Alaris® PCU Model 8015 FIPS 140-2 Level 2 Security Policy

Part Number: 12079232

Copyright Carefusion 2011. May be reproduced only in its original entirety [without revision].

CHANGE RECORD

Revision	*Date*	*Author*	*Description of Change*
0.1	21OCT2010	CareFusion	Initial draft
0.2	16NOV2010	CareFusion	Updated per comments and resolved action items.
0.3	26JAN2011	CareFusion	Updated per IGL technical review comments and resolved action items.
0.4	14APR2011	CareFusion	Updated per CMVP comments

Copyright Carefusion 2011. May be reproduced only in its original entirety [without revision].

Table of Contents

Copyright Carefusion 2011. May be reproduced only in its original entirety [without revision].

1. Introduction

1.1. References

[FIPS 140-2] FIPS Publication 140-2 *Security Requirements for Cryptographic Modules*

[FIPS 180-2] FIPS Publication 180-2 *Secure Hash Standard*

[FIPS 197] FIPS Publication 197 *Advanced Encryption Standard*

FIPS Official Web Site: http://www.itl.nist.gov/fipspubs/

1.2. Definitions and Acronyms

Advanced Encryption Standard (AES)	A cryptographic algorithm; a symmetric block cipher that can encrypt (encipher) and decrypt (decipher) information.
Alaris® System Maintenance (ASM)	A PC-based software tool that allows a hospital to perform routine maintenance and data log downloads from the Alaris® PC 8015 and attached expansion devices.
Alaris® System Manager (Server)	A server based tool that communicates with a network of Alaris® devices, providing patient registration and hospital medical information to Alaris® devices, and receiving infusion pumps logs and other data from Alaris® devices. Due to the similarity of the name with the preceding definition and the potential for confusion, this entity will be described including the word "Server" in this document.
CHAP	Challenge Handshake Authentication Protocol (CHAP) is an authentication scheme used by Point to Point Protocol (PPP) servers to validate the identity of remote clients.
Critical security parameter (CSP)	From FIPS 140-2: security-related information (for example, secret and private cryptographic keys, and authentication data such as passwords and PINs) whose disclosure or modification can compromise the security of a cryptographic module.
Cryptographic boundary	From FIPS 140-2: an explicitly defined continuous perimeter that establishes the physical bounds of a cryptographic module and contains all the hardware, software, and/or firmware components of a cryptographic module.
Cryptographic module (CM)	From FIPS 140-2: the set of hardware, software, and/or firmware that implements approved security functions (including cryptographic algorithms and key generation) and is contained within the cryptographic boundary.
Cryptographic officer (CO)	From FIPS 140-2: an operator or process (subject), acting on behalf of the operator, performing cryptographic initialization or management functions.
Cryptographic user (CU)	From FIPS 140-2: an individual or a process (subject) acting on behalf of the individual that accesses a cryptographic module in order to obtain cryptographic services.
FIPS	Federal Information Processing Standards
FIPS Approved	From FIPS 140-2: FIPS-Approved and/or NIST-recommended.
FIPS-Approved mode of operation	From FIPS 140-2: a mode of the cryptographic module that employs only approved security functions
FIPS-Approved security function	From FIPS 140-2: a security function (e.g., cryptographic algorithm, cryptographic key management technique, or authentication technique) that is one of the following: • Specified in an Approved standard • Adopted in an Approved standard and specified either in an appendix of the Approved standard or in a document referenced by the Approved standard • Specified in the list of Approved security functions
Inter-unit interface (IUI) port	Proprietary physical connector for data and power supply connection.
NIST	National Institute of Standards and Technology

Random Number Generator	From FIPS 140-2: Random Number Generators (RNGs) used for cryptographic applications typically produce a sequence of zero and one bits that may be combined into sub-sequences or blocks of random numbers. There are two basic classes: deterministic and nondeterministic. • RNG (RNG) consists of an algorithm that produces a sequence of bits from an initial value called a seed.. • Nondeterministic RNG (NDRNG) produces output that is dependent on some unpredictable physical source that is outside human control.
Secure Hashing Algorithm (SHA)	An algorithm for computing a one-way, condensed representation of electronic data with secure properties.
Tamper evidence	From FIPS 140-2: the external indication that an attempt has been made to compromise the physical security of a cryptographic module. The evidence of the tamper attempt should be observable by an operator subsequent to the attempt.
Zeroization	From FIPS 140-2: a method of erasing electronically stored data, cryptographic keys, and CSPs by altering or deleting the contents of the data storage to prevent recovery of the data.

1.3. Cryptographic Module Overview

The CareFusion Alaris® PCU Model 8015 (hereafter referred to as the cryptographic module or CM) is the central point-of-care unit, which is the main component of the Alaris® System. The Alaris® System is a modular system intended for adult, pediatric, and neonatal care in a professional healthcare environment. The Alaris® System brings a higher level of medication error prevention to the point of patient care. The CM is multi-chip standalone embodiment validated to FIPS 140-2 Level 2.

