CliniComp
Intelligent Charting & Surveillance

ESSENTRIS RELEASE 1.4
SECURITY TARGET

Prepared by:

CliniComp, Intl.
9655 Towne Centre Drive
San Diego, CA 92121
(858) 546-8202

P/N 255-50042-A (3/08)

This record is maintained throughout the life of the document; each published update is recorded. A Change Package (re-issue of changed pages only) carries change bars in the page margins to identify differences from the preceding issue. Due to the scope of change that necessitates a Revision (re-issue of entire document), a Revision does not carry change bars.

DOCUMENT VERSION NUMBER	REVISION SUMMARY	DATE
Version 1.0	Essentris Security Target Initial Delivery	20 April 2005
Version 1.1	Update for DOUMUS Observation Report 01	20 May 2005
Version 1.2	Update for DOMUS Comments	2 June 2005
Version 1.3	Fix Version control problem	3 June 2005
Version 1.4	Update version issues plus new Conformance Claim	14 June 2005
Version 1.5	Updates to reflect OS SFRs as Environmental	12 October 2005
Version 1.6	Minor changes	13 December 2005
Version 1.7	Typos	20 December 2005
Version 1.8	Comments from CSE: CB_383-4-43_ASE_OR –1	10 January 2006
Version 1.9	Update ST for EAL3	15 November 2006
Version 1.10	Update for Observation Report 10	25 January 2007
Version 1.11	Update for Observation Report 383-4-43-CB-OR-001	13 March 2007
Version 1.12	Update for OR12	18 June 2007

Version 1.13	Added a list of Auditable Events for the TOE to FAU_GEN.1 and updated Section 6.1.3.	31 July 2007
Version 1.14	Updated TOE identification to include the full Server and Client version numbers.	19 September 2007
Version 1.15	Updates based on lab comments.	28 January 2008
Version 1.16	Updated Server and CCI Configuration Tools versions. Other miscellaneous updates.	18 March 2008
Version 1.17	Corrected CCI Configuration Tools version.	19 March 2008
Rev A	Updated document to reflect assigned CCI part number and revision	19 March 2008

Table of Contents

Table of Figures

1 INTRODUCTION

This section identifies the security target (ST), target of evaluation (TOE), and ST organization. This ST describes a set of security requirements and specifications to be used as the basis for evaluations of the Essentris Clinical Information System Rel.1.4. (Essentris)

The ST contains the following additional sections:

Section	Topic
1	Introductory Material for the ST
2	TOE Description
3	TOE Security Environment
4	Security Objectives for Both TOE and TOE Environment
5	IT Security Requirements
6	TOE Summary Specification
7	Protection Profile Claims
8	Rationale

1.1 SECURITY TARGET AND TOE IDENTIFICATION

Target of Evaluation (TOE): Essentris Clinical Information System (Rel 1.4) (Server v204.42, Client v1.4.0002.0033, CCI Configuration Tools 1.4.0002.0032)

Evaluation Assurance Level: (EAL) 3

ST Title: Essentris Release 1.4 Security Target

ST Version: 255-50042-A (3/08)

ST Author: CliniComp, Intl.

1.2 CONFORMANCE CLAIM

Essentris Release 1.4 conforms to Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements (Version 2.3, August 2005). All International Common Criteria Interpretations through October, 2006 have been applied.

Essentris Release 1.4 is conformant to Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements (Version 2.3, August 2005). All International Common Criteria Interpretations through September, 2006 have been applied.

Essentris Release 1.4 is being evaluated to Evaluation Assurance Level 3 (EAL3) under the Canadian Common Criteria Scheme (CCS) using the Common Methodology for Information Technology Security Evaluation, Evaluation methodology, Version 2.3, August 2005. All International Common Criteria Interpretations through October, 2006 have been applied."

2 TOE DESCRIPTION

Essentris is a Commercial Off-the-Shelf (COTS) system developed and maintained by CliniComp International, Inc. (CCI). Essentris is installed at Medical Treatment Facilities (MTF) worldwide and supports health care providers in the delivery of inpatient clinical care. The system consists of COTS clinical information software that is integrated with physiological monitoring and automated medical instruments.

The major elements are the Data Acquisition System (DAS), and the redundant Essentris Central Servers.

2.1 SYSTEM DESCRIPTION

Essentris supports patient care throughout a medical facility, in the critical care, medical-surgical, and mother/infant units, the emergency department, selected outpatient units and a host of other locations. Essentris employs a client-server open architecture design and supports integration and use of industry standard hardware components.

Essentris supports documenting the following types of patient care:

- Physician/nurse histories and physicals
- Progress notes for all disciplines, including occupational therapists and social workers
- Assessments
- Vital sign monitoring
- Critical paths
- Plans of care
- Orders
- Admission data and laboratory and radiology values/results
- Medications/treatments
- Discharge summaries

Essentris also provides for graphical trending of patient parameters, a reference library, patient care educational materials, and various integrated ambulatory and imaging systems. All data values are entered by health care providers and through the acquisition of data from bedside monitoring devices and interfaces. The Essentris software interfaces with hospital information systems via a GUI-based front end for patient administration, laboratory, and radiological data. Essentris is directly connected to Food and Drug Administration regulated medical devices, which measure physiological patient data, electrocardiographs, waveforms, and uterine/fetal activity.

The system interfaces to bedside instruments such as physiologic monitors, ventilators, etc. Not only monitored parameters are read but also available wave forms from bedside instruments such as physiologic monitors and ventilators (EKGs, fetal strips, etc.). The Essentris system has the capability of acquiring, processing and archiving this data for more than 24 hours, assuming adequate hardware facilities are in place. Interfacing with bedside instruments is performed by remote data acquisition units (DAS boxes), which implement each instrument’s individual protocol and perform local processing storage.

System users access Essentris via a Windows (Microsoft) front end. System access devices consist of both fixed and portable workstations designed to support different physical plants and work designs.

Essentris utilizes both CCI installed and existing Medical Treatment Facility Local Area Networks (LAN) supported by the host installation to provide connectivity between the workstations and servers. The LAN is extended to the bedside and operates with Transmission Communications Protocol/Internet Protocol (TCP/IP)100BaseT Ethernet. Essentris uses Health Level-7 (HL-7) bi-directional minimal lower level protocol to communicate with the external interfaces.

The system runs on redundant central computers using the UNIX operating system. This architecture allows upgrades and maintenance with no scheduled downtime.

Essentris is designed so that no single point of failure will prevent its operation or prevent access to patient data. In the event of a loss of one CCI server in a cluster, the users reconnect workstations to one of the remaining CCI server. The failure will require the user to re-launch the user application. The stored data will be restored intact but any data not stored will be lost.

Essentris is comprised of the following hardware components. These hardware components serve as the baseline for all Essentris installations. The specific hardware components and quantities installed at an operational site will vary from MTF-to-MTF depending on the external interfaces; facility size, configuration, mission; and number of units supported. The following table is a sample configuration for Essentris.

EQUIPMENT	DESCRIPTION
MTF Work Station	PC running Windows2000 Manufacturer: COTS Minimum Configuration: *Pentium III 550 MHz; Color High Resolution 1280 x 1024 at 64k colors; 500 MB Hard Drive; 256 MB Memory; 256 MB Virtual Memory; OS Windows NT4.0, Service Pack 6 or higher, Windows 2000, Service aPck 2, or Windows XP; Internet Explorer 5.5 Browser; Network 10 Mbps*
Fetal Monitoring Remote Display	Essentris X Terminal Manufacturer: CCI Type: Proprietary Minimum Configuration: 8MB RAM, 2MB VRAM, 2MB flash memory, color high resolution 17" SVGA non-interlaced monitor, 1280 x 1024 pixels resolution, 0.26mm dot pitch, 10 Base T Ethernet interface, IBM-101 keyboard with pointing device Flat Panel - TFT/AMLCD with 10 Base T Ethernet interface, color high resolution 13" SVGA monitor, 1280 x 1024 pixels resolution, 0.28mm dot pitch, IBM-101 keyboard with pointing device
Printer	Manufacturer: COTS Type: Various laser printers
Data Acquisition System	Manufacturer: CCI Type: Proprietary Minimum Configuration: Motorola-based or MIPS-based system with custom motherboard and other components. Function: Intelligent data acquisition subsystem that interfaces with Automated Medical Instruments (AMIs) and Physiological Monitoring Systems (PMSs) to acquire, validate, and store physiological patient data.

