the following:

- Creates new elements for discovered devices (such as routers, systems, switches, probes, modems) and components (such as interfaces, CPUs, memory, disks) that are not already in the poller configuration.
- Updates any existing elements, if necessary. After an interactive discover process, eHealth updates the poller configuration with both resolved and unresolved element changes.

A discover log consists of a header, a summary section, and several sections that provide details about the infrastructure changes that the discover process found. If the discover process was a scheduled discover job, the discover log specifies the discovered changes that eHealth saved in the poller configuration. The discover log does not include information about every field that is updated.

When eHealth completes the discover process, it displays the number of new elements that it discovered and the number of existing elements that it updated. It also lists updates to metadata, such as elements that have changed groups. eHealth saves these messages in the discoverResults.log file.

2.2.1.2 Discover Log Summary Section

The summary section of the discover log summarizes the information that the discover process found in two parts; Network Change Summary and Duplicate Analysis. The Network Change Details section of the discover log file contains the following subsections:

- New Elements - Specifies the number of discovered elements that are not already in the poller configuration. In the new elements resolved/unresolved entry, the discover log reports the number of new elements found that can and cannot be resolved. For a scheduled discover job, the new elements saved/unsaved entry reports the number of new elements that eHealth added to the poller configuration.
- Updated Elements - Specifies the number of existing elements that eHealth can modify with new information. In the updated elements resolved/unresolved entry, the discover log lists the number of elements that have new information and which of those elements can and cannot be resolved. For a scheduled discover job, the updated elements saved/unsaved entry lists the number of elements that eHealth updated in the poller configuration.
- Discover Key Changes - The Discover Key Changes section lists elements in the poller configuration for which the discover process changed the discover key.
- Missing Elements - Specifies the number of existing elements of the discovered type that have IP addresses falling within the range specified for the discover process, but that were not found during discover.

2.2.2 Using Discover Keys

Whenever possible, the discover process uses a discover key to uniquely identify an element. eHealth creates discover keys for newly discovered elements based on information that it obtains from the MIB at the device. When the discover process finds an element, it compares the discover key for the new element to the discover key for elements that are already in the poller configuration to determine whether the element is new.

2.2.2.1 Discover Key Formats

eHealth uses information that it obtains from the MIB to create and maintain discover keys for component elements in the poller configuration. For interfaces, the discover key also includes a component type that eHealth assigns based on discovered information. All discover keys include different fields that are based on the type of element. The table below lists the types of components for which eHealth can create discover keys and describes their format.

Component Type	**Discover Key Format**
Application service	applicationName
Application service process sets	applicationName
Ascend, Cisco, and Shiva ISDN Interfaces	ras componentType ifDescr
Ascend, Cisco, and Shiva modem interfaces	pool componentType ifDescr
ATM path on a Cisco LightStream 1010 switch	ifDescr VPI
ATM channel on a Cisco LightStream 1010 switch	ifDescr VPI VCI
Bay Networks, WellFleet, and generic Frame Relay permanent virtual circuits (PVCs); other PVCs conforming to RFC 1604	ifDescr DLCI
Cisco Catalyst 5000 Switching System interfaces	port Module-module#-Port-port#
Generic router and system interfaces	componentType ifDescr
Physical disks on systems	deviceName
Processes	processSetName
Process sets	processSetName processName – arguments
QoS	ifDescr direction elementTypeID cbQosCMName
System CPUs; router CPUs	Cpu cpu# or CIP-Cpu cpu#
System disk partitions (including SystemEDGE, Compaq, and others)	partionName

When the TOE saves the results of a discover process, eHealth creates a pollerAudit.*date*.*time*.log file. Where date and time is retrieved from the operating system clock. eHealth saves a minimum of seven files for each type of discover log. It deletes files in excess of the seven files that are older than seven days.

2.2.2.2 Matching on Physical Address

After matching on discover keys, discover compares the physical address (ipPhysAddr) of the elements with those that are stored in the poller configuration. In cases of virtual interfaces, such as Frame Relay (FR) PVCs, ATM PVCs, or workgroup hub modules (where the physical interface can be the same for more than one interface), discover uses the virtual channel identifier to identify virtual addresses within a physical one.

2.2.2.3 Comparing MIB Attributes

If the discover process has not been able to match an incoming element through the device-, agent-, and discover key-matching methods, it compares the MIB attributes of discovered elements to values in the poller configuration to determine whether the discovered elements are new. It compares attributes to identify components for which it cannot create a discover key and to identify devices. eHealth also uses this method to distinguish among two or more component elements that have identical discover keys. Identifying components by comparing MIB attributes can be unreliable because the comparison includes SNMP indexes, which can shift when the device is restarted. The discover process cannot determine whether the SNMP indexes shifted. When it finds an element on an existing device that it cannot match to an element in the poller.cfg file, the discover log lists it as resolved-new, unless the device match is weak, in which case it lists the element as unresolved-new.

2.2.2.4 Finding and Selecting Elements

To find an element, specify a string in the Search for Name field of the Poller Configuration dialog box. Users can use wildcards such as an asterisk (*) to match zero or more characters, or a question mark (?) to match any single character. If a wildcard is not used, the filter displays the elements that contain the specified string anywhere in the name. If the Search for Name field is not complete, the filter displays all elements.

The element list scrolls to the first name that matches the search string. Click Find Next to find the next element that matches the search string. Click Find Previous to find the previous match. When the search reaches the end of the list, a message appears at the bottom of the dialog box. Click Find Next to restart the search.

2.2.3 Collecting Historical Data on Resources on the Network

During installation a discovery process is run to baseline the network resources. After the discovery process has initially populated the database, the TOE uses the poller process to collect historical data on the various elements in the database. The historical data and discovery process update or create elements in the Oracle 9i database. The Poller interface to Oracle is done via an API that performs Oracle Procedure Library calls. These API calls perform inserts and updates to the database. To evaluate the health of network resources, eHealth uses the historical data that it collects to analyze trends and calculate averages. It collects data over a period of time—defined as a baseline period—and calculates a Health Index for various elements polled by the TOE. This index grades the performance of each element based on the utilization and number of errors that eHealth detects. eHealth uses upper limits for utilization and errors, referred to as Trend thresholds, to identify problem areas.

2.2.3.1 Running At-a-Glance Reports

At-a-Glance reports provide a series of charts that show the performance of a specified element during the report period. These charts show the trends for important performance variables for an element. The TOE will compare the activity of several variables to identify related events. Users can run At-a-Glance reports that contain data for part of a day, a single day, several days, a week, several weeks, or a month. At-a-Glance reports for Availability always show actual availability and note when planned downtime occurred. Planned, or scheduled, downtime is the time during which an element in the IT infrastructure is shut down for system maintenance, upgrades, or moves.

The TOE Administrator can restrict end users from running particular reports by modifying their Web user accounts as described in section 2.3.

2.2.3.2 Running Top N Reports

A Top N report is a tabular report that lists all elements in a group, or all elements in a group that exceed or fall below the report criteria goals specified by the TOE Administrator. While troubleshooting the infrastructure or planning for upgrades, Top N reports can identify elements on which to focus management efforts. Users can also use Top N reports to specify a service goal used to compare the performance of the elements that match the report criteria.

For example, Top N report can be configured to show the following:

- 50 LAN/WAN elements that have a bandwidth utilization above 40%
- All system partitions with less than 20% space utilization
- 15 routers that have an average line utilization above 90%, incoming discards greater than 100 frames per second, and outgoing discards greater than 150 frames per second
- All elements in the group Boston-to-NewYork

2.2.3.3 Running Trend Reports

Trend reports analyze the performance of an element or a group of elements based on specific variables. These reports can identify the cause of an unsatisfactory health rating on a specific element, or the performance of a group of elements. They provide information on a single variable for one to ten elements, or on one to ten variables for a single element or a group. Users can select a report period of several hours in a day to a maximum of several days or weeks. Users can display these trends in a variety of chart formats, including line graphs, pie charts, bar charts, or tables. Trend reports for Availability always show actual availability and note when planned downtime occurred.

2.2.3.4 Running eHealth Reports

eHealth is able to evaluate the health of all or a group of elements based on utilization and errors that it detects. The TOE can create Health reports for any network product (for example: LAN/WAN, Router, System, and so on). eHealth reports provide a series of charts that allow users to compare current performance to historical performance for all elements or for a group of elements. When showing availability in a Health report, users can take planned downtime into account.

2.2.3.5 How eHealth Reports Analyze Data

eHealth compares the data for the specified report period to the same type of data that has been retained over a period of weeks. By comparing current data with historical data, users can identify normal patterns of behavior, as well as drastic changes in that behavior. Changes in behavior usually indicate that problems are about to occur or already have occurred. eHealth reports use a service profile to define the analysis ranges and thresholds used for health evaluation.

2.2.3.6 Providing Web Security for Trend and At-a-Glance Reports

The Web User field in the Trend and At-a-Glance Run Report (and Scheduled Report) dialog boxes allows TOE administrators to provide Web security for Trend and At-a-Glance reports that are not associated with groups. TOE administrators can specify a Web user name in this field to specify the name of the only Web user—aside from the Web administrator—who can view Web Trend and At-a-Glance reports. This user is the only user who can view these reports. TOE administrators can also specify multiple user names separated by commas.

2.2.3.7 eHealth Web Server

eHealth provides a Web interface that allows users to access eHealth reports and real-time tools. The Web interface allows users to access eHealth from any remote system using a Web browser. The standard eHealth product provides users with the capability to use the Web server and software to do all of the following:

• View eHealth reports that are run from the eHealth console.
• Generate and view eHealth reports from a Web browser (if the the Web user account has the appropriate permissions).
• Create customized MyHealth report pages that summarize critical resource information.

2.3 eHealth Suite Version 5.7 SP9 Evaluation Scope

This section provides identification and descriptions for the components that comprise the TOE.

2.3.1 Physical Boundary

The TOE runs on a Sun SunFire V210 running Solaris 2.9 that meets the physical hardware requirements as outlined in section 2.3.2.1. to ensure that there is sufficient space for all of the components. The physical boundary of the TOE includes the eHealth Suite Version 5.7 SP9 server software as depicted in Figure 1 and is responsible for implementing the TOE's security functional requirement components. As seen below the Oracle 9i database is installed on the same physical server before the eHealth TOE is installed. The TOE interface to Oracle used to manipulate the database is done via an API that performs Oracle Procedure Library calls. Note: HTTP port 80 is only used for TOE installation, the TOE does not support Port 80 traffic while in operation.

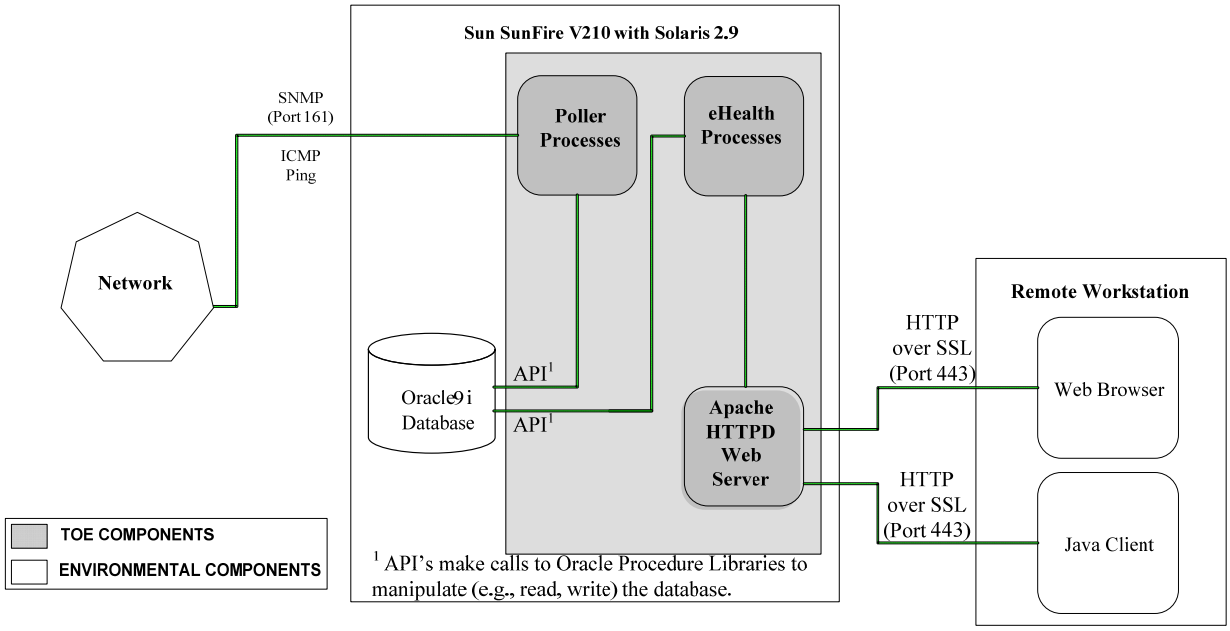

Figure 1 – eHealth Server Physical Boundary

2.3.2 Physical Boundary Components

This section lists the hardware and software components of the product and denotes which are in the TOE and which are in the environment.

2.3.2.1 Hardware Components

This table identifies hardware components and indicates whether or not each component is in the TOE.

TOE or Environment	Component	Description
Environment	eHealth Server UNIX Platform	Sun SunFire V210 running Solaris 2.9 440 MHz CPU 2 GB memory 140 GB Diskdrive
Environment	Remote Workstation Platform	Any standard Windows or Unix workstation, running an approved web browser with javascript enabled Specific version numbers are specified in the Software Components section.

2.3.2.2 Software Components

This table identifies software components and indicates whether or not each component is in the TOE.

TOE or Environment	Component	Description
TOE	eHealth Suite Version 5.7 SP9	Software package installed includes all TOE items listed below: Poller Processes eHealth Processes Apache Web Server v1.3.31 with mod_SSL.
Environment	Solaris 2.9	eHealth Operating System
Environment	Oracle 9i Database	Oracle Database, update 9.2.0.3
Environment	Web Browser	Remote Web Browser with javascript enabled UNIX systems: Mozilla Ver. 1.2.1 or later Windows systems: Internet Explorer Ver. 6.0 or later, Netscape Ver. 7.1 or later, and Mozilla Ver. 1.6 or later

2.3.2.3 Network

The eHealth Server receives information from various different nodes on the network depending on how the eHealth System Administrator configures the TOE to operate. Communications traverse between network nodes and the eHealth Server via the IETF Standard SNMP protocol version 1. eHealth will work with any SNMP manageable device that has defined MIB support which can be certified and supported with eHealth. The SNMP management devices are listed at http://support/concord/devices/.

2.3.2.4 Operating Systems and Applications

2.3.2.4.1 Solaris 2.9

eHealth relies on the OS to provide access to resources (e.g., CPU, memory, disk, networking). Before installation of eHealth the underlying OS (i.e., Solaris 2.9) is configured. All external interfaces to the TOE are disabled with the exception of the HTTP over SSL, Oracle API's, SNMP, and ICMP interfaces as described in figure one above. Physical access to the TOE is initial required for installation but once the TOE is in its operational state no further direct access to the TOE is required. Users of the TOE will interact through the HTTP over SSL interface via a remote workstation. Administrators of the TOE will interact through local access to the Motif console and the HTTP over SSL interface via a remote workstation.

2.3.2.4.2 Oracle 9i

eHealth includes an integrated database, which in Release 5.7 SP9 is the Oracle9i database. (This database is a product that was developed by the Oracle Corporation and not part of the TOE). The evaluated version of Oracle 9i is installed on the Solaris platform before the eHealth Suite is installed. Once installed properly, direct user access to Oracle 9i is not required. Users do not interact directly with Oracle 9i. Users interact directly with the TOE and the TOE access the Oracle 9i database as required to perform its functions, therefore Oracle 9i does not have any externally visible user nor network interfaces. The TOE interface to Oracle used to manipulate the database is done via an API that performs Oracle Procedure Library calls. eHealth uses the database to save all of its element information, polled data(the report data that it collects from critical resources on the network), and poller configuration settings. When the TOE save the results of a discover process, eHealth creates an entry in the database for each element that the discover process found. After each poll, eHealth saves the data it collected for each discovered element in the database.

2.3.2.5 Remote Workstations

End Users of the eHealth Suite interact with the product through the use of HTTP over SSL and a web browser which uses HTML. While the system is configured using HTTP by default, the TOE is configured to use HTTP over SSL for the evaluated configuration. The GUIs then connect directly to the Apache Web Server. The eHealth Apache Web Server relies on the remote web browser in the IT environment to perform all necessary SSL functions to facilitate data encryption and secure communication between remote users and the TOE.

2.3.3 Logical Boundary

The logical boundary of the TOE includes the eHealth Suite Version 5.7 SP9 Server software. This component enforces Authorisation, Authentication, Audit, Data Protection, and Security Management as described in the following subsections.

2.3.3.1 Authorisation

eHealth Suite Authorization protects the server resources from unauthorized access. An End User's capability of accessing pages and files, and running applications or reports are controlled by the corresponding authorization policy.

Access privileges granted to users are managed by the eHealth application. The eHealth application stores the user privilege information on a CSV file on the operating system where eHealth runs. When a user requests content from the eHealth application, the eHealth application will validate the authorization to this content by comparing the validated username provided by the web server with the list of access rights on the Authorization database (CSV). For database access, the eHealth application verifies that the OS user has access to the Oracle database and grants it DBA rights. Additional accounts are granted read only access rights.

The eHealth admin has the privileges associated with the eHealth account created and maintained by the underlying Operating System (i.e., Solaris 2.9). This account will have access to the various files used by the TOE and stored and protected by the underlying OS.

2.3.3.2 Authentication

Authentication services are handled internally through passwords. eHealth Authentication is the process of determining the End User's true identity and mapping them to the appropriate role (i.e., eHealth administrator or End User). This is enforced by the TOE. Authentication through remote access is the only allowed access to the TOE in its operational configuration. The end users identity and password is maintained in a web server configuration file stored on the local Solaris file system.

A remote workstation will use an authorized web browser (see section 2.3.2.2) to interact with the TOE via the SSL Web interface port 443 to the Apache Web Server. A username and password request is issued by the web server. The user provides a username and password to the web server which is passed to the eHealth server via an industry standard web browser, see section 2.3.2.2. for the supported web browsers. The Apache web server will validate the users claimed credentials against password and usernames stored in a web server configuration file stored on the local file system. The TOE will return the success or failure of the authentication process. If properly authenticated, the web server provides the username that has been authenticated to the eHealth application. TOE passwords are stored locally on the operating system in their encrypted form (MD5). When a user presents his password to the TOE it is also hashed with MD5 and the two hashes are compared, if the hash matches then access is allowed.

2.3.3.3 Audit

The TOE generates audit records for selected security events. Events are tracked based on occurrence and who triggered them. Results are recorded to a local log text file on the eHealth Server that is stored and protected by the host Operating System. Logins can be audited via log files prepared by the web server, and displayed to the privileged (administrative user) via the web interface. This login log file is also protected and stored on the host Operating System. As a result, the eHealth System Administrator can utilize the contents of the log files for further processing. A web browser in the TOE environment is required to read the audit records. The eHealth System Administrator interacts with the TOE from a Remote Workstation. The eHealth System Administrator is required to successfully identify and authenticate themselves to the TOE before being granted permission to review the generated audit information.

2.3.3.4 Data Protection

The access control features of the underlying operating system protects all the TOE data. Local access is not permitted by any user other than an authorized IT environment administrator that has an account on the local machine. End Users log on to the machine via a Remote Workstation, and are not permitted to edit any of the information stored on the eHealth Server.

2.3.3.5 Protected Data Transmission

The TOE uses an Apache web-server to support protection of external TOE communication with the users by performing SSL encryption through Apache's OpenSSL-based cryptographic module (mod_SSL). The TOE uses openssl v9.7d. The protocol for transport is HTTP over the Secure Socket Layer protocol, sometimes referred to as "HTTPS" or "HTTP over SSL." HTTP over SSL can be used as the secure communication between the eHealth server and the remote workstation. The eHealth server relies on the users web browser in the IT environment to perform the SSL protocol with its associated cryptography to process certificates for authenticating the end points of the communication channel and to encrypt the data. The cryptographic functionality of the TOE uses valid parameters so that full faith can be placed in the strength of the encryption.

2.3.3.6 Partial TOE Self Protection

Working in concert with its platform, the TOE works with the IT environment (OS and DB) to provide protection of its security functions through non-bypassability and domain separation. All user operations are conducted in the context of an associated session. The TOE manages these sessions to prevent one session from compromising another session. The TOE provides only well-defined interfaces to these sessions, and the sessions allocated only after successful authentication, or when a session is requested from the physically protected local console which is under procedural control. The TOE relies on its platform to operate correctly and to prevent unauthorized access to TOE data and stored executables.

2.3.3.7 Security Management

Security Management is handled by an authorized eHealth Systems Administrator via the Remote Workstation. Access to the Security Management user interface is secured by the core operating system authentication scheme and role based permissions. Administrators are permitted to edit user account attributes and access permissions while end users are denied these privileges.

2.3.4 Evaluated Configuration

The scope and requirements for the evaluated configuration are summarized as follows:
The eHealth Suite Version 5.7 SP9 software (i.e., the TOE) will be installed on the eHealth Server machine with the Solaris 2.9 operating system installed.

The Oracle 9i Database, base version 9.2.0.3, will communicate with the eHealth Suite Version 5.7 SP9 software and will be installed on the eHealth Server machine. The following **optional** components, are licensed separately and not required for proper security operation of the TOE, and therefore they are not part of the evaluated configuration of the TOE:

- SystemEDGE
- Live Health
- OneClick for eHealth (OCE)
- TrapEXPLODER
- Application Response
- Service Availability

2.3.5 System Requirements

This section identifies the hardware and software requirements for the platforms described in the evaluated configuration. The TOE will be evaluated in on a UNIX platform only. This configuration is detailed in the following subsection.

2.3.5.1 eHealth Server UNIX Platform

For the evaluated configuration on the UNIX platform, the TOE will be tested on the following hardware device:
Sun SunFire V210 running Solaris 2.9
440 MHz CPU
2 GB memory
140 GB Diskdrive

2.3.5.2 Remote Workstation Platform

For the evaluated configuration of the TOE, the Remote Workstation can be any standard Windows or UNIX workstation that includes a web browser from the following list:

Mozilla Version 1.2.1 or later (UNIX)
Internet Explorer Version 6.0 or later (Windows)
Netscape Communicator Version 7.1 or later (Windows)
Mozilla Version 1.6 or later (Windows)

3 Security Environment

3.1 Threats to Security

This section defines the threats to security. The TOE security environment consists of the threats as they relate to the TOE and the IT environment protected by the TOE

T.ACCESS A legitimate user of the TOE could gain unauthorized access to resources or information protected by the TOE, or perform operations for which no access rights have been granted, via user error, system error, or other actions.

T.ADMIN_ERROR An administrator may incorrectly install or configure the TOE, or install a corrupted TOE resulting in ineffective security mechanisms.

T.MODIFY Users, whether they be malicious or non-malicious, could attempt to misconfigure or modify their user accounts in an attempt to tamper with TOE resources or modify security information relative to the TOE.

T.PROTECT A user or process may cause, through an unsophisticated attack, TSF data, or executable code to be inappropriately accessed (viewed, modified, or deleted)..

T.MASK Users whether they be malicious or non-malicious, could gain unauthorised access to the TOE by bypassing identification and authentication countermeasures.

T.DOS Users or network services, whether they be malicious or non-malicious, could attempt to disable or degrade the performance of networks, systems, or applications in the network.

T.UNKNOWN Network devices, whether they be malicious or non-malicious, could be added to the IT Environment unknown to the TOE and disable or degrade the performance of networks, systems, or applications in the network.

T.EAVESDROPPING Malicious users could monitor (e.g., Sniff) network traffic in an unauthorized manner.

T.CRYPTO_COMPROMISE A malicious user or process may cause key, data or executable code associated with the cryptographic functionality to be inappropriately accessed (viewed, modified, or deleted), thus compromise the cryptographic mechanisms and the data protected by those mechanisms.

3.2 Secure Usage Assumptions

The specific conditions listed in this section are assumed to exist in the TOE environment. These assumptions are necessary as a result of practical realities in the development of the TOE security requirements and the essential environmental conditions on the use of the TOE.

Personnel Assumptions

A.ADMIN One or more authorised administrators will be assigned to install, configure and manage the TOE and the security of the information it contains.

A.NOEVIL Users of the TOE are not careless, wilfully negligent, or hostile and will follow and abide by the instructions provided by the guidance documentation.

A.PATCHES System Administrators exercise due diligence to patch the IT Environment (e.g., OS and database) so they are not susceptible to network attacks.

A.PASSWORD It is assumed that users will select strong passwords according to the policy described in the administrative guidance and will protect their authentication data

Logical Assumptions

A.LOCATE The network the TOE will monitored is isolated form any other network. The SNMP monitored traffic is limited to the isolated intranet, (i.e., no connections exist to other networks).

Physical Assumptions

A.PROTECT The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.

3.3 Organisational Security Policies

There are NO organizational security polices that apply to the TOE.

4 Security Objectives

This chapter provides a listing of security objectives to ensure that all of the security threats listed in Chapter 3 have been countered. The security objectives are divided into Security Objectives for the TOE (Section 4.1) and Security Objectives for the IT environment (Section 4.2).

4.1 Security Objectives for the TOE

The following security objectives are to be satisfied by the TOE.

O.ACCESS The TOE will provide measures to authorise End Users to access specified TOE resources once the user has been authenticated. User authorisation is based on access rights configured by the eHealth System Administrator of the TOE.

O.AUDIT The TOE will provide measures for recording security-relevant events that will assist the eHealth System Administrators in detecting misuse of the TOE and/or its security features, or in detecting events that would compromise the integrity of the TOE and violate the security objectives of the TOE.

O.IDEN The TOE will provide measures to uniquely identify End Users and will authenticate the claimed identity prior to granting a user access to the TOE.

O.ROBUST_ADMIN_GUIDANCE The TOE will provide administrators with the necessary information for secure delivery and management.

O.SELF_PROTECTION The TSF shall provide protection for itself and its resources from external interference, tampering or unauthorized disclosure, through its own interfaces.

O.MANAGE The TOE will provide eHealth System Administrators with the resources to manage and monitor user accounts, resources and security information relative to the TOE.

O.MONITOR The TOE will collect and analyze critical data for network devices, systems, and applications and report on the performance, capacity, availability, and response of these resources.

O.DISCOVER The TOE will discover new network devices added to the IT environment and report to the TOE when those devices are discovered.

O.CRYPTOGRAPHIC_FUNCTIONS The TOE shall provide cryptographic functions for its own use, including encryption/decryption and password hashing. This will assist authorized users in preventing unauthorized monitoring of networks or information systems that would compromise the integrity of the TOE and violate the security objectives of the TOE.

4.2 Security Objectives for the IT Environment

The following security objectives for the IT environment of the TOE must be satisfied in order for the TOE to fulfill its security objectives.

4.2.1 Security Objectives for the IT Environment

OE.SYSTIME The IT environment will provide reliable system time.