EQUIPMENT	DESCRIPTION
Essentris -Basic server (2 per MTF)	Vendor: Hewlett Packard Corp Type HP rx2600 CPU: Itanium 64 bit CPU Minimum configuration: 8 GB RAM, 2 CPUs, (1) 36 GB SCSI Hard Drive, PCI X-RAID Array w/ (4) 73 GB SCSI Hard Disks, DVD Reader, Ethernet Interfaces
CCI-GDR	Vendor: Hewlett Packard Corp Type HP rx2600 CPU: Itanium 64 bit CPU Minimum configuration: 8 GB RAM, 2 CPUs, (1) 36 GB SCSI Hard Drive, PCI X-RAID Array w/ (4) 73 GB SCSI Hard Disks, DVD Reader, Ethernet Interfaces
Essentris Tape Backup Drive	Vendor: Hewlett Packard StorageWorks Ultrium Tape Storage device. Type: High performance Ultra 3 SCSI device with a maximum burst transfer speed of 160 MB/second with 400 GB capacity on a single cartridge
Uninterruptible Power Supply - 2	Brand: Powerware (formerly BEST) Make/model: FERRUPS 3.1 KVA

Figure 2.1-1 Essentris Hardware Minimum Requirements

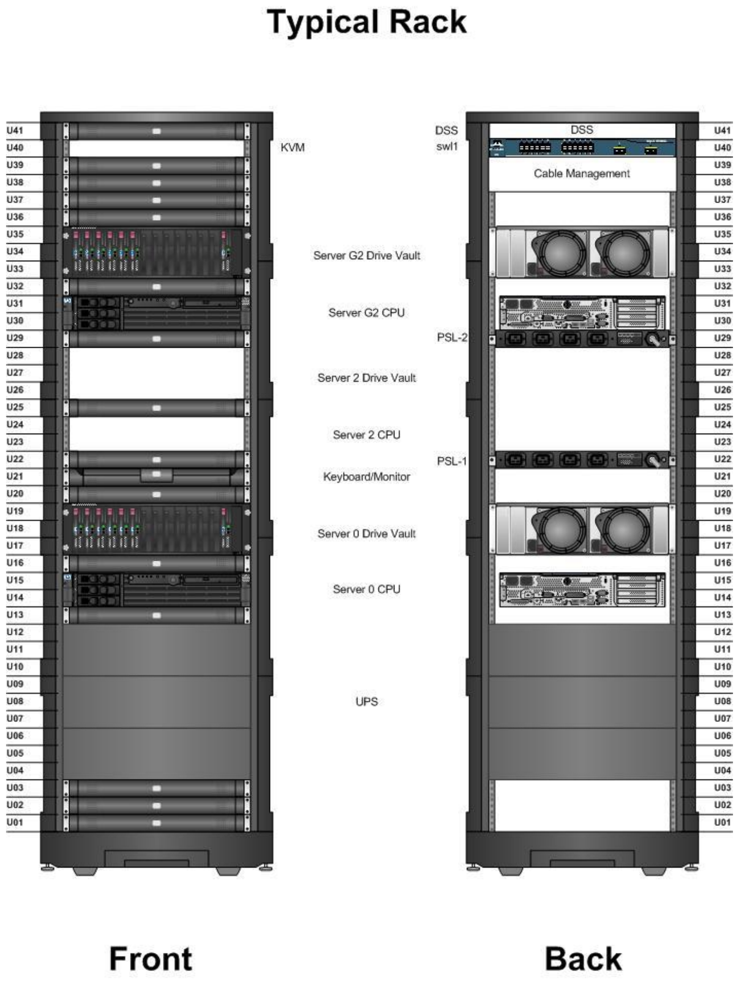

Figure 2.1-2 Typical Rack Configuration

2.1.1 Data Acquisition System (DAS)

The Data Acquisition System provides the interface to bedside instruments, (i.e., physiologic monitors, ventilators, and arterial blood gas machines) and continuous waveforms, EKGs, and fetal heart rate strips. Functionally, the DAS performs continuous queries to all devices and stores the timed parameters in RAM.

DAS runs on CCI's custom equipment based on the Motorola or MIPS CPU with custom motherboards and other components. Connectivity between the DAS and bedside instruments is via a RS232 direct connection or through the MTF physiological monitoring network(s). Other direct connection protocols may be used; however, they need to be converted to RS232 (or RS422 for longer cable runs) to achieve successful connectivity to the DAS.

2.1.2 Operating Systems

Essentris runs on redundant computer systems using the Hewlett Packard's HP-UX commonly referred to as the HP-UX (UNIX) 11.23 Operating System. This strategy supports upgrade and maintenance with no scheduled downtime. The CCI Database (CCIDB) is a proprietary object-based database management system that runs on HP-UX (UNIX) 11.23 server. DAS also runs on a HP-UX (UNIX) 11.23 server. This OS is the current version of the Hewlett-Packard HP-UX (11i) Version 11.11, which has been evaluated at an EAL 4.

2.1.3 GDR

The Global Data Repository (GDR) provides a separate database with a relational software layer that supports Structured Query Language (SQL) queries and is Microsoft ODBC compliant to interface with standard COTS relational database platforms.

The GDR is not the primary repository for Essentris charting data, which are contained in the CCIDB in a proprietary format. Rather, the GDR is the primary repository that enables read-only SQL/ODBC queries of the charted data. The GDR is an Oracle database, which is populated in similar fashion to the redundant CCIDBs. The GDR database can exist on the same hardware platform as the CCIDB and contain identical data as the associated CCIDB, but the data is stored in Oracle tables.

2.1.4 Data Storage and Redundancy

Essentris provides nearly unlimited data storage for permanent and temporary patient files. All patient data for the patient's entire length of stay is stored on-line for a period defined by each MTF and then automatically archived. After a patient's discharge, the related data may be kept on the system for a time frame specified by the MTF. The Essentris administrator sets the time frame at which on-line patient data is archived.

Maintenance scripts are used to verify stored data on the redundant servers is the same. The maintenance scripts generate checksums, which are used to compare redundant CCIDBs. The dbck script runs on one host and parses files to check for corruption. The dbRedundchk script checks files on the redundant servers to verify the files are the same on each server. The dbRedundchk reports checksum discrepancies to CCI support staff, who manually analyzes and corrects the discrepancies. Correcting discrepancies is done in consultation with a Clinical System Adminstrator (CSA), if appropriate. These scripts are also called when unarchiving patient records. In addition, a manual CCIDB database integrity check is performed remotely by CCI support staff when a host is brought into production, for example as part of system recovery or a version upgrade.

2.1.5 Uninterruptible Power Supply

Each CCI clustered server is paired with an Uninterruptible Power Supply (UPS), Powerware FERRUPS 3.1 KVA, for protection from power failure, surges, and spikes. Each UPS provides power failure computer control with a minimum of 100 minutes support at full load. CCI recommends that the UPS be connected to the MTFs emergency power in the event of an extended outage. An Essentris minimum configuration consists of two server racks, which will each have a UPS attached. When three or more servers are delivered there is a maximum of three UPS units across the servers to provide sufficient redundancy in the case of failure of a single rack.

2.1.6 Communications

All of the following Essentris-External interfaces are accomplished via an Ethernet connection to the MTF network and lie within the physical boundary of Essentris. The communications protocols supporting this interface are HL-7 which use TCP/IP. Each data item received from external systems can be identified as a database item in the CCIDB. As a database item, the data item can then be configured to display on more than one Essentris application screen.

2.1.6.1 External Laboratory Interface

External laboratory interface sends laboratory test results to Essentris entered by the MTF laboratory personnel. This data includes result value, flags or “alerts” (e.g., high, low), normal range for a particular value, and annotation (textual) attached to the value. Typically, laboratory values are configured to appear on the Essentris Laboratory and Summary screens.

2.1.6.2 Admission Interface

Admission interface sends inpatient demographic and admission data to Essentris as directed by the MTF admissions and/or clinical staff.

2.1.6.3 Radiology Interface

Essentris receives the results of radiology tests entered by the MTF Radiology staff. This data are textual comments that display in a Radiology note.

2.2 SECURITY ROLE TYPES

The TOE supports the following role types.

- Clinical System Administrator
- User

Each of the role types has specific responsibilities and privileges in the system. These are described in the table below:

Role Type	Responsibility	Privileges
Clinical System Administrator (CSA)	Administrates system accounts for users.	Has access to all user accounts Has access to all user data Creates user accounts, sets user permissions, sets user passwords, and revokes accounts. Administers the Essentris Access Control Policy.
User	Enters data, reviews patient data, prints patient data.	Read, Write, Print based on Access Controls set by administrator.

Figure 2.2-1 Security Roles

2.3 PRODUCT TYPE

Essentris is a commercial off-the-shelf (COTS) system developed and maintained by CliniComp International (CCI). Essentris is installed at Medical Treatment Facilities worldwide and supports health care providers in the delivery of inpatient clinical care.

2.4 TOE BOUNDARY

The physical boundary of the Target of Evaluation (TOE) is the software application of Essentris which includes the CCI Configuration Tools, Terminal Configuration Tool, Staff Configuration Tool, Audit Log Viewer, Preference files, CCIDB, and User Authentication. It excludes the Operating System, MySQL database, GDR, medical devices, hardware platforms and all connected peripheral devices.
The logical TOE boundary includes Audit, Discretionary Access Controls, Authentication and Security Management.

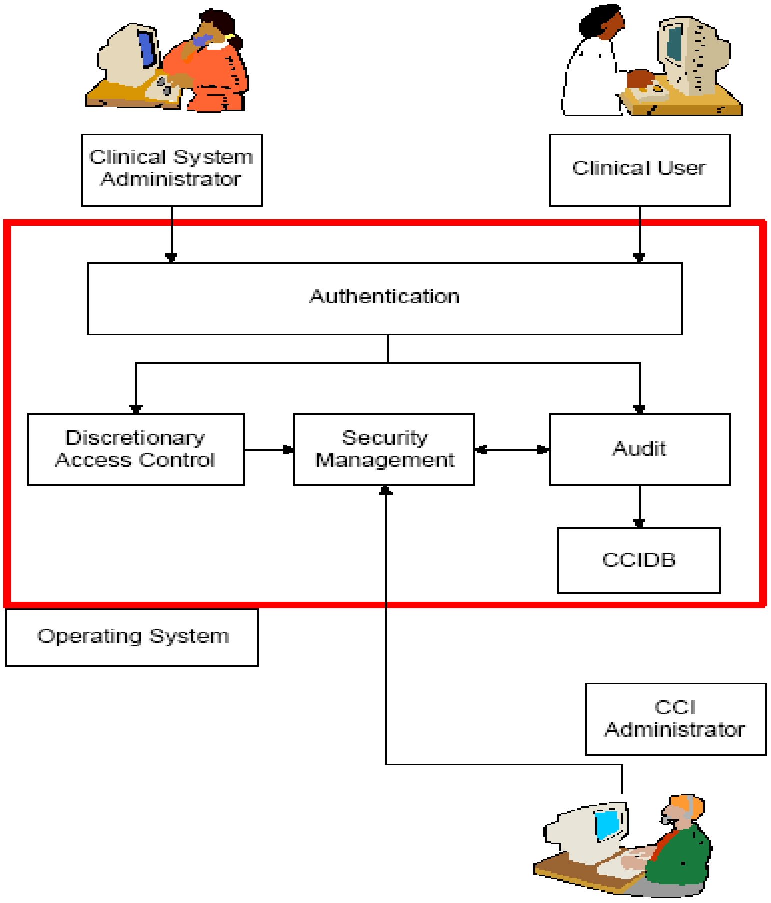

Figure 2.4-1 TOE Security Boundary

2.4.1 Audit (ITSF_AUDIT)

The Audit function is designed to track and store all activities performed on the Essentris System. The Audit Log Viewer allows CSAs to monitor user activity.