OE.FILESYS The security features offered by the underlying Operating System protect the files used by the TOE.

OE.PROTECT The IT environment will work in concert with the TOE to protect it from unauthorised modifications and access to its functions and data within the TOE, through the IT Environment’s interfaces within is scope of control.

4.2.2 Security Objectives for the Non-IT Environment

OE.ADMIN One or more eHealth System Administrators will be assigned to install, patch, configure and manage the TOE and the security of the information it contains.

OE.NOEVIL Users of the TOE are not careless, wilfully negligent, or hostile and will follow and abide by the instructions provided by the guidance documentation.

OE.LOCATE The TOE will be located on an isolated network with no connections to other networks.

OE.PROTECT The parts of the TOE critical to security policy enforcement will be protected from unauthorised physical modification.

OE.PASSWORD Users of the TOE shall ensure that they choose strong passwords and that they protect their authentication data as instructed by the administrator guidance.

5 IT Security Requirements

This chapter identifies the security requirements for the TOE and its IT Environment. The operations performed on Security Functional and Security Assurance Requirement components contained in this section adhere to the conventions as prescribed in Section 1.3.1 of this ST.

5.1 TOE Security Functional Requirements

The following table provides a summary of the Security Functional Requirements implemented by the TOE.

Table 1 – TOE Security Functional Requirements

Security Functional Class	Security Functional Component
Security audit (FAU)	FAU_GEN.1 Audit data generation
	FAU_GEN_EXP.1(1)Discovery Log Generation
	FAU_GEN_EXP.1(2) Poller Audit Generation
	FAU_GEN_EXP.1(3) Message Log Generation
	FAU_GEN_EXP.1(4) eHealth Report Generation
	FAU_GEN.2 User identity association
	FAU_SAR.1 Audit review
	FAU_SAR_EXP.1(1) Audit review
	FAU_SAR.2 Restricted audit review
	FAU_SAR.3 Selectable audit review
Cryptographic Support (FCS)	FCS_CKM.1 Cryptographic Key Management
	FCS_CKM.4 Cryptographic key destruction
	FCS_COP.1(1) Cryptographic Operations
	FCS_COP.1(2) Cryptographic Operations
User data protection (FDP)	FDP_ACC.1 Subset access control
	FDP_ACF.1 Security attribute based access control
Identification and authentication (FIA)	FIA_ATD.1 User attribute definition
	FIA_UAU.2 User authentication before any action
	FIA_UID.2 User identification before any action
Security Management (FMT)	FMT_MOF.1 Management of security functions behavior (1)
	FMT_MOF.1 Management of security functions behavior (2)
	FMT_MSA.2 Secure Security Attributes
	FMT_MSA.3 Static Attribute Initialization
	FMT_MTD.1 Management of TSF data (1)
	FMT_MTD.1 Management of TSF data (2)
	FMT_MTD.1 Management of TSF data (3)
	FMT_SMF.1 Specification of management functions

Security Functional Class	Security Functional Component
	FMT_SMR.1 Security roles
Protection of the TSF (FPT)	FPT_RVM_EXP_TOE.1 Reference Mediation: TOE
	FPT_SEP_EXP_TOE.1 Domain Separation: TOE
Trusted Path/Channels (FTP)	FTP_TRP.1 Trusted Path

The following subsections present the details for each of the TOE Security Functional Requirement components.

5.1.1 Security audit (FAU)

5.1.1.1 FAU_GEN.1 Audit data generation (1)

Hierarchical to: No other components.

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:
a) Start-up and shutdown of the audit functions;
b) All auditable events for the [***not specified***] level of audit; and
c) [generation of reports, viewing of reports, login, and self password changes].

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:
a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and
b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [IP address of the Remote Workstation from which a page was accessed, End User account name, date and time at which the page was accessed, name of the operation that was performed, pathname of the page visited, return code, and the total amount of data (in bytes) that was transferred].

Dependencies: FPT_STM.1 Reliable time stamps

Application Note: The audit records referred to in these SFR's are captured in the Web Server Log httpd-log and httpd-error.

5.1.1.2 FAU_GEN.2 User identity association

Hierarchical to: No other components.

FAU_GEN.2.1 The TSF shall be able to associate each auditable event with the identity of the user that caused the event.

Dependencies: FAU_GEN.1 Audit data generation
FIA_UID.1 Timing of identification

5.1.1.3 FAU_GEN_EXP.1(1) Discovery Log Generation

Hierarchical to: No other components.

FAU_GEN_EXP.1.1(1) The TSF shall be able to generate a discovery log based on the following logical or physical elements:
Audit: Device [system name, unique device ID, IP address]
Audit: Agent [MTF, SNMP port, enterprise ID]
Audit: Element [LAN/WAN Elements, Router/Switch Elements, Traffic Accountant System, Application, Modem Pool and Remote Access Server, Response, QoS]

FAU_GEN_EXP.1.2(1) The TSF shall record within each server object discovery log at least the following information: [
Host
Discover Methods
IP Addresses
IP Exclusion File].

Application Note: The discovery logs probe a range of network IP addresses set by the administrator during installation. The discovery process is run periodically after that and element field changes and new elements found are stored in this log file. After installation the discovery process can be scheduled to run at regular times or run manually from the local console to update information in the poller configuration.

5.1.1.4 FAU_GEN_EXP.1(2) Poller Audit Generation

Hierarchical to: No other components.

FAU_GEN_EXP.1.1(2) The TSF shall be able to generate a poller audit log based on [*collected MIB information from devices on the network]*

Application note: Devices are a set of supported products as specified in [Certified Device List, updated quarterly]

FAU_GEN_EXP.1.2(2) The TSF shall record within each entry of the poller audit log at least the following information: **[**the exact time the change is made, the user id for the user who makes the change, the type of change made and the name of the device and whether the change operation is successful or not].

Dependencies: FPT_STM.1 Reliable time stamps

Application Note: During installation, the Poller component of the TOE populates the Oracle database with information on devices eHealth monitors in database objects called “elements”. Poller audit logs track changes to these elements. The Poller interface to Oracle is done via an API that performs Oracle Procedure Library calls. These API calls perform inserts and updates to the database.

5.1.1.5 FAU_GEN_EXP.1(3) Message Log generation

Hierarchical to: No other components.

FAU_GEN_EXP.1.1(3) The TSF shall be able to generate a message log based [*all internal running process and program events eHealth monitors]*

FAU_GEN_EXP.1.2(3) The TSF shall record within each entry of the message log at least the following information: **[**the exact date and time the event occured, the process and job id who invoked the event, the type of event and the status of the event (i.e., whether the event operation is successful or not)].

Dependencies: FPT_STM.1 Reliable time stamps

Application Note: Message logs capture messages from all other internal running processes and programs in the TOE. For example the messages will contain information on jobs that started and finished by the TOE, as well as error messages. .

5.1.1.6 FAU_GEN_EXP.1(4) Report generation

Hierarchical to: No other components.

FAU_GEN_EXP.1.1(4) The TOE shall be able to generate reports of statistical data stored in the Oracle 9i database generated by poller process.

Application Note: These reports pull from data generated as a result of the poller process. Specific report types are discussed in section 2.2.3. The standard report types are trend, top N, and at-a-glance.

FAU_GEN_EXP.1.2(4) The TOE shall be able to generate a report list of eHealth reports generated by any authorized user of the TOE.

FAU_GEN_EXP.1.3(4) The TOE shall display within each report record the following information: Date and time of the event, type of event, the element, title of the report, group the element belongs to, and the type of report that was run

Dependencies: FPT_STM.1 Reliable time stamps

Application Note: This report list refers to the ability of the TOE to preserve a list of reports run by all users of the TOE.

5.1.1.7 FAU_SAR.1 Audit review

Hierarchical to: No other components.

FAU_SAR.1.1 The TSF shall provide [eHealth System Administrators] with the capability to read [the IP address of the Remote Workstation from which a page was accessed, End User account name, date and time at which the page was accessed, name of the operation that was performed, pathname of the page visited, return code, and the total amount of data (in bytes) that was transferred] from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

Dependencies: FAU_GEN.1 Audit Data Generation

5.1.1.8 FAU_SAR.2 Restricted audit review

Hierarchical to: No other components.

FAU_SAR.2.1 The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

Dependencies: FAU_SAR.1 Audit review

Application Note: The TOE can restrict the ability of users to see elements in various reports based on group membership of the user and the element. If the element and user are in the same group access is allowed.

5.1.1.9 FAU_SAR.3 Selectable audit review

FAU_SAR.3.1 The TSF shall provide the ability to perform [**sorting**] of audit data based on [user identity, page type, individual statistics, time range, Remote Workstation node].

Dependencies: FAU_SAR.1 Audit review

5.1.1.10 FAU_SAR_EXP.1(1) Audit review

Hierarchical to: No other components.

FAU_SAR_EXP.1.1(1) The TSF shall provide [End Users and eHealth administrator] with the capability to read [all information] collected in [FAU_GEN_EXP.1(1), FAU_GEN_EXP.1(2), FAU_GEN_EXP.1(3), FAU_GEN_EXP.1(4)] from the [discover logs, poller audit logs, message logs, and eHealth reports].

Dependencies: FAU_GEN_EXP.1(1) Discovery log generation
FAU_GEN_EXP.1(2) Poller audit generation
FAU_GEN_EXP.1(3) Message log generation
FAU_GEN_EXP.1(4) Report generation

5.1.2 Cryptographic Support (FCS)

The cryptography used in this product has not been FIPS certified nor has it been analyzed or tested to conform to cryptographic standards during this evaluation. All cryptography has only been asserted as tested by the vendor.

5.1.2.1 FCS_CKM.1 Cryptographic key generation

Hierarchical to:	No other components.
FCS_CKM.1.1	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [RSA] and specified cryptographic key sizes [1024 bits] that meet the following: [ANSI X9.31 and ANSI X9.80].
Dependencies:	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction FMT_MSA.2 Secure security attributes
Application note:	This SFR supports key generation for SSL.

5.1.2.2 FCS_CKM.4 Cryptographic key destruction

Hierarchical to:	No other components.
FCS_CKM.4.1	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [overwrite method] that meets the following: [no standard].
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FMT_MSA.2 Secure security attributes
Application note:	This SFR supports key destruction for SSL.

5.1.2.3 FCS_COP.1 Cryptographic operation (1)

Hierarchical to:	No other components.
FCS_COP.1.1(1)	The TSF shall perform [encryption and decryption] in accordance with a specified cryptographic algorithm [3DES-EDE-CBC] and cryptographic key sizes [168 bits] that meet the following: [FIPS 46-3].
Dependencies:	[FDP_ITC.1 Import of user data without security attributes Or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
Application Note:	This SFR supports the mod_ssl module used in the Apache Web Server component of the TOE.

5.1.2.4 FCS_COP.1 Cryptographic operation (2)

Hierarchical to:	No other components.
FCS_COP.1.1	The TSF shall perform [password hashing] in accordance with a specified cryptographic algorithm [MD5] and cryptographic key sizes [64 bit] that meet the following: [RFC 1321].
Dependencies:	[FDP_ITC.1 Import of user data without security attributes Or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
Application Note:	This SFR supports the mod_auth_digest module used in the Apache Web Server component of the TOE.

5.1.3 User data protection (FDP)

5.1.3.1 FDP_ACC.1 Subset access control

Hierarchical to: No other components.
FDP_ACC.1.1 The TSF shall enforce [Discretionary Access Control] on [all operations among user and elements].
Dependencies: FDP_ACF.1 Security attribute based access control
Application Note: Users are assigned to groups which is synonymous with roles.

5.1.3.2 FDP_ACF.1 Security attribute based access control

Hierarchical to: No other components.
FDP_ACF.1.1 The TSF shall enforce the [Discretionary Access Control] to objects based on the following: [elements, groups, group lists]

Application Note: Elements are assigned to groups and placed into group lists. Users are also assigned to groups. If the group a user belongs to is the same as the group associated with an element read access for that element is authorized for that user by the TOE.

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [users are assigned to groups to control their access to read elements].

See Application Note for FDP_ACF.1.1 for more information.

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [a user that is the admin can access objects regardless of privileges].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the [no rules]

Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialisation

5.1.4 Identification and authentication (FIA)

5.1.4.1 FIA_ATD.1 User attribute definition

Hierarchical to: No other components.
FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [*userID, password, groups, grouplists*].
Dependencies: No dependencies.

See Application Note for FDP_ACF.1.1 for more information.

5.1.4.2 FIA_UAU.2 User authentication before any action

Hierarchical to: FIA_UAU.1
FIA_UAU.2.1 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.
Dependencies: FIA_UID.1 Timing of identification

5.1.4.3 FIA_UID.2 User identification before any action

Hierarchical to: FIA_UID.1
FIA_UID.2.1 The TSF shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user.
Dependencies: No dependencies

5.1.5 Security Management (FMT)

5.1.5.1 FMT_MOF.1 Management of security functions behaviour(1)

Hierarchical to: No other components.

FMT_MOF.1.1(1) The TSF shall restrict the ability to [**determine the behaviour of, disable, enable, modify the behaviour of**] the functions [modify system settings, modify user settings] to [the eHealth System Administrators].

Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

Application Note: The user and system settings are explicitly defined in FMT_SMF.1.

5.1.5.2 FMT_MOF.1 Management of security functions behaviour(2)

Hierarchical to: No other components.

FMT_MOF.1.1(2) The TSF shall restrict the ability to [**enable]** the functions [*generate views of the Elements stored in Oracle 9i*] to [authenticated users].

Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

Application Note: Groups are used to control access permissions for eHealth users. A user can only view (i.e., read, or create reports based on the view) the Elements stored in the Oracle 9i database for which his group matches a group associated with the Element. eHealth Administrators can view and create reports on any Elements in the database. See the application note for FDP_ACF.1.1 for more information.