2.4.2 Discretionary Access Control (ITSF_DAC)

Discretionary Access Control (DAC) restricts user access to system data and functions based upon the user’s duties and responsibilities for providing patient care.

In addition, Essentris limits access to the data or functions that can be performed from an individual terminal. Users are also limited to only certain applications and functions.

2.4.3 Authentication (ITSF_AUTHENTICATION)

Authentication ensures that individual accountability can be established and maintained for users, and that access control decisions can be made based on user security attributes.

2.4.4 Security Management (ITSF_SECURITY MANAGEMENT)

The security management objective is to provide separate security-relevant system management functions from non-security-relevant functions.

3 TOE SECURITY ENVIRONMENT

The TOE Security environment consists of the Threats to Security, Organizational Security Policies, and usage assumptions as they relate to the Essentris Clinical Information System.

Essentris provides for a level of protection that is appropriate for **The Health Insurance Portability and Accountability Act of 1996** (HIPAA) compliant Information Technology (IT) environment. It is designed to withstand logical attacks originating from outside the security boundary.

3.1 THREATS TO SECURITY

Threats are those circumstances and events with the potential to cause harm to a system. This report considers the variety of threats to which Essentris may be subjected. In examining these threats the various types of harms that can be caused to the system are identified.

The list of harms must address the various components of the system including its data, software, hardware, network infrastructure, facility, and support organizations. For the purposes of this analysis, the list of potential harms to Essentris has been summarized as follows:

Name (T = Threat)	Threat	Method
T.ACCESS	Impeding the availability of system services	An unauthorized user could prevent speedy access to patient data interrupting or disrupting patient care.
T.DISCLOSE	Unauthorized disclosure of sensitive information	An unauthorized user could access patient data in violation of HIPAA. Information could be disclosed to non-authorized persons.
T.MODIFY	Unauthorized modification of information	An unauthorized user could alter patient data resulting in incorrect information being available to authorized users.
T.RESOURCE	Unauthorized use of system resources	An unauthorized user could use system resources for their personal use. This could result in denial of timely patient care.

Figure 3.1-1 Threat Agents

3.2 ORGANIZATIONAL SECURITY POLICY

An Organizational Security Policy is a set of rules or procedures imposed by an organization on its operations to protect its sensitive data. The following policies are required to be enforced in the organization that hosts the TOE.

Name	Policy
P.ACCOUNTABILITY	The users of the system shall be held accountable for their actions within the system.
P.DISCRETIONARY-ACCESS	Only those users who have been authorized to access the information within the system may access the system
P.NEED_TO_KNOW	The system must limit the access to, modification of, and destruction of the information in protected resources to those authorized users which have a “need to know” for that information.

Figure 3.2-1 Secure Usage Assumptions

3.3 SECURE USAGE ASSUMPTIONS

The specific conditions listed below are assumed to exist in the TOE environment. These assumptions include both practical realities in the implementation of the TOE, security requirements and the essential environmental conditions on the use of the TOE.

Name (A=Assumption)	**Condition**	**Assumption**
A.ADMIN	Personnel	Systems administration functions are only performed by trained and trusted system administrators.
A.AVAIL	Environment	The TOE will be installed in an IT environment built for complete system and data availability.
A.CONNECT	Environment	All connections to peripheral devices reside within the controlled access facilities. TOE only addresses security concerns related to the manipulation of the TOE through its authorized access points. Internal communication paths to access points such as terminals are assumed to be adequately protected.
A.INTERNAL_CHANNEL	Environment	The internal communication channel between the TOE Client and Server platforms is a LAN that resides within the controlled access facilities. Internal communication paths connecting TOE Client and Server Platforms are assumed to be adequately protected.
A.LOCATE	Environment	The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.
A.NOEVIL	Personnel	Authorized administrators and installers are non-hostile.

Figure 3.3-1 Secure Usage Assumptions

4 SECURITY OBJECTIVES

The fundamental security objectives for Essentris are the HIPAA security requirements:

- Protect Sensitive Information (SI) from unauthorized disclosure, modification, and deletion
- Protect critical services and resources from unauthorized use and security-relevant denial of service conditions.

Essentris security safeguards protect the system and data from unauthorized disclosure, modification, and destruction. This section reviews the Essentris fundamental security objectives and identifies the means provided in support of the security objectives described below:

Essentris enforces confidentiality of sensitive system data by ensuring that system access is granted only after positive identification of system users. In addition, Essentris limits access to devices. Each user is granted permissions (e.g., none, read, write, and modify) by the Clinical System Administrator (CSA) for each Essentris application based on the need-to-know criteria established within the respective MTF.

Essentris enforces data integrity by requiring each user to enter a User Identification Code (UIC) and password prior to executing the store function. Essentris also identifies each instance where stored data has been deleted or modified, including the user performing the action. The authorized user for all stored data entries is recorded in the Essentris database.

Essentris ensures individual accountability by associating each recorded event to a specific user based upon a unique UIC assigned to the user account by the system. In addition to the requirement for users to enter their UIC and password in order to gain system access, Essentris users must enter their UIC and password in order to complete most transactions. Accountability is further enhanced by requiring approval and countersigning of certain critical functions, (i.e., ordering medication, ordering treatment) based on a user's assigned permissions. Essentris also provides the capability to restrict access to patient data within a unit to only those terminals physically located in the unit. When implemented properly, this capability restricts authorized users in one unit from accessing data on patients assigned to another unit.

Essentris is a fully redundant system, ensuring complete system and data availability. Protection against external system threats is enforced by the HP-UX (UNIX) 11.23 Operating System.

Name (O = Objective)	Objective	
O.ACCOUNTABILITY	The TSF shall hold users of the system accountable for their actions within the system.	**TOE Security Objective**
O.AUDITING	The TSF must record the security relevant actions of users of the TOE. The TSF must present this information to authorized Administrators.	**IT Environment Security Objective and** **TOE Security Objective**

Name (O = Objective)	Objective	
O.AUTHENTICATION	The TSF grants system access only after positive identification of system users.	**TOE Security Objective**
O.CONFIDENTIALITY	Essentris enforces confidentiality of sensitive system data by ensuring that system access is granted only after positive identification of system users.	**IT Environment Security Objective and** **TOE Security Objective**
O.DISCRETIONARY_ ACCESS	The TSF must ensure that only authorized users gain access to the TOE and its resources,	**TOE Security Objective**
O.ENFORCEMENT	The TSF must be designed and implemented in a manner, which ensures that the organizational policies are enforced in the target environment without by-pass and interference.	**IT Environment Security Objective and** **TOE Security Objective**
O.INTEGRITY	The TSF requires each user to enter a User Identification Code (UIC) and password prior to executing the store function.	**TOE Security Objective**
O.NON-REPUDIATION	Essentris identifies each instance where stored data has been deleted or modified, including the user performing the action.	**IT Environment Security Objective and TOE Security Objective**
O.ADMIN	Administrators are trained and trusted to perform their System Administration Functions.	**Non-IT**
O.AVAILABILITY	Essentris provides a fully redundant system to ensure complete system and data availability except during schedule maintenance outages.	**Non-IT**
O.CONNECT	Essentris internal and external connections reside within controlled access facilities.	**Non-IT**
O.INTERNAL_CHANNEL	The TSF requires that LAN connections between the TOE Server and Client platforms are physically isolated from external communications channels.	**Non-IT**

Figure 3.3-1 Security Objectives

5 IT SECURITY REQUIREMENTS

5.1 TOE IT SECURITY FUNCTIONAL REQUIREMENTS

TOE security functional requirements (SFRS) are defined as functional components drawn from part 2 of the Common Criteria. The TOE meets all SFRS claimed in the next section.

CC Component	Name	Hierarchal To	Dependencies
FAU_GEN.1	Audit data generation		FPT_STM.1
FAU_GEN.2	User identity association		FAU_GEN.1 FIA_UID.1
FAU_SAR.1	Audit review		FAU_GEN.1
FAU_SAR.2	Restricted audit review		FAU_SAR.1
FAU_SAR.3	Selectable audit review		FAU_SAR.1
FAU_STG.1	Protected audit trail storage		FAU_GEN.1
FDP_ACC.1	Subset access control policy		FDP_ACF.1
FDP_ACF.1	Security attribute based access control		FDP_ACC.1 FMT_MSA.3
FIA_ATD.1	User attribute definition		
FIA_UAU.2	Timing of authentication	FIA_UAU.1	FIA_UID.1
FIA_UAU.7	Protected authentication feedback		FIA_UAU.1
FIA_UID.2	User identification before any action	FIA_UID.1	
FIA_USB.1	User-subject binding		FIA_ATD.1
FMT_MSA.1	Management of security attributes		FDP_ACC.1 FMT_SMF.1 FMT_SMR.1
FMT_MSA.3	Static attribute initialization		FMT_MSA.1 FMT_SMR.1

CC Component	Name	Hierarchal To	Dependencies
FMT_MTD.1	Management of TSF data		FMT_SMF.1 FMT_SMR.1
FMT_SMF.1	Specification of management functions		
FMT_SMR.1	Security roles		FIA_UID.1

Figure 5.1-1 Security Functional Requirements

5.1.1 Security Audit Data Generation (FAU_GEN)

This family defines requirements for recording the occurrence of security relevant events that take place under TSF control. This family identifies the level of auditing, enumerates the types of events that shall be auditable by the TSF, and identifies the minimum set of audit-related information that should be provided within various audit record types.

5.1.1.1 FAU_GEN.1 Audit data generation

Hierarchal to no other component.

5.1.1.1.1 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 *none* level of audit;

c) [*The auditable events specified in* Figure 5.1-2 Auditable Events].

Auditable Event	Description
All requests to perform an operation on an object covered by the SFP (Related SFR: FDP_ACF.1)	
All use of the authentication mechanism	
Successful use of the user identification mechanism	User identity
Creation of a user account	User identity
Modifications to the permissions and properties of a user account	User identity
Deletion of a user account	User identity
Creation of a user role	User role identity
Modifications to a user role	User role identity
All modifications to the values of TSF data (Related SFR: FMT_MTD.1)	
Use of the management functions (Related SFR: FMT_SMF.1)	

Figure 5.1-2 Auditable Events

5.1.1.1.2 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.

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, *no other audit relevant information*

Dependencies: FPT_STM Reliable time stamps

5.1.1.2 FAU_GEN.2 User identity association

Hierarchal to no other component.

5.1.1.2.1 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

5.1.2 Security Audit Response (FAU_SAR)

This family defines the requirements for audit tools that should be available to authorized users to assist in the review of audit data.

5.1.2.1 FAU_SAR.1 security audit review

Hierarchal to no other component.

5.1.2.1.1 FAU_SAR.1.1

The TSF shall provide *CSA* with the capability to read *UserID, UserName, Action performed, and Time stamp* from the audit records.

5.1.2.1.2 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

5.1.2.2 FAU_SAR.2 Restricted audit review

Hierarchal to no other component.

5.1.2.2.1 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

5.1.2.3 FAU_SAR.3 Selectable audit review

Hierarchal to no other component.

5.1.2.3.1 FAU_SAR.3.1

The TSF shall provide the ability to perform *searches* of audit data based on *span of time, operator, and staff name,*

.

Dependencies: FAU_SAR.1 Audit review

5.1.3 Security Audit Event Storage (FAU_STG)

This family defines the requirements for the TSF to be able to create and maintain a secure audit trail.

5.1.3.1 FAU_STG.1 Protected audit trail storage

Hierarchal to no other component.

5.1.3.1.1 FAU_STG.1.1

The TSF shall protect the stored audit records from unauthorized deletion.

5.1.3.1.2 FAU_STG.1.2

The TSF shall be able to *detect* unauthorized modifications to the stored audit records in the audit trail.

Dependencies: FAU_GEN.1 Audit data generation

5.1.4 Access Control Policy (FDP_ACC)

This family identifies the access control SFPs (by name) and defines the scope of control of the policies that form the identified access control portion of the TSP. This scope of control is characterized by three sets: the subjects under control of the policy, the objects under control of the policy, and the operations among controlled subjects and controlled objects that are covered by the policy. The criteria allow multiple policies to exist, each having a unique name. This is accomplished by iterating components from this family once for each named access control policy. The rules that define the functionality of an access control SFP will be defined by FDP_ACF. The names of the access control SFPs identified here in FDP_ACC are meant to be used throughout the remainder of the functional components that have an operation that calls for an assignment or selection of an "access control SFP."

5.1.4.1 FDP_ACC.1 Subset access control

Hierarchal to no other component.

5.1.4.1.1 FDP_ACC.1.1

The TSF shall enforce the *Essentris Access Control* on

Objects: All objects created, stored, handled and destroyed in the device
Operations: *Read, Write, Modify, None.*

Dependencies: FDP_ACF.1 Security attribute based access control

5.1.5 Access Control Functions (FDP_ACF)

This family describes the rules for the specific functions that can implement an access control policy named in FDP_ACC. FDP_ACC specifies the scope of control of the policy.

5.1.5.1 FDP_ACF.1 Security attribute based access control

Hierarchal to no other components

5.1.5.1.1 FDP_ACF.1.1

The TSF shall enforce the *Essentris Access Control* to objects based on:

Subject attributes: UserID, Password, Role.
Operations: Read, Write, Modify, None

5.1.5.1.2 FDP_ACF.1.2

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: *Read, Write, Modify, None*

5.1.5.1.3 FDP_ACF.1.3

The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: *None*

5.1.5.1.4 FDP_ACF.1.4

The TSF shall explicitly deny access of subjects to objects based on the *Read, Write, Modify, None attributes that explicitly deny access of subjects to objects*.

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

5.1.6 User Attribute Definition (FIA_ATD)

All authorized users may have a set of security attributes, other than the user's identity, that is used to enforce the TSP. This family defines the requirements for associating user security attributes with users as needed to support the TSP.

5.1.6.1 FIA_ATD.1 User attribute definition

All authorized users may have a set of security attributes, other than the user's identity, that is used to enforce the TSP. This family defines the requirements for associating user security attributes with users as needed to support the TSP.

5.1.6.1.1 FIA_ATD.1.1

The TSF shall maintain the following list of security attributes belonging to individual users: *Read, Write, Modify, None*.

Dependencies: No dependencies

5.1.7 User Authentication (FIA_UAU)

This family defines the types of user authentication mechanisms supported by the TSF. This family also defines the required attributes on which the user authentication mechanisms must be based.

5.1.7.1 FIA_UAU.2 User authentication before any action

Hierarchical to: FIA_UAU.1

5.1.7.1.1 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

5.1.7.2 FIA_UAU.7 Protected authentication feedback

Hierarchical to: FIA_UAU.1

5.1.7.2.1 FIA_UAU.7.1

The TSF shall provide only *the authentication screen* to the user while the authentication is in progress.

Dependencies: FIA_UAU.1 Timing of identification

5.1.8 User Identification (FIA_UID)

This family defines the conditions under which users shall be required to identify themselves before performing any other actions that are to be mediated by the TSF and which require user identification.

5.1.8.1 FIA_UID.2 User identification before any action

Hierarchical to: **FIA_UID.1**

5.1.8.1.1 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 as defined

Dependencies: No dependencies

5.1.9 User-Subject Binding (FIA_USB)

An authenticated user, in order to use the TOE, typically activates a subject. The user's security attributes are associated (totally or partially) with this subject. This family defines requirements to create and maintain the association of the user's security attributes to a subject acting on the user's behalf.

5.1.9.1 FIA_USB.1 User-subject binding

Hierarchal to no other components

5.1.9.1.1 FIA_USB.1.1

The TSF shall associate the appropriate user security attributes with subjects acting on behalf of that user:

The UserID and Password is used to enforce the Essentris Access Control Policy

The user role which is used to enforce the Essentris Access Control Policy

The appropriate other user security attributes: Read, Write, Modify, None.

5.1.9.1.2 FIA_USB.1.2

The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: *Read, Write, Modify, None.*

5.1.9.1.3 FIA_USB.1.3

The TSF shall enforce the following rules governing changes to the user security attributes with subjects acting on the behalf of users: *none.*

Dependencies: FIA_ATD.1 User attribute definition

5.1.10 Management of Security Attributes (FMT_MSA)

This family allows authorized users control over the management of security attributes. This management might include capabilities for viewing and modifying of security attributes.

5.1.10.1 FMT_MSA.1

Hierarchical to: No other components.

5.1.10.1.1 FMT_MSA.1.1

The TSF shall enforce the *Essentris Access Control,* to restrict the ability to: *change_default, modify, delete,* the security attributes *Read, Write, Modify, None* to *the CSA*.

Dependencies: [FDP_ACC.1 Subset access control or
FDP_IFC.1 Subset information flow control]
FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

5.1.10.2 FMT_MSA.3

Hierarchical to: No other components

5.1.10.2.1 FMT_MSA.3.1

The TSF shall enforce the *Essentris Access Control,* to provide *permissive* default values for security attributes that are used to enforce the *SFP*.

5.1.10.2.2 FMT_MSA.3.2

The TSF shall allow the *CSA* 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

5.1.11 Management of TDF Data (FMT_MTD)

This family allows authorized users (roles) control over the management of TSF data. Examples of TSF data include audit information, clock, system configuration and other TSF configuration parameters.

5.1.11.1 FMT_MTD.1

Hierarchical to: No other components

5.1.11.1.1 FMT_MTD.1.1

The TSF shall restrict the ability to *change_default, query, modify, delete, clear,* the *Read, Write, Modify, None* to the CSA

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

5.1.12 Specification of Management Functions (FMT_SMF)

This family allows the specification of the management functions to be provided by the TOE. Management functions provide TSFI that allow administrators to define the parameters that control the operation of security-related aspects of the TOE, such as data protection attributes, TOE protection attributes, audit attributes, and identification and authentication attributes. This family works in conjunction with the other components in the FMT class: the component in this family calls out the management functions, and other families in FMT: Security Management restricts the ability to use these management functions.

5.1.12.1 FMT_SMF.1

Hierarchical to: No other components

5.1.12.1.1 FMT_SMF.1.1

The TSF shall be capable of performing the following security management functions: *Data protection attributes, TOE Protection Attributes, audit attributes, and identification and authentication attributes.*

Dependencies: No Dependencies

5.1.13 Senior Management Roles (FMT_SMR)

This family is intended to control the assignment of different roles to users. The capabilities of these roles with respect to security management are described in the other families in this class.

5.1.13.1 FMT_SMR.1

Hierarchical to: No other components

5.1.13.1.1 FMT_SMR.1.1

The TSF shall maintain the roles *Clinical System Administrator and User*.

5.1.13.1.2 FMT_SMR.1.2

The TSF shall be able to associate users with roles.