5.1.5.3 FMT_MSA.2 Secure Security Attributes

Hierarchical to: No other components.

FMT_MSA.2.1 The TSF shall ensure that only secure values are accepted for security attributes.

Dependencies: ADV_SPM.1 Informal TOE security policy model
[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]
FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

5.1.5.4 FMT_MSA.3 Static Attribute Initialization

Hierarchical to: No other components.

FMT_MSA.3.1 The TSF shall enforce the [*Discretionary Access Control Policy*] to provide [**restrictive**] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [*eHealth System Administrators*] to specify alternative initial values to override the default values when an object or information is created.

Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

5.1.5.5 FMT_MTD.1 Management of TSF data(1)

Hierarchical to: No other components.

FMT_MTD.1.1(1) The TSF shall restrict the ability to [***query***] the [*eHealth reports*] to [*Authenticated Users*].

Dependencies: FMT_SMF.1 Specification of management functions

FMT_SMR.1 Security roles
Application Note: This SFR is used to restrict the ability to query eHealth reports generated by TOE users, see section 6.1.4.3 for more information on eHealth Reports.

5.1.5.6 FMT_MTD.1 Management of TSF data(2)

Hierarchical to: No other components.
FMT_MTD.1.1(2) The TSF shall restrict the ability to [**modify**] the [user password] to [the specific End User, eHealth System Administrator].
Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

5.1.5.7 FMT_MTD.1 Management of TSF data(3)

Hierarchical to: No other components.
FMT_MTD.1.1(3) The TSF shall restrict the ability to [**modify**] the [End User Profiles, Access Permissions] to [eHealth Systems Administrators].
Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles
Application Notes: End user profiles are used by the eHealth administrators to set users permissions, change passwords, and restrict access to various eHealth reports.

5.1.5.8 FMT_SMF.1 Specification of management functions

Hierarchical to: No other components.
FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions: [

1. set or change the password of a user and force a user to change his or her own password;
2. Define Custom Reports
3. Invoke the Discover Program
4. Schedule Tasks
5. View the message logs
6. Add, delete, view, and Modify users and user Attributes (including passwords)
7. View User Attributes (administrators only)
8. Create, Modify or Delete Grouplists
9. Create New or Modify Groups
10. Run eHealth Reports (At-A-Glance, Top N, and Trend)
11. Query eHealth Reports (At-A-Glance, Top N, and Trend)
12. View the Web Access Logs]

Dependencies: No dependencies.

Application Notes: These functions are accomplished via the Web interface and through local access by the administrators to the Motif Console.

5.1.5.9 FMT_SMR.1.1 Security roles

Hierarchical to: No other components.
FMT_SMR.1.1 The TSF shall maintain the roles [*End User and eHealth System Administrator*].
FMT_SMR.1.2 The TSF shall be able to associate users with roles.
Dependencies: FIA_UID.1 Timing of identification

5.1.6 Protection of the TSF (FPT)

5.1.6.1 FPT_RVM_EXP_TOE.1 Non-bypassability of the TSP: TOE

Hierarchical to: No other components.

FPT_RVM_EXP_TOE.1.1 The TSF, when invoked by the underlying host OS, shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

Dependencies: No dependencies.

5.1.6.2 FPT_SEP_EXP_TOE.1 TSF domain separation: TOE

Hierarchical to: No other components.

FPT_SEP_ EXP_TOE.1.1 The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects initiating actions through its own TSFI.

FPT_SEP_ EXP_TOE.1.2 The TSF shall enforce separation between the security domains of subjects in the TSC.

Dependencies: No dependencies.

5.1.6.3 FTP_TRP.1 Trusted Path

Hierarchical to: No other components.

FTP_TRP.1.1 The TSF shall provide a communication path between itself and [remote] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from [disclosure].

Application note: This SFR is included to capture SSL encryption functionality.

FTP_TRP.1.2 The TSF shall permit [the remote users] to initiate communication via the trusted path.

FTP_TRP.1.3 The TSF shall require the use of the trusted path for [initial user authentication].

Dependencies: No dependencies

5.2 Strength of Function

The password policy is strictly enforced by good operational security practices. No probabilistic or permutational mechanisms exist within the TOE therefore an SOF claim is not applicable.

5.3 TOE Security Assurance Requirements

This section identifies the Security Assurance Requirement components met by the TOE. These assurance components meet the requirements for EAL2.

5.3.1 Configuration Management (ACM)

5.3.1.1 Configuration items (ACM_CAP.2)

ACM_CAP.2.1D The developer shall provide a reference for the TOE.
ACM_CAP.2.2D The developer shall use a CM system.
ACM_CAP.2.3D The developer shall provide CM documentation.
ACM_CAP.2.1C The reference for the TOE shall be unique to each version of the TOE.
ACM_CAP.2.2C The TOE shall be labelled with its reference.
ACM_CAP.2.3C The CM documentation shall include a configuration list.
ACM_CAP.2.4C The configuration list shall uniquely identify all configuration items that comprise the TOE.
ACM_CAP.2.5C The configuration list shall describe the configuration items that comprise the TOE.
ACM_CAP.2.6C The CM documentation shall describe the method used to uniquely identify the configuration items.
ACM_CAP.2.7C The CM system shall uniquely identify all configuration items.
ACM_CAP.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.2 Delivery and operation (ADO)

5.3.2.1 Delivery procedures (ADO_DEL.1)

ADO_DEL.1.1D The developer shall document procedures for delivery of the TOE or parts of it to the user.
ADO_DEL.1.2D The developer shall use the delivery procedures.
ADO_DEL.1.1C The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to a user's site.
ADO_DEL.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.2.2 Installation, generation, and start-up procedures (ADO_IGS.1)

ADO_IGS.1.1D The developer shall document procedures necessary for the secure installation, generation, and start-up of the TOE.
ADO_IGS.1.1C The installation, generation and start-up documentation shall describe all the steps necessary for secure installation, generation, and start-up of the TOE.
ADO_IGS.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ADO_IGS.1.2E The evaluator shall determine that the installation, generation, and start up procedures result in a secure configuration.

5.3.3 Development (ADV)

5.3.3.1 Informal functional specification (ADV_FSP.1)

ADV_FSP.1.1D The developer shall provide a functional specification.
ADV_FSP.1.1C The functional specification shall describe the TSF and its external interfaces using an informal style.
ADV_FSP.1.2C The functional specification shall be internally consistent.
ADV_FSP.1.3C The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing details of effects, exceptions and error messages, as appropriate.
ADV_FSP.1.4C The functional specification shall completely represent the TSF.
ADV_FSP.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ADV_FSP.1.2E The evaluator shall determine that the functional specification is an accurate and complete instantiation of the TOE security functional requirements.

5.3.3.2 Descriptive high-level design (ADV_HLD.1)

ADV_HLD.1.1D The developer shall provide the high-level design of the TSF.

ADV_HLD.1.1C The presentation of the high-level design shall be informal.

ADV_HLD.1.2C The high-level design shall be internally consistent.

ADV_HLD.1.3C The high-level design shall describe the structure of the TSF in terms of subsystems.

ADV_HLD.1.4C The high-level design shall describe the security functionality provided by each subsystem of the TSF.

ADV_HLD.1.5C The high-level design shall identify any underlying hardware, firmware, and/or software required by the TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, or software.

ADV_HLD.1.6C The high-level design shall identify all interfaces to the subsystems of the TSF.

ADV_HLD.1.7C The high-level design shall identify which of the interfaces to the subsystem of the TSF are externally visible.

ADV_HLD.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_HLD.1.2E The evaluator shall determine that the high-level design is an accurate and complete instantiation of the TOE security functional requirements.

5.3.3.3 Informal correspondence demonstration (ADV_RCR.1)

ADV_RCR.1.1D The developer shall provide an analysis of correspondence between all adjacent pairs of TSF representations that are provided.

ADV_RCR.1.1C For each adjacent pair of provided TSF representations, the analysis shall demonstrate that all relevant security functionality of the more abstract TSF representation is correctly and completely refined in the less abstract TSF representation.

ADV_RCR.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.4 Guidance documents (AGD)

5.3.4.1 Administrator guidance (AGD_ADM.1)

AGD_ADM.1.1D The developer shall provide administrator guidance addressed to system administrative personnel.

AGD_ADM.1.1C The administrator guidance shall describe the administrative functions and interfaces available to the administrator of the TOE.

AGD_ADM.1.2C The administrator guidance shall describe how to administer the TOE in a secure manner.

AGD_ADM.1.3C The administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment.

AGD_ADM.1.4C The administrator guidance shall describe all assumptions regarding user behaviour that are relevant to secure operation of the TOE.

AGD_ADM.1.5C The administrator guidance shall describe all security parameters under the control of the administrator, indicating secure values as appropriate.

AGD_ADM.1.6C The administrator guidance shall describe each type of security relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_ADM.1.7C The administrator guidance shall be consistent with all other documentation supplied for evaluation.

AGD_ADM.1.8C The administrator guidance shall describe all security requirements for the IT environment that are relevant to the administrator.

AGD_ADM.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.4.2 User guidance (AGD_USR.1)

AGD_USR.1.1D	The developer shall provide user guidance.
AGD_USR.1.1C	The user guidance shall describe the functions and interfaces available to the non-administrative users of the TOE.
AGD_USR.1.2C	The user guidance shall describe the use of user-accessible security functions provided by the TOE.
AGD_USR.1.3C	The user guidance shall contain warnings about user-accessible functions and privileges that should be controlled in a secure processing environment.
AGD_USR.1.4C	The user guidance shall clearly present all user responsibilities necessary for secure operation of the TOE, including those related to assumptions regarding user behaviour found in the statement of TOE security environment.
AGD_USR.1.5C	The user guidance shall be consistent with all other documentation supplied for evaluation.
AGD_USR.1.6C	The user guidance shall describe all security requirements for the IT environment that are relevant to the user.
AGD_USR.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.5 Tests (ATE)

5.3.5.1 Evidence of coverage (ATE_COV.1)

ATE_COV.1.1D	The developer shall provide evidence of the test coverage.
ATE_COV.1.1C	The evidence of the test coverage shall show the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.
ATE_COV.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.5.2 Functional testing (ATE_FUN.1)

ATE_FUN.1.1D	The developer shall test the TSF and document the results.
ATE_FUN.1.2D	The developer shall provide test documentation.
ATE_FUN.1.1C	The test documentation shall consist of test plans, test procedure descriptions, expected test results and actual test results.
ATE_FUN.1.2C	The test plans shall identify the security functions to be tested and describe the goal of the tests to be performed.
ATE_FUN.1.3C	The test procedure descriptions shall identify the tests to be performed and describe the scenarios for testing each security function. These scenarios shall include any ordering dependencies on the results of other tests.
ATE_FUN.1.4C	The expected test results shall show the anticipated outputs from a successful execution of the tests.
ATE_FUN.1.5C	The test results from the developer execution of the tests shall demonstrate that each tested security function behaved as specified.
ATE_FUN.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.5.3 Independent testing - sample (ATE_IND.2)

ATE_IND.2.1D	The developer shall provide the TOE for testing.
ATE_IND.2.1C	The TOE shall be suitable for testing.
ATE_IND.2.2C	The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.
ATE_IND.2.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ATE_IND.2.2E	The evaluator shall test a subset of the TSF as appropriate to confirm that the TOE operates as specified.

ATE_IND.2.3E The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.

5.3.6 Vulnerability assessment (AVA)

5.3.6.1 Strength of TOE security function evaluation (AVA_SOF.1)

AVA_SOF.1.1D The developer shall perform a strength of TOE security function analysis for each mechanism identified in the ST as having a strength of TOE security function claim.

AVA_SOF.1.1C For each mechanism with a strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the minimum strength level of SOF-basic.

AVA_SOF.1.2C For each mechanism with a specific strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the specific strength of function metric of SOF-basic.

AVA_SOF.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_SOF.1.2E The evaluator shall confirm that the strength claims are correct.

5.3.6.2 Developer vulnerability analysis (AVA_VLA.1)

AVA_VLA.1.1D The developer shall perform a vulnerability analysis.

AVA_VLA.1.2D The developer shall provide vulnerability analysis documentation.

AVA_VLA.1.1C The vulnerability analysis documentation shall describe the analysis of the TOE deliverables performed to search for obvious ways in which a user can violate the TSP.

AVA_VLA.1.2C The vulnerability analysis documentation shall describe the disposition of obvious vulnerabilities.

AVA_VLA.1.3C The vulnerability analysis documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE.

AVA_VLA.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_VLA.1.2E The evaluator shall conduct penetration testing, building on the developer vulnerability analysis, to ensure obvious vulnerabilities have been addressed.

5.4 Environment Security Functional Requirements

This section identifies the security functional requirements that have been levied to the IT environment and must be enforced in order for the TOE to securely enforce its stated functional claims. These Security Functional Requirements are identified in the following table.

Table 2 - TOE Security Assurance Measures

Security Functional Class	Security Functional Component
Security audit (FAU)	FAU_STG.1 Protected audit trail storage
Protection of the TSF (FPT)	FPT_RVM_EXP.1 Reference Mediation: IT Environment FPT_SEP_EXP.1 Domain Separation: IT Environment FPT_STM.1 Reliable time stamps

The following subsections present the details for each of the IT environment Security Functional Requirement components.