Dependencies: FIA_UID.1 Timing of identification

5.2 SECURITY REQUIREMENTS FOR THE IT ENVIRONMENT

Essentris runs on a secure EAL 4 OS, which is outside the TOE security boundary. The OS provides reference mediation, domain separation, and secure time stamp for the Essentris product.

CC Component	Name	Hierarchal To	Dependencies
FPT_RVM.1	Non-bypassability of the TSP		
FPT_SEP.1	TSF domain separation		
FPT_STM.1	Reliable time stamps		

Figure 5.2-1 Security Requirements for the IT Environment

5.2.1 Reference Mediation (FPT_RVM)

The requirements of this family address the "always invoked" aspect of a traditional reference monitor. The goal of this family is to ensure, with respect to a given SFP, that all actions requiring policy enforcement are validated by the TSF against the SFP. If the portion of the TSF that enforces the SFP also meets the requirements of appropriate components from FPT_SEP (Domain separation) and ADV_INT (TSF internals), then that portion of the TSF provides a "reference monitor" for that SFP.

A TSF that implements a SFP provides effective protection against unauthorized operation if and only if all enforceable actions (e.g. accesses to objects) requested by untrusted subjects with respect to any or all of that SFP are validated by the TSF before succeeding. If an action that could be enforceable by the TSF is incorrectly enforced or incorrectly bypassed, the overall enforcement of the SFP could be compromised. Subjects could then bypass the SFP in a variety of unauthorized ways (e.g. circumvent access checks for some subjects or objects, bypass checks for objects whose protection was assumed by applications, retain access rights beyond their intended lifetime, bypass auditing of audited actions, or bypass authentication). Note that some subjects, the so called "trusted subjects" with respect to a specific SFP, might be trusted to enforce the SFP by themselves, and bypass the mediation of the SFP.

5.2.1.1 FPT_RVM.1

Hierarchical to: No other components.

5.2.1.1.1 FPT_RVM.1.1

The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

Dependencies: No dependencies

5.2.2 Domain Separation (FPT_SEP)

The components of this family ensure that at least one security domain is available for the TSF's own execution and that the TSF is protected from external interference and tampering (e.g. by modification of TSF code or data structures) by untrusted subjects. Satisfying the requirements of this family makes the TSF selfprotecting, meaning that an untrusted subject cannot modify or damage the TSF.

5.2.2.1 FPT_SEP.1

Hierarchical to: No other components

5.2.2.1.1 FPT_SEP.1.1

The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

5.2.2.1.2 FPT_SEP.1.2

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

Dependencies: No dependencies

5.2.3 Time Stamps (FPT_STM)

This family addresses requirements for a reliable time stamp function within a TOE.

5.2.3.1 FPT_STM.1 Reliable time stamps

Hierarchical to: No other components.

5.2.3.1.1 FPT_STM.1.1

The TSF shall be able to provide reliable time stamps for its own use.

Dependencies: No dependencies

5.3 SECURITY ASSURANCE REQUIREMENTS

The following Security Assurance Requirements are claimed in accordance with EAL 3 requirements, as stated in Part 3 of the CC:

ACM_CAP.3	Authorization Controls
ACM_SCP.1	TOE CM coverage
ADO_DEL.1	Delivery procedures
ADO_IGS.1	Installation, generation, and start-up procedures
ADV_FSP.1	Informal functional specification
ADV_HLD.2	Security enforcing high-level design
ADV_RCR.1	Informal correspondence demonstration
AGD_ADM.1	Administrator guidance
AGD_USR.1	User guidance
ALC_DVS.1	Identification of security measures
ATE_COV.2	Analysis of coverage
ATE_DPT.1	Testing: high level design
ATE_FUN.1	Functional testing
ATE_IND.2	Independent testing – sample
AVA_MSU.1	Examination of guidance
AVA_SOF.1	Strength of TOE security function evaluation
AVA_VLA.1	Developer vulnerability analysis

Figure 5.3-1 Security Assurance Requirements

5.4 STRENGTH OF SECURITY FUNCTION CLAIM

Strength of function, as a CC concept, applies to probabilities or permutational mechanisms that are non-cryptographic in nature. This ST claims AVA-SOF.1 applicability for the user identification and authentication SFRs: FIA-UID.2 and FIA-UAU.2 through the user password entry function (see ITSF_AUTHENTICATION in Section 6.1) and its mechanisms.

The minimum strength of function level for the password entry mechanism is SOF-Basic.

6 TOE SUMMARY SPECIFICATION

6.1 STATEMENT OF SECURITY FUNCTIONS

The TOE IT Security Functions are listed as follows:

ITSF_AUDIT	The TOE performs audit functions by recording each instance where data is stored, deleted, or modified. It also records the user performing the action and the time of the action. Audit events are determined by the user with privileges of read, write or modify.
ITSF_DAC	Restricts user access to system data and functions by controlling user privileges (e.g., read, write, and modify). Each user is required to enter a User Identification Code (UIC) and password prior to executing any function. The TOE controls access of an identified and authenticated user to those user data objects whose attribute is identical to that of the currently authenticated user. If a terminal is inadvertently left unattended, the TOE provides security features such as a terminal time out, terminal lock, and authentication to prevent unauthorized access to the application functions and sensitive patient data. The TOE also enforces the roles *Clinical System Administrator* and *User* and associates the users with those roles.
ITSF_AUTHENTICATION	The TOE grants system access only after positive identification of system users.
ITSF_SECURITY_MANAGEMENT	The TOE ensures individual accountability by associating each recorded event to a specific user based upon a unique User Identification Code (UIC) assigned to the user account by the system at a specific time.

Figure 6.1-1 TOE IT Security Functions

6.1.1 Audit (ITSF_AUDIT)

The Audit function is designed to track and store all activities performed on the Essentris System. This audit function includes the UserID, username, action performed and timestamp.

Essentris ensures individual accountability by associating each recorded event to a specific user based upon a unique staff identification code assigned to the user account by the system. After entering their UIC and password in order to gain system access, users must again enter their UIC and password in order to complete most transactions, such as, storing, modifying or deleting data. It also provides protection against a user later denying that some functions occurred.

The Audit Log Viewer allows CSAs to monitor user activity. It displays if users were granted access to an application or if permission is denied. It also displays the number of incorrect password attempts. The Audit Log Viewer can query by user name all the activity of a specific user.

6.1.2 Discretionary Access Control (ITSF_DAC)

The Essentris Access Control Policy restricts user access to system data and functions based upon the user's duties and responsibilities for providing patient care. Essentris applications enforce access control by controlling user privileges (e.g., read, write, and modify). This restricts access to both sensitive patient data and application functions. Users must enter their assigned UIC and password to access the system and perform certain functions (i.e., store data, order approval, order entry, etc.) associated with an application. Users are denied access to a screen menu if they do not have the appropriate permissions. By limiting access to an application, the user is also denied access to the sensitive patient data stored by the system.

In addition, Essentris limits access to the data or functions that can be performed from an individual terminal. Essentris can restrict access from a terminal to clinical units, subject to override within an individual user's permissions. This safeguard restricts users in one unit from obtaining information about a patient in another unit. In conjunction with user access controls, this is an effective tool to deter system users from performing unauthorized activities.

If a terminal is inadvertently left unattended, the TOE provides security features such as a terminal time out, terminal lock, and authentication to prevent unauthorized access to the application functions and sensitive patient data. Within Essentris, access permissions are defined through the Staff Configuration Tool (SCT) and Terminal Configuration Tool (TCT). Access to the SCT and TCT tools is restricted to the CSA or individuals with equivalent permissions.

Sensitive patient data in Essentris is duplicated across several servers. Unintentional destruction of data on one server would not affect the data residing on the other server. CCI maintains a strict policy on accessing sensitive patient data stored on the Medical Treatment Facility Essentris servers. CCI personnel with *root* permissions are limited, to the maximum extent required, to provide continued support. Essentris can utilize redundant hosts containing identical databases and configuration files.

6.1.3 Authentication (ITSF_AUTHENTICATION)

Authentication ensures that individual accountability can be established and maintained for users, and that access control decisions can be made based on user security attributes. Authentication prevents unauthorized system access by requiring that users positively identify themselves prior to being granted system access. The Identification and Authentication (I&A) safeguard also assigns a unique identifier to each user that will enforce accountability of all user actions.

Essentris users must enter a unique UIC and password to access the system and perform application functions. The UIC and password are assigned to users when their account is established.

CCI recommends that all MTFs request and allow CCI to implement the following password procedure on their Essentris installation:

a) Passwords will contain a minimum of eight characters .
b) The password will not be a word found in any dictionary (English or foreign).
c) The password will not be a common usage word such as:
   i) Names of family, pets, friends, co-workers, fantasy characters, etc.
   ii) Computer terms and names, commands, sites, companies, hardware, software.
   iii) Birthdays and other personal information such as addresses and phone numbers.
   iv) Word or number patterns like "aaabbb", "qwerty", "123321", etc.
d) Passwords must have the following characteristics:
   i) Contain both upper and lower case characters (e.g., a-z, A-Z)
   ii) Contain at least one numeral (e.g., 0-9)
   iii) Contain at least one special character (e.g., `~!@#$%^&()_+=\[]{};':",./<>?)*
e) Passwords will never be written down or stored on-line.

In CC mode, Essentris is configured to lockout accounts after five (5) sequential failed login attempts on that account.

The overall strength of function of the TOE IT security functions is SOF basic. Only the USER_LOGIN function is realized by a probabilistic mechanism and the strength of this function is SOF basic on the assumption that the users will choose passwords of sufficient length and complexity to be consistent with this claim.

6.1.4 Security Management (ITSF_SECURITY MANAGEMENT)

The security management objective is to provide separate security-relevant system management functions from non-security-relevant functions.

Security safeguards managed by the Essentris application include user identification and authentication, terminal access restrictions, user access restrictions based on assigned permissions, and auditing of user transactions. Essentris system security safeguards are configured and managed through the Essentris SCT and TCT modules. Access to the SCT and TCT modules is restricted to the MTF CSA. The CSA is responsible for establishing user accounts, granting user permissions based on their need-to-know, and controlling the system security configuration.

6.1.5 Statement of Assurance Measures

The assurance measures that are provided by the TOE are described below:

AM_ACM_CAP.3	The CM system ensures the integrity of the TOE from the early design stages through all subsequent maintenance efforts.
AM_ACM_SCP.1	Indicates the TOE items that need to be controlled by the configuration management system.
AM_ADO_DEL.1	The TOE ensures that secure delivery of the TOE is achieved.
AM_ADO_IGS.1	Installation procedures are adequate to ensure that the user starts the TOE with a secure configuration.
AM_ADV_FSP.1	An informal functional specification is supplied for the TOE.
AM_ADV_HLD.2	Identifies the basic structure of the TSF and the major hardware, firmware, and software elements.
AM_ADV_RCR.1	A representational correspondence is supplied to connect the TOE summary specification to the informal functional specification of TSFs is provided; to connect the informal functional specification to the high level design; and to connect the Informal Functional specification to the High Level Design.
AM_AGD_ADM.1	The administrator’s guide is adequate to provide administrators with the required knowledge to securely configure and maintain the TOE within the environment.
AM_AGD_USR.1	The user guidance is adequate to provide the user with the required knowledge to correctly perform login procedures and to provide security awareness of the TOE and its policies.
AM_ALC_DVS.1	Identification of security measures in the life cycle documentation is provided.
AM_ATE_COV.2	The completeness of the functional tests performed by the developer on the TOE.
AM_ATE_DPT.1	Testing with respect to the High Level Design is provided.
AM_ATE_FUN.1	Functional testing of all security functions is provided in the *Essentris Tests and Analysis Overview*, which will be provided as part of the evidence.

AM_ATE_IND.2	Independent testing specifies the degree to which the functional testing of the TOE must be performed by a party other than the developer (e.g. a third party).
AM_AVA_MSU.1	Investigates whether an administrator or user, with an understanding of the guidance documentation, would reasonably be able to determine if the TOE is configured and operating in a manner that is insecure.
AM_AVA_SOF.1	The TOE Strength of Function Analysis addresses the requirements of AVA_SOF.1.
AM_AVA_VLA.1	Identification of flaws potentially introduced in the different refinement steps of the development.

7 PROTECTION PROFILE CLAIMS

There are no Protection Profile claims made for the TOE.

8 RATIONALE

8.1 SECURITY OBJECTIVES RATIONALE AND TRACABILITY

This section shows that the security objectives of the TOE are appropriate to the problems defined in the Security Environment section (Section 3). This is done through a series of tables and matrices that reference threats, security policies and assumptions, each addressed by one or more security objectives. An informal proposition follows to show for each threat, assumption or policy, why each security objective provides an effective countermeasure to prevent an attack or mitigate risk.

8.1.1 Security Mapping Objectives

Security Objectives Assumption	O.ADMIN	O.AVAILABILITY	O.CONNECT	O.INTERNAL_CHANNEL
A.ADMIN	**X**			
A.AVAIL		**X**		
A.CONNECT				**X**
A.INTERNAL_CHANNEL			**X**	**X**
A.LOCATE		**X**		
A.NOEVIL	**X**			

Figure 8.1-1 Mapping for Each of the Security Objectives

Assumption	Security Objective	Rationale
A.ADMIN	**O.ADMIN**	O.ADMIN ensures Administrators are trained and trusted to perform their System Administration Functions.
A.AVAIL	**O.AVAILABILITY**	O.AVAILABILTY addresses A.AVAIL by ensuring the system is available and fully redundant.
A.CONNECT	**O.INTERNAL_CHANNEL**	O.INTERNAL_CHANNEL addresses A.CONNECT by ensuring that all LAN connections between the TOE Server and Client platforms are physically isolated from external communications channels.
A.INTERNAL_CHANNEL	**O.CONNECT** **O.INTERNAL_CHANNEL**	O.CONNECT provides for A.INTERNAL CHANNEL by ensuring that all internal and external connections reside within controlled access facilities. O.INTERNAL_CHANNEL addresses A.INTERNAL_CHANNEL by ensuring that the LAN connectivity services between the TOE Server and Client platforms are physically isolated from external communication channels, provide assured identification of their end points and protect the channel data from modification.
A.LOCATE	**O.CONNECT**	O.CONNECT addresses A.LOCATE by ensuring the system is housed in a secure access facility.
A.NOEVIL	**O.ADMIN**	O.ADMIN addresses A.NOEVIL by ensuring that all administrators of the system are non - threatening and trusted.

Figure 8.1-2 Assumptions against Objectives

8.1.2 TOE Security Objectives rationale for threats

Security Objectives Threats	O.AUDITING	O.AUTHENTICATION	O.CONFIDENTIALITY	O.DISCRETIONARY_ACCESS	O.INTEGRITY	O.NON_REPUDIATION
T.ACCESS			X	X		
T.DISCLOSE			X			
T.MODIFY	X			X	X	X
T.RESOURCE		X		X		

Threat	Security Objective	Rationale
T.ACCESS	O.CONFIDENTIALITY O.DISCRETIONARY_ACCESS	O.CONFIDENTIALITY and O.DISCRETIONARY_ACCESS prevent the possibility of T.ACCESS by enforcing only authorized users to interrupt system services within the TOE.
T.DISCLOSE	O.CONFIDENTIALITY	O.CONFIDENTIALITY ensures that T.DISCLOSE will not occur by forcing only authorized users access to sensitive data.
T.MODIFY	O.AUDITING O.DISCRETIONARY_ACCESS O.INTEGRITY O.NON-REPUDIATION	O.DISCRETIONARY_ACCESS prevents T.MODIFY by ensuring all users have appropriate access rights before allowing modification to the system. O.AUDITING and O.NON_REPUDIATION ensures that any changes are recorded, identifying what user made the change. O.INTEGRITY ensures that data is not changed in an unauthorized or unrecorded manner.
T.RESOURCE	O.AUTHENTICATION O.DISCRETIONARY_ACCESS	O.DISCRETIONARY_ACCESS and O.AUTHENTICATION prevent the possibility of T.RESOURCE by ensuring that system resources are unavailable to unauthorized users and authorized users, for personal use.

Figure 8.1-3 Objectives against threats

Security Objectives Policies	O.AUDITING	O.DISCRETIONARY_ACCESS	O.ENFORCEMENT	O.ACCOUNTABILITY
P.ACCOUNTABILITY	X		X	X
P.DISCRETIONARY-ACCESS		X	X	
P.NEED_TO_KNOW		X	X	

Organizational Policy	Security Objectives	Rationale
P.ACCOUNTABILITY	**O.AUDITING** **O.ENFORCEMENT** **O.ACCOUNTABILITY**	P.ACCOUNTABILTY states the users of the system shall be held accountable for their actions within the system. The policy is implemented by O.AUDITING by recording actions in an audit trail. O.ENFORCEMENT ensures these functions are always invoked and operational. O.ACCOUNTABILTY provides for the ability to track user actions to enforce the security policy.
P.DISCRETIONARY-ACCESS	**O.DISCRETIONARY_ACCESS** **O.ENFORCEMENT**	P.DISCRETIONARY_ACCESS states only those users who have been authorized to access the information within the system may access the system and; O.DISCRETIONARY_ACCESS ensures that all users are authenticated prior to accessing any functions of the TOE. O.ENFORCEMENT ensures that these functions are invoked when necessary.
P.NEED_TO_KNOW	**O.ENFORCEMENT** **O.DISCRETIONARY_ACCESS**	P.NEED_TO_KNOW states the system must limit the access to modification and destruction of the information in protected resources to those authorized users which have a “need to know” for that information. O.DISCRETIONARY_ACCESS ensures that all users are authenticated based on assigned access roles to the TOE. O.ENFORCMENT ensures these functions are always operational.

Figure 8.1-4 Objectives against policies

8.2 SECURITY FUNCTIONAL REQUIREMENTS RATIONALE

This section provides evidence that demonstrates that the security objectives for the TOE and the IT environment are satisfied by the security requirements.

These mappings demonstrate that all TOE security requirements can be traced back to one or more TOE security objective(s), and all TOE security objectives are supported by at least one security requirement.

Together the set of Security requirements for both the TOE and the IT environment form a mutually supportive whole to counteract the level of known threats in the systems environment where the TOE will be installed. These security requirements together ensure the operation of the TOE in the manner to which it was designed in the environment it was designed for.

Security Functional Requirement	O.ACCOUNTABILITY	O.AUDITING	O.AUTHENTICATION	O.CONFIDENTIALITY	O.DISCRETIONARY_ACCESS	O.ENFORCEMENT	O.INTEGRITY	O.NON-REPUDIATION
FAU_GEN.1	**X**	**X**						**X**
FAU_GEN.2	**X**	**X**	**X**	**X**				**X**
FAU_SAR.1	**X**	**X**						
FAU_SAR.2	**X**	**X**						
FAU_SAR.3	**X**	**X**						
FAU_STG.1	**X**	**X**						
FDP_ACC.1					**X**			
FDP_ACF.1				**X**	**X**		**X**	
FIA_ATD.1					X			
FIA_UAU.2			**X**			**X**		
FIA_UAU.7			**X**	**X**		**X**		
FIA_UID.2				**X**	**X**		**X**	
FIA_USB.1				**X**	**X**			

Security Functional Requirement	O.ACCOUNTABILITY	O.AUDITING	O.AUTHENTICATION	O.CONFIDENTIALITY	O.DISCRETIONARY_ACCESS	O.ENFORCEMENT	O.INTEGRITY	O.NON-REPUDIATION
FMT_MTD.1					X			
FMT_MSA.1					X			
FMT_MSA.3				X	X			
FMT_SMF.1					X			
FMT_SMR.1				X	X	X		
FPT_RVM.1				X		X		
FPT_SEP.1						X		
FPT_STM.1		X						X

Figure 8.2-1 Security Functional Requirements Rationale

The rationale for the SFRs against the security objectives of the TOE and its IT environment is given in the table below. Each Objective maps to at least one SFR and a statement follows describing why each objective is met by the specified security functional requirement(s).