5.4.1 Security audit (FAU)

5.4.1.1 FAU_STG.1 Protected audit trail storage

Hierarchical to:	FAU_STG.1
FAU_STG.1.1	The **IT environment** shall protect the stored audit records from unauthorised deletion.
FAU_STG.1.2	The **IT environment** shall be able to [***prevent***] unauthorised modifications to the audit records in the audit trail.
Dependencies:	FAU_GEN.1 Audit data generation

5.4.2 Protection of the TSF (FPT)

5.4.2.1 FPT_RVM_EXP.1 Partial Non-bypassability of the TSP: IT Environment

Hierarchical to:	No other components.
FPT_RVM_EXP.1.1	The security functions of the TOE server OS shall ensure that TOE server OS security policy enforcement functions are invoked and succeed before each function within the scope of control of the TOE server OS is allowed to proceed.
Dependencies:	No dependencies.

5.4.2.2 FPT_SEP_EXP.1 Partial Domain Separation: IT Environment

Hierarchical to:	No other components.
FPT_SEP_EXP.1.1	The security functions of the TOE server OS shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects in the scope of control of the TOE server OS.
FPT_SEP_EXP.1.2	The security functions of the TOE server OS shall enforce separation between the security domains of subjects in the scope of control of the TOE server OS.
Dependencies:	No dependencies

5.4.2.3 FPT_STM.1 Reliable time stamps

Hierarchical to:	No other components.
FPT_STM.1.1	The **IT environment** shall be able to provide reliable time-stamps for **use by the TOE**.
Dependencies:	No dependencies
Application Note:	The Underlying OS needs to provide reliable time stamps from the system clock that is used for inclusion in the audit records generated by the TOE.

6 TOE Summary Specification

6.1 TOE Security Functions

This section describes the security functions provided by the TOE.

6.1.1 Authorisation

Authorisation is used in the eHealth Suite Version 5.7 SP9. Authorisation protects the system resources from unauthorised access. The authorization policy controls an authorized user capability of accessing pages and files, or running applications. Access privileges granted to users are managed by the eHealth application. The eHealth application stores the privilege information on a CSV file on the system where eHealth runs. When the user requests content from the eHealth application, the eHealth application will validate the authorization to this content by comparing the validated username provided by the web server with the list of access rights on the Authorization database (CSV). Users do not access the database directly, but instead can view elements within the database via reports if the user is authorized to read those elements. For database access, the eHealth application verifies that the OS user has access to the Oracle database and grants it DBA rights. The TOE requires administrators and users to establish robust password for the users of the TOE.

6.1.2 Data Protection

Access to TOE data is protected through the access control provided by the TOE. In order to manipulate data, an administrator must successfully login via the Remote Workstation. End Users are not given permission to modify anything on the system besides their personal password attributes. Data storage is handled by the underlying Operating System upon which the eHealth Suite resides and the Oracle 9i database.

6.1.2.1 Configuration

The TOE supports a policy that is created by the eHealth System Administrator upon installation of the TOE. Once the eHealth Administrator has successfully logged in, there are several processes that are invoked to begin setting up the access, authorization, audit, data protection, and security management settings. As a part of the initial installation, a configuration process is invoked that (in conjunction with a discovery process) identifies and sets up communication channels with machines using SNMP protocol version 1. Identification information for these machines is then added to processing tables within the eHealth Suite. These processing tables enable the TOE to monitor network resources. Only machines that are on this list (using SNMP protocol version 1) are permitted to communicate with the TOE. Additionally, the initial installation of the eHealth Suite sets up an administrative account. Once the eHealth Suite Version 5.7 SP9 is installed, the administrator can begin to setup and configure user accounts from the web interface. The eHealth Suite software provides the authenticated administrators with the ability to view audit trails according to the attributes that the administrator requested to view in the GUI. The eHealth Suite also provides data protection and security management functionality through the GUI. Authenticated administrators are permitted to manage user accounts and to control which users have access to which data groups.

6.1.2.2 Configuration Server Process

The Configuration Server is a permanently-running process on the eHealth Suite, and maintains an in-memory image of all elements defined in the system. The primary function of the Configuration Server process is to process files of individual-operation DCI files[1], and store the resulting changes in the Oracle 9i Database. Due to the complexities of element processing, the in-memory image is maintained to aid the performance of the operation processing algorithms. Each element change, whether explicit or derived from element constraints, is logged in a machine and human readable file called the poller audit log. This log, whose size is user-settable, is a record of each change, including user, time, attribute identification, old attribute value, and new attribute value. It is useful to users who need to resolve changes for diagnostic or accounting purposes. The TOE interfaces to Oracle that can read or write the data stored in the database is done via an API that performs Oracle Procedure Library calls.

6.1.2.3 Authorisation Evaluation Process

When users request access to resources protected by the TOE, their requests are assessed according to the eHealth discretionary access control policy. The eHealth Server checks the permissions set by the eHealth System Administrator for the End User account being accessed to determine which functions the user will be permitted to perform.

The eHealth Web server has secure access. Secure access, to the eHealth Web server is enabled by default. Secure access, requires users to log in using an eHealth Web user name and password. To allow a user to access the secure Web server and Web reports, the TOE administrator must create a Web user account for the user. After the TOE administrator enables Web security, administrative functions such as modifying user accounts, changing site configurations, or displaying access logs are available in the Authorized Access area. When the TOE Administrator clicks Authorized Access on the Administration page, he/she is prompted to specify a user name and password. The Authorized Access menu appears, and the TOE administrator can access the following administrative functions:

- Manage Users
- Access Logs
- Site Configuration
- Change Password
- Advanced Logging

6.1.3 Authentication

Authentication is provided via the Apache Web Server component of the TOE. The TOE will ensure that users are authenticated before allowing TSF access through the browser based GUI. Authentication is through a user password configured to be consistent with the documented users policy. A policy to ensure a hard-to-guess password is specified in the administrator and user guidance. The TOE compares the entered user name and password with the attributes of the user account for its authentication and identification of users.

6.1.3.1 Configuration

Once the administrator has logged onto the eHealth Suite and configured end user accounts, the TOE is then setup to authenticate users from a Remote Workstation. A user accesses the eHealth Server through a browser on their Remote Workstation. The connection is established using HTTP over SSL. While the system is configured using HTTP by default, the TOE is configured to use HTTP over SSL for the evaluated configuration.

6.1.3.2 Authentication Evaluation Process

In the case of the Web Server Interface, the user initiates authentication to the web server component of the TOE using digest authentication from Apache, specifically the Apache module mod_auth_digest controls the encryption of the passwords, and protects the TOE from replay attacks. During the I&A process the user performs the SSL protocol handshake, is prompted with a login pop up window, and is allowed to enter I&A credentials. Authentication requires both a valid authentication attempt via SSL and a valid certificate exchange between the TOE (i.e., Apache Server) and the remote web browser.

The TOE maintains user identity, authentication data (I&A credentials), and authorizations on each user of the system. These take the form of the tuplet {username, password, group}. The username, group, and password are stored in the underlying operation system. For clarification, the password is not stored directly, but rather as a cryptographic hash. The Identification and Authentication function stores the users associated role, which essentially takes the form of the couplet {username, group}.

A user must authenticate to the eHealth Suite to perform any action on the TOE. The information is sent encrypted via HTTP over SSL, as described above, from the user's web browser to the eHealth Suite where access is either granted or denied.

6.1.3.3 Strength of Function

The password policy is strictly enforced by good operational security practices. No probabilistic or permutational mechanisms exist within the TOE therefore an SOF claim is not applicable.

6.1.3.4 Password Management

The eHealth Suite enables the eHealth Administrator to set up end user accounts on the eHealth Server with a default password of his/her choice. End users are permitted to change their passwords at any time following a successful login.

6.1.3.4.1 Lost Password Management

In the event that an End User loses his or her password, the eHealth System Administrator must change the password in the eHealth Suite. The End User may then login to the eHealth Server and modify their password.

6.1.3.4.2 Password Reset

The eHealth Administrator will reset an End User password upon request from the user. This reset will set a temporary password that the End User will be prompted to change upon first login.

6.1.4 Audit

The TOE produces audit data (i.e., access logs) to track all users interaction with the TOE through the Web Server component of the TOE, including password changes, generation of reports, and viewing reports. This section of the TSS will describe access logs, the poller process, and end user reports.

The TOE relies upon the underlying OS to store the audit data generated by the TOE.

6.1.4.1 Access Logs (i.e., Web Server Access Logs)

Using the Access Logs option in the Site Management area of the Administration page, eHealth System Administrators can generate a detailed list of all connections that all or specific End Users have made to the eHealth Suite, all or specific Web pages that End Users have accessed, and a specific time and date range during which the access occurred. In addition, the eHealth System Administrator can also display summary statistics of individual connections to the eHealth Suite (that is, for each report page). The following figure describes the report details and page statistics that can be obtain by generating an access log.

Figure 2 – Access Log Attributes

Report Details	Individual Page Statistics
• Time range during which user(s) accessed the Web server • Name of user(s) who accessed the Web server • Type of report page that the user(s) accessed • Workstation IP addresses from which the user(s) performed the operation • Total number of operations performed	• IP address of workstation from which the page was accessed • Web user account name(s) • Date and time at which the page was accessed • Name of the operation that was performed (for example: GET or POST) • Pathname of the page that the user (s) visited • Return code • Total amount of data (in bytes) that was transferred

The TOE calls these audit files Access logs in the user GUI, they are synonymous with standard Apache web logs. The log files specifically are:

1. Web Server Log httpd-log – Standard Apache web log of all HTTP requests, including user login, password changes, report generation, and viewing of reports.
2. Web Server Log httpd-error – Standard Apache web log errors resulting from HTTP requests.

6.1.4.2 eHealth Poller Process

During installation a discovery process is run to baseline the network resources. After the discovery process has populated the database. The TOE uses the poller process to collect historical data on the various elements in the database. The historical data and discovery process update or create elements in the Oracle 9i database. The TOE creates audit data to monitor these actions as described below:

1. Poller Audit Logs – Log new element additions, element deletions, and changes to any field of any element. Includes the time of change, user name, element id, field name, old value, and new value.
2. Discover Log – Describes the results of an element merge operation detailing what elements matched, the quality of the match, and field changes and any new elements found.
3. Message Log - Statistics Polling static window messages are stored on the underlying OS in a file called messages.stats.log.

6.1.4.3 eHealth Reports

eHealth identifies and collects data from existing devices, agents, and management systems in the network intranet. To evaluate the health of these network resources, eHealth uses the historical data that it collects to analyze trends and calculate averages. It collects data over a period of time for various elements polled by the TOE. This data grades the performance of each element based on the utilization and number of errors that eHealth detects. eHealth uses upper limits for utilization and errors, referred to as Trend thresholds, to identify problem areas. eHealth Administrators and users can generate reports on the collected data to manage network resources. When a report is generated, the TOE records the following information: date and time of the event, type of event, the element reported on, title of the report, group the element belongs to, and the type of report that was run.

eHealth reports provide an easy-to-read picture of the historical and current performance of the elements that were polled. The various reports assist users in optimizing network performance, recognizing trends, and identifying potential problems before they affect critical services. This section describes the basic reports that are available to the TOE users.

6.1.4.3.1 At-a-Glance Reports

At-a-Glance reports provide a series of charts that show the performance of critical variables for a specified element during the report period. A report period is the time range included in a report. When end users run a report, they can specify the time range. The time options vary with each report type, but the report period can consist of hours, days, weeks, or months. These charts show the trends for important variables such as the following:

- CPU utilization
- Buffer management
- Traffic activity by protocol
- Total throughput
- Disk faults
- Disk I/O

At-a-Glance reports provide detailed information for all the critical performance parameters available, depending on the element reported on. At-a-Glance reports present the variables on identical time axes that allow TOE users to examine the interaction of critical performance indicators over the report period. Users can compare these charts to determine whether activity in one chart coincides with activity in other charts. For example, At-a-Glance reports can compare bandwidth utilization, bytes in & bytes out, frames in & frames out, errors in & errors out, availability, latency, etc.

6.1.4.3.2 Top N Reports

Top N reports are tabular reports that list all elements in a group, or all elements in a group that exceed or fall below the values that end users specify. For example, end users can run a Top N report to show the following:

- 50 LAN/WAN elements that have a bandwidth utilization above 40%
- All system partitions that have less than 20% utilization
- The 15 routers that have an average line utilization above 90%, incoming discards greater than 100 frames per second, and outgoing discards greater than 150 frames per second
- All elements in the group Boston-to-New York

When end users run a Top N report, they can specify the following criteria:

- Number of elements and element types to display
- Element group within which to search
- Up to six variables on which to report
- Service goal for each variable
- Filter criteria for each variable
- Ascending or descending display order
- Report period

6.1.4.3.3 Trend Reports

Trend reports show the performance of an element or a group of elements, over a specified period of time, based on specific variables. These reports identify the cause of an unsatisfactory health rating on a specific element, or the performance of a group of elements. If end users run the report for a group of elements, they can generate separate charts per element or aggregate the data for all elements as a total variable value.

Because of its flexibility, end users can use a Trend report to reveal traffic patterns over time, as well as relationships between elements and between variables. If the Trend report indicates that two variables are correlated, then it suggests a causal relationship between them. For instance, if the bandwidth utilization and the collision rate on an Ethernet segment show a strong correlation, it means that the high bandwidth utilization is causing the high rate of collisions. Similarly, a strong correlation between bandwidth utilization and discards suggests that high bandwidth utilization is causing network congestion, which, in turn, causes packets to be discarded.

6.1.5 Security Management

Security Management is implemented by the TOE through interactions by the administrator from a Remote Workstation and locally on the TOE via the X Windows (Motif) console. For remote access the administrator logs into the eHealth Suite via an SSL enabled web browser. Once authenticated, the administrator has access to security management tabs within the eHealth Suite software that enable him/her to control system access by others. The administrator can control which data objects users may generate reports on or view. Additionally, the administrator may manage login attributes of the End Users. From the Motif console the local administrators can manage user accounts, groups, and grouplists; view the system message logs, schedule jobs and manually run the discover process.