Security Objective	SFR	Rationale
O.ACCOUNTABILITY	**FAU_GEN.1** **FAU_GEN.2** **FAU_SAR.1** **FAU_SAR.2** **FAU_SAR.3** **FAU_STG.1**	FAU_GEN.1 and FAU_GEN.2 provide that audit records will be generated for selected events and the TSF shall be able to associate each event with the identity of the user that caused the event. FAU_SAR.1 provides that the TSF shall provide authorized administrators with the capability to read all audit information from the audit records and that the audit records will be presented in a manner suitable for the user to interpret the information. FAU_SAR.2 provides that he TSF will restrict users from having read access to the audit records, except those users that have been granted explicit read access. FAU_SAR.3 provides that the TSF shall provide

Security Objective	SFR	Rationale
		the ability to perform searches of specified types on the audit records. FAU_STG.1 provides that the TSF shall protect the stored audit records from unauthorized deletion and to prevent modification to the other records. Thus the integrity of audit records is assured.
O.AUDITING	**FAU_GEN.1** **FAU_GEN.2** **FAU_SAR.1** **FAU_SAR.2** **FAU_SAR.3** **FAU_STG.1** **FPT_STM.1**	FAU_GEN.1 and FAU_GEN.2 provide that audit records will be generated for selected events and the TSF shall be able to associate each event with the identity of the user that caused the event. FAU_SAR.1 provides that the TSF shall provide authorized administrators with the capability to read all audit information from the audit records and that the audit records will be presented in a manner suitable for the user to interpret the information. FAU_SAR.2 provides that he TSF will restrict users from having read access to the audit records, except those users that have been granted explicit read access. FAU_SAR.3 provides that the TSF shall provide the ability to perform searches of specified types on the audit records. FAU_STG.1 provides that the TSF shall protect the stored audit records from unauthorized deletion and to prevent modification to the other records. Thus the integrity of audit records is assured. FPT_STM.1 provides that the TSF will be able to provide reliable time stamp to show when auditable events occurred.
O.AUTHENTICATION	**FAU_GEN.2** **FIA_UAU.2** **FIA_UAU.7**	FAU_GEN.2 provides that audit records will be generated for selected events and the TSF shall be able to associate each event with the identity of the user that caused the event. FIA_UAU.2 provides that The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user. FIA_UAU.7 ensures that the TSF shall provide only *the* authentication *screen* to the user while the authentication is in progress.
O.CONFIDENTIALITY	**FAU_GEN.2** **FDP_ACF.1** **FIA_UAU.7** **FIA_UID.2** **FIA_USB.1** **FMT_MSA.3** **FMT_SMR.1** **FPT_RVM.1**	FAU_GEN.2 provides that audit records will be generated for selected events and the TSF shall be able to associate each event with the identity of the user that caused the event. FDP_ACF.1 provides that the TSF shall enforce the Essentris Access Control to objects based on: Subject attributes: UserID, Password, and Roles. The TSF shall enforce the Read, Write, Modify, and None rules to determine if an operation among controlled subjects and controlled objects is allowed. Furthermore, the TSF shall explicitly deny

Security Objective	SFR	Rationale
		access of subjects to objects based on the Read, Write, Modify, and None attributes that explicitly deny access of subjects to objects. FIA_UAU.7 ensures that the TSF shall provide only the authentication screen to the user while the authentication is in progress. FAU_UID.2 ensures that the TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user. FIA_USB.1 The TSF shall associate the appropriate user security attributes with subjects acting on behalf of that user: *The UserID* and *Password is used to enforce the Essentris Access Control Policy* *The user role which is used to enforce the Essentris Access Control Policy* is the CSA *The appropriate other user security attributes* are *Read, Write, Modify,* and *None.* Further, the TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: *Read, Write, Modify,* and *None.* FMT_MSA.3 provides that the TSF shall enforce the *Essentris Access Control,* to provide *permissive* default values for security attributes that are used to enforce the *SFP*. The TSF shall also allow the *CSA* to specify alternative initial values to override the default values when an object or information is created. FMT_SMR.1 provides that the TSF shall maintain the roles *Clinical System Administrator and User* and that the TSF shall be able to associate users with roles. FPT_RVM.1 provides that the TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.
O.DISCRETIONARY_ACCESS	**FDP_ACC.1** **FDP_ACF.1** **FIA_ATD.1** **FIA_UID.2** **FIA_USB.1** **FMT_MTD.1** **FMT_MSA.1** **FMT_MSA.3** **FMT_SMF.1** **FMT_SMR.1**	FDP_ACC.1 provides that the TSF shall enforce the *Essentris Access Control* on Objects*:* All objects created, stored, handled and destroyed in the device *Operations*: *Read, Write, Modify,* and *None.* FDP_ACF.1 provides that the TSF shall enforce the Essentris Access Control to objects based on: Subject attributes: UserID, Password, and Roles. FIA_ATD.1.1 provides that the TSF shall maintain the following list of security attributes belonging to individual users: *Read, Write, Modify,* and *None*. FIA_UID.2 ensures that the TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Security Objective	SFR	Rationale
		FIA_USB.1 The TSF shall associate the appropriate user security attributes with subjects acting on behalf of that user: *The UserID* and *Password is used to enforce the Essentris Access Control Policy.* *The user role which is used to enforce the Essentris Access Control Policy is the CSA The appropriate following other user security attributes are Read, Write, Modify, and None.* Further, the TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: *Read, Write, Modify,* and *None.* FMT_MSA.1 provides that the TSF shall enforce the *Essentris Access Control,* to restrict the ability to: *change_default, modify,* and *delete,* the security attributes *Read, Write, Modify,* and *None* to *the CSA*. FMT_MSA.3 provides that the TSF shall enforce the *Essentris Access Control,* to provide *permissive* default values for security attributes that are used to enforce the *SFP*. The TSF shall also allow the *CSA* to specify alternative initial values to override the default values when an object or information is created. FMT_SMF.1 provides that the TSF shall be capable of performing the following security management functions: *Data protection attributes, TOE Protection Attributes, audit attributes, and identification and authentication attributes.* FMT_SMR.1 provides that the TSF shall maintain the roles *Clinical System Administrator and User* and that the TSF shall be able to associate users with roles.
O.ENFORCEMENT	**FIA_UAU.2** **FIA_UAU.7** **FMT_SMR.1** **FPT_RVM.1** **FPT_SEP.1**	FIA_UAU.2 provides that The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user. FIA_UAU.7 ensures that the TSF shall provide only the authentication screen to the user while the authentication is in progress. FMT_SMR.1 provides that the TSF shall maintain the roles *Clinical System Administrator and User* and that the TSF shall be able to associate users with roles. FPT_RVM.1 provides that the TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed. FPT_SEP.1 provides that the TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects and that the TSF shall enforce separation

Security Objective	SFR	Rationale
		between the security domains of subjects in the TSC.
O.INTEGRITY	**FDP_ACF.1** **FIA_UID.2**	FDP_ACF.1 provides that the TSF shall enforce the Essentris Access Control to objects based on: Subject attributes: UserID, Password, and Roles. FAU_UID.2 ensures that the TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.
O.NON-REPUDIATION	**FAU_GEN.1** **FAU_GEN.2** **FPT_STM.1**	FAU_GEN.1 and FAU_GEN.2 provide that audit records will be generated for selected events and the TSF shall be able to associate each event with the identity of the user that caused the event. FPT_STM.1 provides that the TSF will be able to provide a reliable time stamp to show when auditable events occurred.

8.3 ASSURANCE LEVEL RATIONALE

Given the statement of Security environment and security objectives contained in this ST, an assurance level of EAL3 is appropriate for the basic level of protection provided by the TOE and its physical architecture. For IT Security Environments that address the issues raised in the environmental assumptions, the TOE provides secure discretionary access control and audit services.

8.4 SFR DEPENDENCY RATIONALE

The following table shows the dependency analysis of the claimed SFR for the TOE.

The SFRs are listed in the rows with each related dependency listed in the corresponding columns.

SFR Dependency Matrix	FPT_STM.1	FAU_GEN.1	FIA_UID.1	FAU_SAR.1	FDP_ACF.1	FDP_ACC.1	FMT_MSA.1	FMT_MSA.3	FIA_UAU.1	FIA_ATD.1	FMT_SMR.1	FMT_SMF.1
FAU_GEN.1	X											
FAU_GEN.2		X	X									
FAU_SAR.1		X										
FAU_SAR.2				X								
FAU_SAR.3				X								
FAU_STG.1		X										
FDP_ACC.1					X							
FDP_ACF.1						X		X				
FIA_UAU.2			X									
FIA_UAU.7									X			
FIA_USB.1										X		
FMT_SMR.1			X									
FMT_MSA.1						X					X	X
FMT_MSA.3							X					
FMT_MTD.1											X	X
FMT_SMF.1							X				X	

Figure 8.4-1 SFR Dependency Table

8.4.1 Unsupported dependencies

No unsupported dependencies.

8.5 TOE SUMMARY SPECIFICATION RATIONALE

8.5.1 IT Security Functions Rationale

The mapping between the IT security functions and the SFRs is shown in the table below. Each SFR maps to at least one ITSF.

	ITSF_AUDIT	ITSF_DAC	ITSF_AUTHENTICATION	ITSF_SECURITY MANAGEMENT
FAU_GEN.1	X			
FAU_GEN.2	X			
FAU_SAR.1	X			
FAU_SAR.2	X			
FAU_SAR.3	X			
FAU_STG.1	X			
FDP_ACC.1		X		
FDP_ACF.1		X		
FIA_ATD.1		X	X	
FIA_UAU.2		X	X	
FIA_UAU.7		X	X	
FIA_UID.2		X	X	
FIA_USB.1			X	
FMT_MTD.1		X		X
FMT_MSA.1		X		X
FMT_MSA.3		X		X
FMT_SMF.1			X	X
FMT_SMR.1		X		X

Figure 8.5-1 IT Security Functions

8.5.2 IT to SFR Rationale

The detailed mapping of the TSF to the Security Functional Requirements is below. The TOE IT Security Functions are referenced to the list of SFRs. An explanation describing how the ITSFs cover each SFR is included.

Security Functional Requirement	IT Security Function	IT to SFR Rationale
FAU_GEN.1	**ITSF_AUDIT**	ITSF_AUDIT creates audit records satisfying the FAU-GEN.1 requirements for auditable events.
FAU_GEN.2	**ITSF_AUDIT**	ITSF_AUDIT creates audit records satisfying the FAU-GEN.2 requirements for association of auditable events with user name.
FAU_SAR.1	**ITSF_AUDIT**	ITSF_AUDIT creates audit records satisfying the FAU_SAR.1 requirements for auditable events.
FAU_SAR.2	**ITSF_AUDIT**	ITSF_AUDIT prohibits all users except trusted administrators from read access to the audit trail.
FAU_SAR.3	**ITSF_AUDIT**	ITSF_AUDIT provides the ability to search for audit events satisfying specified span of time, UserID and user name.
FAU_STG.1	**ITSF_AUDIT**	ITSF_AUDIT protects audit records from deletion or modification.
FDP_ACC.1	**ITSF_DAC**	ITSF_DAC provides the TOE DAC policy on all objects created, stored and handled by TOE.
FDP_ACF.1	**ITSF_DAC**	ITSF_DAC provides the TOE DAC policy on all objects created, stored and handled by TOE based on User ID, Password, and Role.
FIA_ATD.1	**ITSF_DAC** **ITSF_AUTHENTICATION**	ITSF_DAC maintains the required user attributes required to mediate al DAC policies. ITSF_AUTHENTICATION provides a binding between a user name and security attributes.
FIA_UAU.2	**ITSF_DAC** **ITSF_AUTHENTICATION**	ITSF_DAC does not permit user actions other than user authentication to be performed prior to user authentication. ITSF_AUTHENTICATION provides a binding between a user name and security attributes.
FIA_UAU.7	**ITSF_DAC** **ITSF_AUTHENTICATION**	ITSF_DAC does not provide feedback to the user while authentication is in progress. ITSF_AUTHENTICATION provides a binding between a user name and security attributes.
FIA_UID.2	**ITSF_DAC** **ITSF_AUTHENTICATION**	ITSF_DAC requires each user to be identified before allowing any other action. ITSF_AUTHENTICATION provides a binding between a user name and security attributes. .

Security Functional Requirement	IT Security Function	IT to SFR Rationale
FIA_USB.1	**ITSF_AUTHENTICATION**	ITSF_AUTHENTICATION provides a binding between a user name and security attributes.
FMT MSA.1	**ITSF_DAC** **ITSF_SECURITY MANAGEMENT**	ITSF_DAC restricts the ability to modify the security attributes associated with a named object to the administrator. ITSF_SECURITY MANAGEMENT ensures that security related attributes can only be changed by the CSA.
FMT MSA.3	**ITSF_DAC** **ITSF_SECURITY MANAGEMENT**	ITSF_DAC restricts the ability to enter invalid security attributes. ITSF_SECURITY MANAGEMENT ensures that only the CSA can enter valid security attributes.
FMT_MTD.1	**ITSF_DAC** **ITSF_SECURITY MANAGEMENT**	ITSF_DAC restricts the ability to modify the user security attributes, other than authentication data to authorized administrators. ITSF_SECURITY MANAGEMENT ensures that only the CSA can manage TSF data.
FMT_SMF.1	**ITSF_AUTHENTICATION** **ITSF_SECURITY MANAGEMENT**	ITSF_AUTHENTICATION allows authorized administrators to perform security management functions. ITSF_SECURITY MANAGEMENT ensures that only the CSA can perform security management functions.
FMT_SMR.1	**ITSF_DAC** **ITSF_SECURITY MANAGEMENT**	ITSF_DAC enforces the security role types of CSA and User. . ITSF_SECURITY MANAGEMENT ensures that the security role types for the CSA and User are managed..

Figure 8.5-2 IT Security Functions Table

8.6 FUNCTIONAL CLAIMS RATIONALE

The selected functionality for this ST is consistent with and appropriate for the security objectives for the TOE. There are 4 major security functions the TOE performs. Each of the below listed security services represent the overall security objectives of the TOE and its IT environment.

- **Discretionary Access Control**
- **Authentication**
- **Audit**
- **Security Management**

These objectives form a cohesive set of security requirements of the TOE and its IT environment. The group is consistent with the level of capability and motivation any given threat agent is likely to possess. Given the sensitive nature of the data stored in the TOE, the group is sufficient to support the overall security objectives of the TOE.

8.6.1 TOE SOF Claims

The overall TOE SOF claim is SOF-basic because this SOF is sufficient to resist the threats identified in Section 3.1. Section 8.1 provides evidence that demonstrates that TOE threats are countered by the TOE security objectives. Section 8.2 demonstrates that the security objectives for the TOE and the TOE environment are satisfied by the security requirements. The SOF-basic claim for the TOE applies because the TOE protects against an unskilled attacker with no special tools from accessing the TOE. The claim of SOF-basic ensures that Essentris is resistant to a low attack potential because the systems containing critical patient data and information is located in a secure, locked facility and cannot be accessed by users without physical access to the healthcare facility without sophisticated hacking tools and prior authentication. Furthermore, the claim SOF-basic ensures that an unskilled attacker cannot access the internal healthcare facility network from a phone line or outside computer.

8.6.2 ASSURANCE MEASURES RATIONALE

Assurance Components	Description	Assurance Measures	Compliance
ACM_CAP.3	Authorisation controls	AM_ACM_CAP.3	TOE releases are adequately identified with the version number. All Configuration Items that comprise the TOE are under Configuration Management and are included on a Configuration List. The CM system (described in the CM plan) shall provide measures such that only authorized changes are made to the configuration items.

Assurance Components	Description	Assurance Measures	Compliance
ACM_SCP.1	TOE CM coverage	AM_ACM_SCP.1	The coverage of the configuration management system includes implementation representation; and the evaluation evidence required by the assurance components in the ST.
ADO_DEL.1	Delivery procedures	AM_ADO_DEL.1	The TOE documented delivery procedures ensure that secure delivery of the TOE to the user's site is achieved.
ADO_IGS.1	Installation, generation, and start-up procedures	AM_ADO_IGS.1	Automated installation procedures are adequate to ensure that the user starts the TOE with a secure configuration.
ADV_FSP.1	Informal functional specification	AM_ADV_FSP.1	An informal functional specification is supplied that completely represents the TSF and describes its external interfaces using an informal style.
ADV_HLD.2	Security enforcing high-level design	AM_ADV_HLD.2	High-level design documentation supplied describes, in an informal manner, the TSF design, its subsystems and interfaces, and the security functionality provided by the subsystem.
ADV_RCR.1	Informal correspondence demonstration	AM_ADV_RCR.1	A representational correspondence is supplied to connect the TOE summary specification to the informal functional specification of TSFs is provided; to connect the informal functional specification to the high level design.
AGD_ADM.1	Administrative guidance	AM_AGD_ADM.1	The administrator's guide is adequate to provide administrators with the required knowledge to securely configure and maintain the TOE within the environment.
AGD_USR.1	User guidance	AM_AGD_USR.1	The user guidance is adequate to provide the user with the required knowledge to operate in a secure manner and describes all security information relevant to the user.
ALC_DVS.1	Identification of security measures	AM_ALC_DVS.1	The development environment is a secure facility. The security documentation describes physical, procedural, personnel and other security measures that protect the integrity and confidentiality of the design, maintenance and implementation of the TOE in its development environment.

Assurance Components	Description	Assurance Measures	Compliance
ATE_COV.2	Analysis of coverage	AM_ATE_COV.2	The analysis of test coverage provided demonstrates that the correspondence between the TSF as described in the functional specification and the tests identified in the test documentation is complete.
ATE_DPT.1	Testing; high level design	AM_ATE_DPT.1	The depth of functional testing is analyzed and it is demonstrated that the TSF operates in accordance with its high-level design.
ATE_FUN.1	Functional testing	AM_ATE_FUN.1	Functional testing of all security functions is provided in the *Essentris Tests and Analysis Overview*, which will be provided as part of the evidence.
ATE_IND.2	Independent testing – sample	AM_ATE_IND.2	A sample of functional testing was performed by an independent third party.
AVA_MSU.1	Examination of guidance	AM_AVA_MSU.1	The guidance documentation identifies all modes of operations, their consequences and implications for maintaining secure operation.
AVA_SOF.1	Strength of TOE security function evaluation	AM_AVA_SOF.1	The TOE Strength of Function Analysis address the requirements of AVA_SOF.1 with the minimum strength level defined in the ST.
AVA_VLA.1	Developer vulnerability analysis	AM_AVA_VLA.1	The TOE vulnerability analysis is performed to ascertain the presence of obvious security vulnerabilities, and to confirm that they cannot be exploited in the intended environment for the TOE.