6.1.5.1 Managing User Accounts Using Groups and Group Lists

Elements may be collected together via objects known as groups, and the groups in turn in to group lists. These form not only fundamental domain-level collection facilities, but also for the basis for access control among multiple users.

Users are assigned to certain groups to control their access to the corresponding elements contained therein. An administrator grants this access to users via a web interface. When a user is allowed to “see” (i.e., read) an element, that user may observe its configuration information and run reports which contain that element.

eHealth enables the TOE administrator to organize elements into groups so that related elements can be associated with one another (such as those for a specific department or customer) and generate reports for those specific element sets, or so that the TOE administrator can filter the elements shown in the console. To organize groups, the TOE administrator can use group lists. For example, TOE administrators can use group lists to model larger organizations such as all of the groups for a customer, a company, geographic region, and so on. By focusing on a subset of elements—rather than all elements in the IT infrastructure—the TOE can create effective reports that address specific needs. A group can belong to multiple group lists. Groups and group lists can be used together to control access to reports and elements via the Web interface.

As soon as elements are discovered of a specific type, eHealth creates a default group called All that includes all discovered elements of that type. For example, if the TOE has 40,000 LAN/WAN elements, the LAN/WAN All group includes all 40,000 LAN/WAN elements. If the TOE has one system element, the System All group contains that one system element. The TOE cannot add or delete All groups.

6.1.5.2 Changing User Passwords

The TOE administrator can add new users and set their permissions. The TOE administrator can add, modify, and delete user and system passwords for all users. Other users can modify their own passwords only.

6.1.5.3 Providing Access to Groups and Reports

As the TOE administrator, it is possible to grant users permissions to view and use none, some, or all groups and group lists. For example, Internet Service Provider (ISP) operators need to see a group list that contains all of their customers. However, they would likely create a group for each customer and restrict access so that each customer views only their own activity. Groups and group lists also restrict which eHealth reports a user can run.

To assign permissions to use groups and group lists the TOE administrator logs in to the Web server, and selects the user name to modify the access permissions. For each technology type listed in the Groups and Group Lists sections, the TOE administrator can do one of the following:

- Select No access to prevent the user from viewing any groups, group lists, or elements for that technology type.
- Select All elements to allow the Web user to view all groups, group lists, and elements for that technology type.
- Select one or more groups or group lists from each list to restrict the user to only those groups or group lists and the elements they contain.

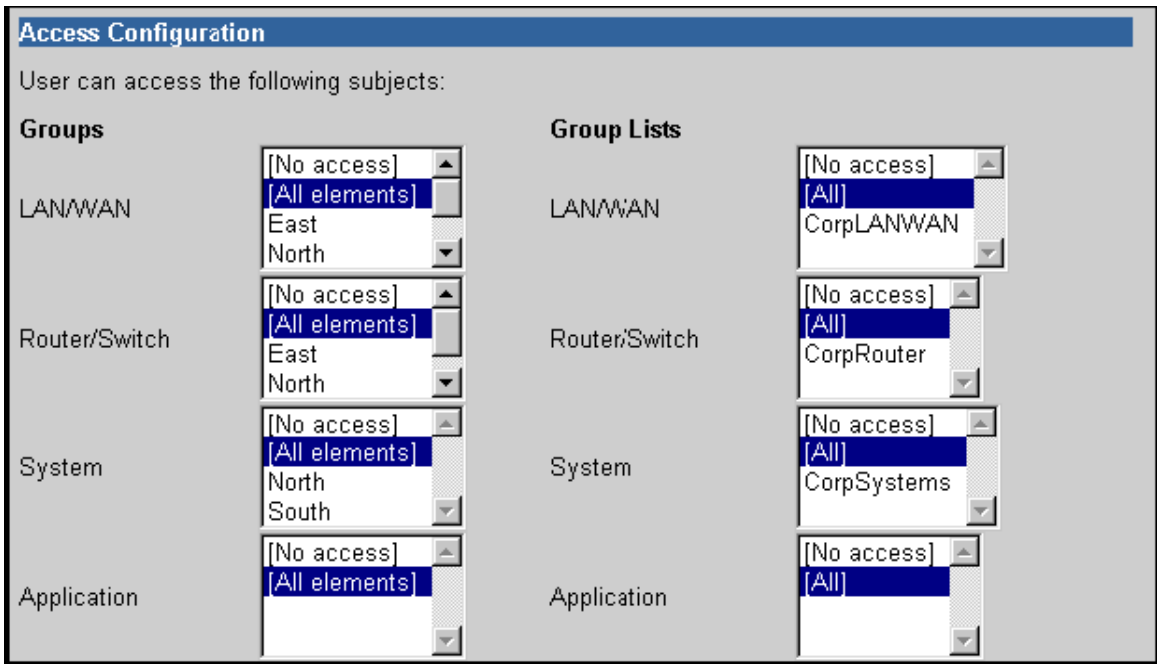

Figure 3 - Example of Group Level Access Permissions

6.1.6 Trusted Path

The protection mechanisms employed by the TOE ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed. More specifically, once a user has been authenticated via Web interface, the Identification and Authentication is used to query and return the user's role. The role is used to determine what functionality is presented to the user. For the Application TOE, the host IT environment administrator can access the TOE to change the time and halt the execution of the application. Because the host IT environment is considered to be a trusted IT entity and the interface established to change the time and halt the TOE is via a trusted path, the security domain for the Application TOE is still considered protected from interference and tampering. A trusted path is established for all user communication between the TOE and the remote administration console via HTTP over SSL. No other means, other than described above, are provided for the user to interact with the TOE. The use of SSL ensures that all traffic to and from the TOE via the remote administration interface is protected from unauthorized disclosure. The passwords are not sent in the clear but use an MD5 hash for comparison to a shared secret on the TOE. All SSL data is encrypted with a 3DES and RSA is used for symmetric key exchange.

6.1.7 Self Protection

The Self-protection function is responsible for providing an execution domain that is protected from interference and tampering by unauthorized users. The TOE is a application running on a dedicated device that executes all of its processes internally. It is accessible only via the defined interfaces and only authorized users and the host IT environment for the TOEs are able to modify the functionality of the TOE. The poller interface enforces domain separation in that any data sent to this interface (which is presumed untrusted) is logically separated from all other TOE data. It is never executed but rather is parsed for analysis. Traffic flowing through the TOE is subject to the policies as defined by the authorized users. At all physical interfaces, the TOE intercedes to ensure domain separation. Traffic can only come into the TOE via four physical interfaces, the local CLI interface (which is used only during initial setup and configuration of the TOE), the network interface (access to which is controlled by a username and a password), the Oracle Database (which is only accessible by internal TOE processes) or the poller interface (where the traffic is monitored and analyzed by the TOE but no actions can be executed). Traffic and/or unauthorized users cannot bypass the identification and authentication mechanisms, preventing interference and tampering by untrusted subjects and thereby maintaining a domain for its own execution. The self protection function of the Module TOE and the self protection features of the host IT environment work together to satisfy the self protection requirements. The reliable time value is received upon boot up or modified via a trusted channel from the host IT Environment. The host IT Environment mediates its interfaces to only allowed authorized modifications while protecting those interfaces from interference and tampering. For example, once the clock is initialized or modified via the trusted interface the IT Environment ensures those interfaces are free from interference and tampering.

6.2 TOE Security Assurance Measures

This section identifies the assurance measures provided by the developer in order to meet the security assurance requirement components for EAL2. These measures are identified in the following table.

Table 3 - Secuirty Assurance Measures

Component	Document(s)	Rationale
ACM_CAP.2: Configuration Management	[1] Build and Kitting Windowsv2.0 [2] eHealth Nightly Builds (UNIX)v2.0 [3] NVM IT Backup Strategy v1.1 [4] NVM Source Code Best Practices v1.1 [5] New eHealth Checkin Process Rollout for eHealth Suite Version 5.7 version 2.0 [6] Configuration Item List.txt [7] CA eHealth 5.7 SP9 Delivery	These documents describe configuration management in regard to planning for the release of the CA components.
ADO_DEL.1: Delivery procedures	[1] Concord Communications Software Delivery Procedures, Version 1.0 [2] CA eHealth 5.7 SP9 Delivery	Software Delivery Procedures document describes product delivery for CA.
ADO_IGS.1: Installation, generation, and start-up procedures	[1] installation GuideUNIX57 (MN-INSTALUN-003) [2] eHealth Installation Addendum for UNIX (r5.7) [3] CA eHealth 5.7 SP9 Delivery [4] eHealth+SSL+SiteMinder	These guides describe how to set the system up on a UNIX machine.

ADV_FSP.1: Informal functional specification	[1] Functional Specification Document for CA eHealth v 5.7 SP9 v1.2 [2] eHealth Administration Reference (MN-EHADMREF-002) [3] eHealth Web Administration Guide (MN-EHWEBADM-001) [4] eHealth Administration Guide (MN-EHADMGD-002) [5] eHealth Installation Guide: New Installations (UNIX) (MN-INSTALUN-003) [6] Querying the Database Using the DB API (MN-DBAPI-002) [7] Introduction to eHealth (MN-INTROEH-002) [8] eHealth Web Help Contents v5.7	These documents describe the informal functional specification of the TOE.
ADV_HLD.1: Descriptive high-level design	[1] High Level Design Document for CA eHealth v 5.7 SP9 v1.3 [2] eHealth Administration Reference (MN-EHADMREF-002) [3] eHealth Web Administration Guide (MN-EHWEBADM-001) [4] eHealth Administration Guide (MN-EHADMGD-002) [5] eHealth Installation Guide: New Installations (UNIX) (MN-INSTALUN-003) [6] Querying the Database Using the DB API (MN-DBAPI-002) [7] Introduction to eHealth (MN-INTROEH-002) [8] eHealth Web Help Contents v5.7	These documents provide an overview of how the product operates and the interfaces that stimulate the TOE.

ADV_RCR.1: Informal correspondence demonstration	[1] Functional Specification Document for CA eHealth v 5.7 SP9 v1.2 [2] High Level Design Document for CA eHealth v 5.7 SP9 v1.3	These documents describes the informal correspondence demonstration of the TOE.
AGD_ADM.1: Administrator guidance	[1] Computer Associates eHealth Suite Version 5.7 Admin Supplemental Guidance, v1.0 [2] eHealth Web Administration Guide (MN-EHWEBADM-001) [3] eHealth Administrator Guide (MN-EHADMGD-002) [4] eHealth Administration Reference (MN-EHADMREF-002) [5] eHealth Web Help Contents v5.7	These documents describe the processes to be used for proper administration of the TOE.
AGD_USR.1: User guidance	[1] eHealth Web Help Contents v5.7 [2] Computer Associates eHealth Suite Version 5.7 Admin Supplemental Guidance, v1.0	This document describes the proper use of the TOE from a user standpoint.
ATE_COV.1: Evidence of coverage	[1] eHealth Security Version 5.7 Test Plan v1.0 [2] eal_security_pts_57.xls	These are the eHealth test procedures that outline coverage of security requirements from the ST.
ATE_FUN.1: Functional testing	[1] eHealth Security Version 5.7 Test Plan v1.0 [2] eal_security_pts_57.xls	These are the eHealth test procedures that demonstrate compliance to the security requirements from the ST.
ATE_IND.2: Independent testing	[1] eHealth Security Version 5.7 Test Plan v1.0 [2] eal_security_pts_57.xls	This document describes the functional test plan and functional tests performed by the developer of the TOE.

AVA_SOF.1: Strength of TOE security function evaluation	[1] Computer Associates eHealth Suite Version 5.7 Admin Supplemental Guidance, v1.0	This document contains the Strength of function analysis.
AVA_VLA.1: Developer vulnerability analysis	[1] CA eHealth Suite v5.7 SP9 Vulnerability Analysis v1.1	This is the eHealth vulnerability analysis documenting common known vulnerabilities of similar product type.

7 Protection Profile Claims

This Security Target does not claim Protection Profile conformance.

8 Rationale

8.1 Security Objectives Rationale

The following tables provide a mapping with rationale to identify the security objectives that address the stated assumptions and threats.

Table 4 - Assumptions to Objectives Mapping

Assumption	Objective	Rationale
A.ADMIN One or more authorised administrators will be assigned to install, configure and manage the TOE and the security of the information it contains.	OE.ADMIN One or more eHealth System Administrators will be assigned to install, patch, configure and manage the TOE and the security of the information it contains.	OE.ADMIN maps to A.ADMIN in order to ensure that eHealth System Administrators install, manage and operate the IT Environment in a manner that maintains its security objectives.
A.PATCHES System Administrators exercise due diligence to patch the IT Environment (e.g., OS and database) so they are not susceptible to network attacks.	OE.ADMIN One or more eHealth System Administrators will be assigned to install, patch, configure and manage the TOE and the security of the information it contains.	OE.ADMIN maps to A.PATCHES in order to ensure that eHealth System Administrators properly patch the IT Environment in a manner that maintains its security objectives.
A.NOEVIL Users of the TOE are not careless, willfully negligent, or hostile and will follow and abide by the instructions provided by the guidance documentation.	OE.NOEVIL Users of the TOE are not careless, willfully negligent, or hostile and will follow and abide by the instructions provided by the guidance documentation.	OE.NOEVIL directly maps to A.NOEVIL and ensures that all users of the TOE are properly trained in the configuration and usage of the TOE and will follow the guidance provided.
A.LOCATE The network the TOE will monitored is isolated form any other network. The SNMP monitored traffic is limited to the isolated intranet, (i.e., no connections exist to other networks).	OE.LOCATE The TOE will be located on an isolated network with no connections to other networks.	OE.LOCATE directly maps to A.LOCATE to ensure that the monitored network is isolated and safe from interference by other networks.
A.PROTECT The parts of the TOE critical to security policy enforcement will be protected from unauthorised physical modification.	OE.PROTECT The parts of the TOE critical to security policy enforcement will be protected from unauthorised physical modification.	OE.PROTECT directly maps to A.PROTECT to ensure that those responsible for the TOE must ensure that the TOE hardware and software critical to security policy are protected from physical attack and unauthorised physical modification, which might compromise the TOE security objectives.
A.PASSWORD It is assumed that users will select strong passwords according to the policy described in the administrative guidance and will protect their authentication data.	OE.PASSWORD ensures that users of the TOE shall be instructed by the administrator guidance to choose strong passwords in accordance with the documented password policy and to protect their authentication data.	OE.PASSWORD directly maps to A.PASSWORD to ensure that users will select strong passwords according to the policy described in the administrative guidance and will protect their authentication data

Table 5 - Threat to Objective Mapping

Threat	Objective	Rationale
T.ACCESS A legitimate user of the TOE could gain unauthorized access to resources or information protected by the TOE, or perform operations for which no access rights have been granted, via user error, system error, or other actions.	O.ACCESS The TOE will provide measures to authorise End Users to access specified TOE resources once the user has be authenticated. User authorisation is based on access rights configured by the eHealth System Administrator of the TOE. OE.FILESYS The security features offered by the underlying Operating System protect the files used by the TOE.	O.ACCESS addresses T.ACCESS by providing the eHealth Administrator with the capability to specify access restrictions on the protected TOE resources to End Users. OE.FILESYS addresses T.ACCESS by ensuring that the underlying Operating System provides the capability to store and protect the files used by the TOE.
T.ADMIN_ERROR An administrator may incorrectly install or configure the TOE, or install a corrupted TOE resulting in ineffective security mechanisms.	O.ROBUST_ADMIN_GUIDANCE The TOE will provide administrators with the necessary information for secure delivery and management. O.MANAGE The TOE will provide eHealth System Administrators with the resources to manage and monitor user accounts, resources and security information relative to the TOE.	O.ROBUST_ADMIN_GUIDANCE (ADO_DEL.2, ADO_IGS.1, AGD_ADM.1, AGD_USR.1, AVA_MSU.2) help to mitigate this threat by ensuring the TOE administrators have guidance that instructs them how to administer the TOE in a secure manner and to provide the administrator with instructions to ensure the TOE was not corrupted during the delivery process. Having this guidance helps to reduce the mistakes that an administrator might make that could cause the TOE to be configured in a way that is unsecure. O.MANAGE addresses T.ADMIN_ERROR by ensuring that only eHealth System Administrators can use the provided resources for managing and monitoring user accounts, TOE resources and security information relative to the TOE.
T.MASK Users whether they be malicious or non-malicious, could gain unauthorised access to the TOE by bypassing identification and authentication countermeasures.	O.AUDIT The TOE will provide measures for recording security relevant events that will assist the eHealth System Administrators in detecting misuse of the TOE and/or its security features that would compromise the integrity of the TOE and violate the security objectives of the TOE. OE.SYSTIME The operating environment will provide reliable system time. O.IDEN The TOE will provide measures to uniquely identify End Users and will authenticate the claimed identity prior to granting a user access to the TOE.	O.AUDIT addresses T.MASK by providing the eHealth System Administrators with tools necessary to monitor user activity to ensure that misuse of the TOE does not occur. OE.SYSTIME addresses this threat by providing an audit mechanism in the underlying Operating System includes the current date and time in each audit record. All audit records that include the user ID, will also include the date and time that the event occurred. O.IDEN addresses T.MASK by providing measures to uniquely identify and authenticate End Users through successful login to the Apache Web Server through HTTP over SSL
T.MODIFY Users, whether they be malicious or non-malicious, could attempt to misconfigure or modify their	O.MANAGE The TOE will provide eHealth System Administrators with the resources to manage and monitor user accounts, resources and security	O.MANAGE addresses T.MODIFY by ensuring that only eHealth System Administrators can use the provided resources for managing and monitoring user

Threat	Objective	Rationale
user accounts in an attempt to tamper with TOE resources or modify security information relative to the TOE.	information relative to the TOE.	accounts, TOE resources and security information relative to the TOE.
T.PROTECT The TOE may be vulnerable to attacks against itself or may be bypassable.	O.SELF_PROTECTION The TSF shall provide protection for itself and its resources from external interference, tampering or unauthorized disclosure, through its own interfaces. OE.PROTECT The IT environment will work in concert with the TOE to protect it from unauthorised modifications and access to its functions and data within the TOE, through the IT Environment's interfaces within is scope of control.	O.SELF_PROTECTION (FPT_SEP.1, FPT_RVM.1) contributes to countering this threat by ensuring that the TSF can protect itself from users. If the TSF could not maintain and control its domain of execution, it could not be trusted to control access to the resources under its control. OE.PROTECT (FPT_SEP.1, FPT_RVM.1) contributes to countering this threat by ensuring that the IT environment maintains domain separation and works in concert with the TOE to protect it from unauthorised modifications.
T.DOS Users, whether they be malicious or non-malicious, could attempt to disable or modify routing of network appliances (i.e., routers, switches, etc.) in an attempt to cause slow or unavailable network resources to the network users.	O.MONITOR The TOE will collect, and analyze critical data for network devices, systems, and applications and report on the performance, capacity, availability, and response of these resources.	O.MONITOR mitigates this threat by having the TOE auditing the health and status of network devices
T.UNKNOWN Network devices, whether they be malicious or non-malicious, could be added to the IT Environment unknown to the TOE and disable or degrade the performance of networks, systems, or applications in the network.	O.DISCOVER The TOE will discover new network devices added to the IT environment and report to the TOE when those devices are discovered.	O.DISCOVER (FAU_GEN_EXP.1(1) mitigates this threat by detecting and auditing when new network devices, systems, or applications are added to the network monitored by the TOE.
T.CRYPTO_COMPROMISE A malicious user or process may cause key, data or executable code associated with the cryptographic functionality to be inappropriately accessed (viewed, modified, or deleted), thus compromise the cryptographic mechanisms and the data protected by those mechanisms.	O.CRYPTOGRAPHIC FUNCTIONS The TOE shall provide cryptographic functions for its own use, including encryption/decryption and digital signatures. O.ROBUST_ADMIN_GUIDANCE The TOE will ensure that any information contained in a protected resource is not released when the resource is reallocated. O.SELF_PROTECTION The TSF will maintain a domain for its own execution that protects itself and its resources from external interference, tampering, or unauthorized disclosure. The TSF will provide a High Availability	O.CRYPTOGRAPHIC_FUNCTIONS (FCS_CKM.1, FCS_CKM.4, FCS_COP.1, FMT_MSA.2, FTP_TRP.1) mitigates the possibility of malicious users or processes from gaining inappropriate access to cryptographic data, including keys. This objective ensures that the cryptographic data does not reside in a resource that has been used by the cryptographic module and then reallocated to another process. O.ROBUST_ADMIN_GUIDANCE (ADO_DEL.2,ADO_IGS.1, AGD_ADM.1, AGD_USR.1, AVA_MSU.2) help to mitigate this threat by ensuring the TOE administrators have guidance that instructs

Threat	Objective	Rationale
	configuration which allows for continued operation of the TOE in the event of a single unit failure.	them how to administer the TOE in a secure manner and to provide the administrator with instructions to ensure the TOE was not corrupted during the delivery process. Having this guidance helps to reduce the mistakes that an administrator might make that could cause the TOE to be configured in a way that is unsecure O.SELF_PROTECTION (FPT_SEP.1, FPT_RVM.1) contributes to countering this threat by ensuring that the TSF can protect itself from users. If the TSF could not maintain and control its domain of execution, it could not be trusted to control access to the resources under its control, which includes the cryptographic data and executable code.
T.EAVESDROPPING Unauthorized monitoring of networks or information systems	O.CRYPTOGRAPHIC FUNCTIONS The TOE shall provide cryptographic functions for its own use, including encryption/decryption and digital signatures. O.SELF_PROTECTION The TSF will maintain a domain for its own execution that protects itself and its resources from external interference, tampering, or unauthorized disclosure. The TSF will provide a High Availability configuration which allows for continued operation of the TOE in the event of a single unit failure.	O. CRYPTOGRAPHIC FUNCTIONS (FCS_CKM.1, FCS_CKM.4, FCS_COP.1, FMT_MSA.2, FTP_TRP.1) mitigates T.EAVESDROPPING by ensuring that all communication to and from the TOE are not sent unless they are encrypted. O.SELF_PROTECTION (FPT_SEP.1, FPT_RVM.1) contributes to countering this threat by ensuring that the TSF can protect itself from users. If the TSF could not maintain and control its domain of execution, it could not be trusted to control access to the resources under its control.

8.2 Security Functional Requirements Rationale

The following table provides a mapping with rationale to identify the Security Functional Requirement components that address the stated TOE and IT environment objectives.

Table 6 - Security Functional Requirements Rationale

Objective	Security Functional Components	Rationale
O.ACCESS The TOE will provide measures to authorize End Users to access specified TOE resources once the user has been authenticated. User authorization is based on access rights configured by the eHealth System Administrator of the TOE.	FDP_ACC.1 Subset access control	FDP_ACC.1 requires the TOE to prevent unauthorized access to TOE resources by enforcing the eHealth discretionary Access Control Policy.
	FDP_ACF.1 Security attribute based access control	FDP_ACF.1 requires the TOE to enforce the eHealth Access Control Policy on the protected TOE resources and requires the eHealth System Administrators to configure End User access rights accordingly.
O.AUDIT The TOE will provide measures for recording security relevant events that will assist the eHealth System Administrators in detecting misuse of the TOE and/or its security features that would compromise the integrity of the TOE and violate the security objectives of the TOE.	FAU_GEN.1 Audit data generation	FAU_GEN.1 defines the security relevant events that will be recorded by the TOE along with the details of the event that will be recorded.
	FAU_GEN.2 User identity association	FAU_GEN.2 requires the TOE to associate each auditable event with the identity of the End User or eHealth System Administrator that caused the event.
	FAU_SAR.1 Audit Review	FAU_SAR.1 requires that the TOE provide audit records in a manner that is suitable for an administrator to interpret.
	FAU_SAR.2 Restricted audit review	FAU_SAR.2 ensures that the TOE provides mechanisms to protect the audit records from unauthorized access.
	FAU_SAR.3 Selectable audit review	FAU_SAR.3 provides the ability for an administrator to sort the audit data to readily locate security relevant events of interest.
O.DISCOVER The TOE will discover new network devices added to the IT environment and report to the TOE when those devices are discovered.	FAU_GEN_EXP.1(1)Audit data generation	FAU_GEN_EXP.1(1) requires generation discovery log based on additional logical or physical elements and the ability to record information for each server object audit job.
O.MONITOR The TOE will collect and analyze critical data for network devices, systems, and applications and report on the performance, capacity, availability, and response of these	FAU_GEN_EXP.1(1)Audit data generation	FAU_GEN_EXP.1(1) requires generation discovery log based on additional logical or physical elements and the ability to record information for each server object audit job.

Objective	Security Functional Components	Rationale
resources.	FAU_GEN_EXP.1(2)Audit data generation	FAU_GEN_EXP.1(2) requires generation of poller audit logs based on MIBs and recording information within each entry of the web log.
	FAU_GEN_EXP.1(3)Audit data generation	FAU_GEN_EXP.1(3) requires generation of message logs and recording information within each entry of the poller audit log.
	FAU_GEN_EXP.1(4) Audit data generation	FAU_GEN_EXP.1(4) requires the TOE to be able to generate reports based on data stored in the Oracle database populated by the TOE.
	FAU_SAR_EXP.1(1) Audit review	FAU_SAR_EXP.1(1) requires the TOE to read information collected in FAU_GEN_EXP.1(1), FAU_GEN_EXP.1(2), FAU_GEN_EXP.1(3) FAU_GEN_EXP.1(4) from the discover logs, poller audit logs, message logs, and eHealth reports in a manner that is suitable for an administrator to interpret.
O.IDEN The TOE will provide measures to uniquely identify End Users and will authenticate the claimed identity prior to granting a user access to the TOE.	FIA_ATD.1 User attribute definition	FIA_ATD.1 ensures that End Users have a defined set of tasks that they can perform based on their access permissions defined by the eHealth System Administrator.
	FIA_UAU.2 User authentication before any action	FIA_UAU.2 requires a user be authenticated before any access to the TOE and resources protected by the TOE is allowed.
	FIA_UID.2 User identification before any action	FIA_UID.2 requires a user be identified before any access to the TOE and resources protected by the TOE is allowed.
O.MANAGE The TOE will provide eHealth System Administrators with the resources to manage and monitor user accounts, resources and security information relative to the TOE.	FMT_MSA.3Static Attribute Initialization	FMT_MSA.3 restricts the default values for users to no access. Only after an administrator has added permissions for an end user is he allowed to access.

Objective	Security Functional Components	Rationale
	FMT_MOF.1 Management of security functions behaviour	FMT_MOF.1 ensures that modification of any setting on the eHealth Server is handled by an eHealth System Administrator. End Users are permitted to modify their own password once authenticated through the web browser. Also permits authenticated end users to modify their own password, but not the password of any other user.
	FMT_MTD.1 Management of TSF data.	FMT_MTD.1 allows only authorized users to run and/or view reports on the eHealth Server.
	FMT_SMF.1 Specification of management functions	FMT_SMF.1 requires that the TOE provide the ability to manage its security functions including the management of user accounts and user access rights, TOE resources and security information recorded in the audit logs.
	FMT_SMR.1 Security roles	FMT_SMR.1 requires the TOE to provide the ability to set roles for security relevant authority as well as to restrict the ability to define and assign roles to ehealth System Administrators.
OE.SYSTIME The operating environment will provide reliable system time.	FPT_STM.1 Reliable Time Stamps	FPT_STM.1 requires that the underlying Operating System on the eHealth Server provide the timestamp for the audit trail.
OE.FILESYS The security features offered by the underlying Operating System protect the audit files.	FAU_STG.1 Protected Audit Trail Storage	FAU_STG.1 requires that the underlying Operating System on the eHealth Server protect the audit records generated by the TOE.
O.ROBUST_ADMIN_GUIDANCE The TOE will provide administrators with the necessary information for secure delivery and management.	ADO_DEL.1 Delivery procedures	ADO_DEL.1 describes product delivery and a description of all procedures used to ensure objectives are not compromised in the delivery process.
	ADO_IGS.1 Installation, generation, and startup procedures	ADO_IGS.1 document the procedures necessary and describe the steps required for the secure installation, generation, and start-up of the TOE.
	AGD_ADM.1 Administrator guidance	AGD_ADM.1 describes the processes to be used for proper administration of the TOE.
	AGD_USR.1 User guidance	AGD_USR.1 describes the proper use of the TOE from a user standpoint.
	AVA_MSU.1 Examination of guidance	AVA_MSU.1 describes the procedures to help the TOE users security install the product and software and perform operations.
OE.PROTECT The IT Environment will maintain a domain	FPT_RVM_EXP.1 Non-bypassability of the TSP	FPT_RVM_EXP.1 requires that the operating environment provide

Objective	Security Functional Components	Rationale
for its own execution that protects itself and its resources from external interference, tampering, or unauthorized disclosure.		mechanisms to prevent bypassing the security features provided and enforced by the TOE.
	FPT_SEP_EXP.1 TSF domain separation	FPT_SEP_EXP.1 requires that the operating environment provide an isolated domain for the TOE to operate.
O.SELF_PROTECTION The TSF will maintain a domain for its own execution that protects itself and its resources from external interference, tampering, or unauthorized disclosure.	FPT_RVM_EXP_TOE.1 Non-bypassability of the TSP	FPT_RVM_EXP_TOE.1 requires that the operating environment provide mechanisms to prevent bypassing the security features provided and enforced by the TOE.
	FPT_SEP_EXP_TOE.1 TSF domain separation	FPT_SEP_EXP_TOE.1 requires that the operating environment provide an isolated domain for the TOE to operate.
O.CRYPTOGRAPHIC_FUNCTIONS The TOE shall provide cryptographic functions for its own use, including encryption/decryption and password hashing.	FCS_CKM.1 Cryptographic key generation FCS_CKM.4 Cryptographic key destruction FCS_COP.1 Cryptographic operation FMT_MSA.2 Secure Security Attributes FPT_TRP.1 Trusted Path	This objective is to provide cryptographic functionality that is used by the TOE. The core functionality to be supported is encryption/decryption using a symmetric algorithm, and digital signature generation and verification using asymmetric algorithms. Since these operations involve cryptographic keys, how the keys are generated and/or otherwise obtained, and destroyed is specified. FCS_CKM.1 is a requirement that a cryptomodule generate symmetric keys. These keys are used for secure communication between remote users and the TOE (FPT_TRP.1). For SSL (RSA and 3DES)., such keys are used by the encryption/decryption functionality specified in FCS_COP.1(1). For mod_auth_digest (MD5) the algorithm is used for hashing user passwords and the functionality is specified in FCS_COP.1(2) Cryptographic keys must be generated using secure attributes to reduce the risk of compromise (FMT_MSA.2).

8.3 Security Assurance Requirements Rationale

The rationale for the Security Assurance Requirements is discussed in **Error! Reference source not found.**, TOE Security Assurance Measures of Section 6.2.

8.4 Requirement Dependency Rationale

All Security Functional Requirement component dependencies have been met by the TOE with the exception of FMT_MSA.1, FPT_STM.1 and ADV_SPM.1.

FMT_MSA.1 is a dependency for FMT_MSA.2 and FMT_MSA.3. The functionality was captured in FMT_MOF.1 and specific user and system settings/attributes controlled by the "Discretionary Access Control Policy" is defined in FMT_SMF.1.

FPT_STM.1, Reliable Time Stamps is a dependency on FAU_GEN.1, which is met by the IT environment. The underlying Operating System will be available to the TOE for use in determining the timestamp for the audit trail.

ADV_SPM.1 is a dependency of FMT_MSA.2. FMT_MSA.2 is included to satisfy the dependency for FCS requirements. ADV_SPM.1 is not applicable with regards to supporting cryptographic functionality and therefore is not included in this ST.

8.5 Explicitly Stated Requirements Rationale

This TOE contains the following explicit security functions:
FAU_GEN_EXP.1(1)
FAU_GEN_EXP.1(2)
FAU_GEN_EXP.1(3)
FAU_GEN_EXP.1(4)
FAU_SAR.EXP.1(1)
FPT_RVM_EXP_TOE.1
FPT_SEP_EXP_TOE.1
FPT_RVM_EXP.1
FPT_SEP_EXP.1

FAU_GEN_EXP.1(1), FAU_GEN_EXP.1(2), FAU_GEN_EXP.1(3), FAU_GEN_EXP.1(4) were created to capture the basic functionality provide by the TOE. FAU_GEN_EXP.1(1) allows for TOE to perform discovery of the monitored network and generate a discovery log to identify the logical or physical elements that were discovered. FAU_GEN_EXP.1(2) was created to the TOE to continue polling those elements discovered during the discovery process and generating a poller audit log to record captured information within each entry of the remote MIBs. FAU_GEN_EXP.1(3) was created to allow the TOE to record audit data in a message log to capture statistics polling window messages FAU_GEN_EXP.1(4) was created to allow end-users and administrators of the TOE to query the data collected by the other logs and run graphical reports on the data and track trends and perform analysis that can be used to improve the "health" of the network monitored by the polling process.

FAU_SAR.EXP.1(1) was created to provide additional capabilities of the TOE to read information collected in FAU_GEN_EXP.1(1), FAU_GEN_EXP.1(2), FAU_GEN_EXP.1(3), and FAU_GEN_EXP.1(4).

FPT_RVM_EXP_TOE.1, FPT_SEP_EXP_TOE.1, FPT_RVM_EXP.1, and FPT_SEP_EXP_.1 had to be explicitly stated because the TOE is software only and therefore can only provide partial TOE self-protection while relying on the OS and Hardware platforms to provide the full protection. The approach used for these requirements is according to the NIAP policy requiring software-only TOEs to use explicit requirements to specify the aspects provided by the TOE and those provided by the platform. The current reference for this policy is documents: 'TOE Protection, March 12, 2005', and 'CCEVS Policy on Accepting Security Target, April 8, 2005'. As with FPT_RVM.1, and FPT_SEP.1, on which they were based, these explicit requirements have no dependencies.

This Security Target does not include any explicitly stated Security Assurance Requirements.

8.6 TOE Summary Specification Rationale

This section identifies the security functions provided by the TOE mapped to the security functional requirement components contained in this ST. This mapping is provided in the following table.

Table 7 - SR to SFR Mapping

Security Function	Security Functional Components
Authorisation	FDP_ACC.1 Subset access control
	FDP_ACF.1 Security attribute based access control
Authentication	FIA_ATD.1 User attribute definition
	FIA_UAU.2 User authentication before any action
	FIA_UID.2 User identification before any action
Audit	FAU_GEN.1 Audit data generation
	FAU_GEN.2 User identity association
	FAU_GEN_EXP.1 Audit data generation
	FAU_SAR.1 Audit Review
	FAU_SAR.2 Restricted audit review
	FAU_SAR.3 Selectable audit review
	FAU_SAR_EXP.1 Audit Review
Data Protection	FDP_ACC.1 Subset access control
	FDP_ACF.1 Security attribute based access control
Security Management	FMT_MOF.1 Management of security functions behaviour
	FMT_MTD.1 Management of TSF data

Security Function	Security Functional Components
	FMT_MSA.3 Static Attribute Definition
	FMT_SMF.1 Specification of management functions
	FMT_SMR.1 Security roles
Self Protection	FPT_SEP_EXP_TOE.1 Domain Separation
	FPT_RVM_EXP_TOE.1 Reference Mediation
Trusted Path	FTP_TRP.1 Trusted Path
	FMT_MSA.2 Secure Security Attributes
	FCS_CKM.1 Cryptographic Key Management
	FCS_CKM.4 Cryptographic Key Destruction
	FCS_COP.1 Cryptographic Operations

8.6.1 Authorisation

The Authorisation function of the TOE enforces the FDP_ACC.1 and FDP_ACF.1 requirements. Authorisation protects the system resources from unauthorised access. Users' capability of accessing pages and files, or running applications is controlled by the corresponding authorisation policy. The TOE supports a policy that is created by the administrator upon installation of the system.

8.6.2 Authentication

The authentication function of the TOE enforces the FIA_ATD.1, FIA_UAU.2 and FIA_UID.2 requirements. Authentication is the process of determining the user's true identity. After following the configuration steps listed above in the authorisation section, the eHealth Suite is setup to authenticate users. A user accesses the eHealth Server through a browser on their Remote Workstation. The connection is established using HTTP over SSL. A user must authenticate to the eHealth Suite when challenged by providing a valid username and corresponding password. The information is sent encrypted from the user's web browser to the eHealth Server where access is either granted or denied by the eHealth Suite. User authentication is meaningful only if there is an extremely low probability of success for random attempts to authenticate as an authorized user. The requirement ensures that the secret authentication data is computationally difficult to guess randomly.

8.6.3 Audit

The audit function of the TOE enforces the FAU_GEN_EXP.1, FAU_GEN.1 FAU_GEN.2, FAU_SAR_EXP, and FAU_SAR requirements. The primary purpose of the audit security function FAU_GEN.1 is to generate auditable events as configured by the administrator. This is achieved by capturing events into a record that is stored as a flat file and protected by the local Operating System. FAU_GEN_EXP.1 captures the ability of the TOE to discover elements (FAU_GEN_EXP.1.1(1)) of resources in the intranet, and store those in a Oracle 9i database. Once the elements are populated in the database, the poller process "polls" these elements (FAU_GEN_EXP.1.1(2)) and identifies attributes of the elements. These attributes can be used to create reports (FAU_GEN_EXP.1.1(4)) that help the users of the TOE, track the health of the network over a period of time. Furthermore, Statistics Polling static window messages are stored (FAU_GEN_EXP.1.1(3)) on the underlying OS in a file called messages.stats.log. On the TOE these files can reach a maximum size of 100 MB. Once the log file reaches the maximum size, eHealth moves it to a backup log file named messagesbackup.bak and overwrites the existing backup log file, if one exists. eHealth then starts a new log file using the default file name. When the TOE saves the results of a discover process, the TOE creates a pollerAudit.*date*.*time*.log file. Where data and time come from the operating system clock. The TOE saves a minimum of seven files for each type of discover log. It deletes files in excess of the seven files that are older than seven days.

8.6.4 Data Protection

The data protection function of the TOE enforces the FDP_ACC.1 and FDP_ACF.1 requirements. Data is also protected through the access control provided by the TOE. In order to manipulate data, an administrator must successfully login to either the local machine where the eHealth Suite resides or via a Remote Workstation. End Users are not given permission to modify anything on the system besides their personal password attributes.

8.6.5 Security Management

The security management function of the TOE enforces the FMT_MOF.1, FMT_MTD.1, FMT_SMF.1, and FMT_SMR.1 requirements Security Management is implemented by the TOE through interactions by the administrator from a Remote Workstation and a local console. The administrator logs into the eHealth Suite from an SSL enabled web browser for remote access, and local authentication is used for the local Motif console. Once authenticated, the administrator has access to security management tabs within the eHealth Suite software that enable him/her to control system access by others. The administrator can control which data objects users may generate reports on or view. Additionally, the administrator may manage login attributes of the End Users.

8.6.6 Trusted Path

FCS_CKM.1, and FCS_CKM.4 are implemented by the Trusted Path Function. The TOE implements the cryptographic key generation and destruction functions of the SSL protocol to protect the communication channel for remote administration. FTP_TRP and FCS_COP.1 ensures the TOE implements SSL crypto operations to protect the communication channel for remote administration. FMT_MSA.2 ensures the TOE implements crypto operations using valid parameter values. The cryptography used in this product has not been FIPS certified nor has it been analyzed or tested to conform to cryptographic standards during this evaluation. All cryptography has only been asserted as tested by the vendor."

8.6.7 Self Protection

FPT_RVM_EXP_TOE.1 is implemented by the Self-Protection Function. The TOE makes sure that security enforcing functions are invoked and succeed before allowing any other mediated action to occur. FPT_SEP_EXP_TOE.1 is implemented by the Self-Protection Function. The Self-Protection Function provides a protected execution domain and a separation of traffic streams traversing the TOE. The TOE is a dedicated device, with no general purpose operating system, or programming interface. No untrusted processes are permitted on the TOE.

8.7 Strength of Function Rationale

As stated in section 6.1.3.3, there are no functions that support probabilistic or permutational methods, because the password policy for selecting a strong password for user authentication is enforced by the user only and described in the administrator and user guidance.

---

[i] “DCI” stands for Database Configuration Interchange, and such files represent configuration information in a proprietary ascii format. “Individual-operation” files are DCI files with a set of explicit instructions for adding configuration objects to the system.