Figure 1 depicts the CM (outlined in red) in an operational context. The Alaris® Systems Manager (Server) software controls communication and data transfer between the server and other systems and software resident on the network including the Alaris® System, Alaris® Connectivity Gateway, and Guardrails® Continuous Quality Improvement (CQI) database. This browser-based software interface allows the hospital’s Guardrails® data sets to be uploaded to the Alaris® System while providing device data reporting on successful uploads and downloads of CQI log data. The Alaris® Systems Manager (Server) also provides data communication support for the Alaris® Connectivity Gateway by providing interface capability to other hospital systems. The Alaris® Connectivity Gateway can provide subscription services to a broad range of hospital applications, including Pharmacy, MAR, Clinical Information Systems, and other monitoring/patient tracking systems.

The CM cryptographic functions provide:

- Strong authentication of the Alaris® Systems Manager (Server) by the CM
- AES encryption of traffic from the CM to the Alaris® Systems Manager (Server)
- AES decryption of traffic from the Alaris® Systems Manager (Server) to the CM

Copyright Carefusion 2011. May be reproduced only in its original entirety [without revision].

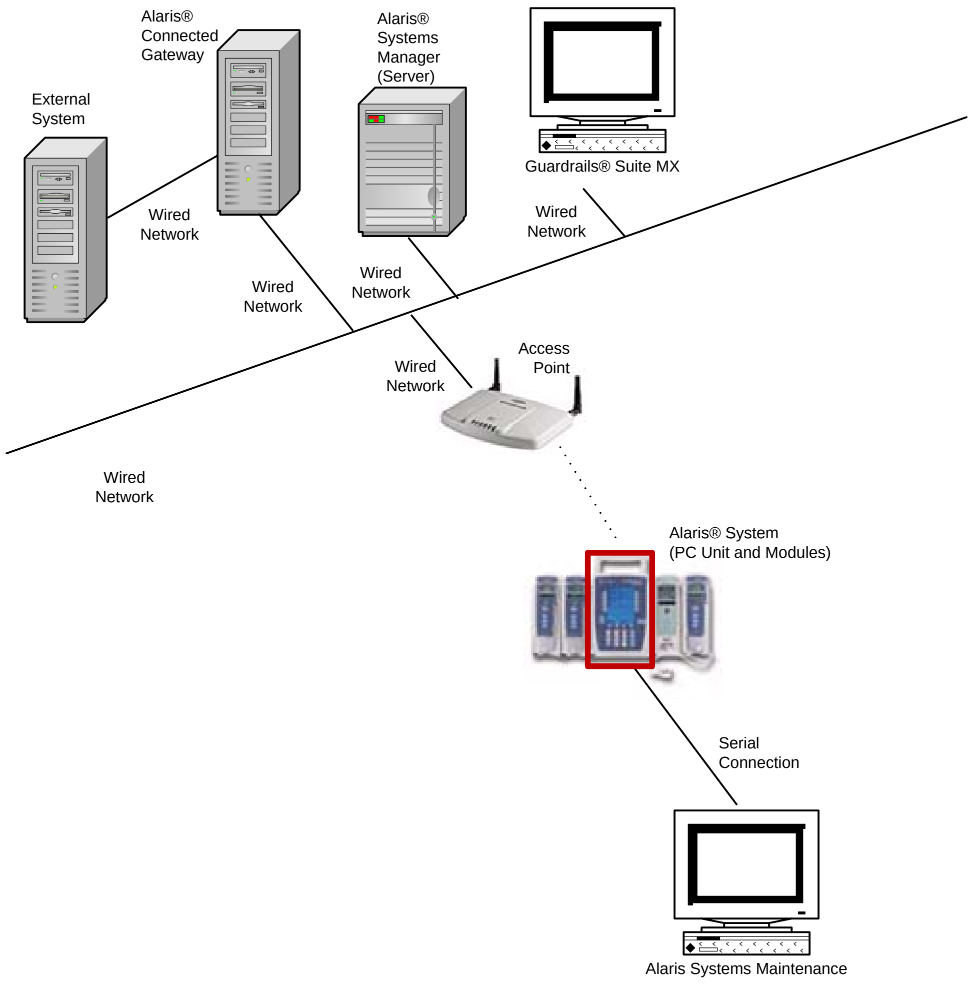


Figure 1 - Operational Context for the PCU 8015

The CM uses an off-the-shelf 802.11 device to communicate with system wireless access points. No FIPS 140-2 security claim is made for 802.11-related functionality.

Traffic is secured by AES encryption and decryption between the CM and the Alaris® Systems Manager (Server) independent of the 802.11 protocol choices made on the intervening wireless access point.

Copyright Carefusion 2011. May be reproduced only in its original entirety [without revision].

Table 1 indicates the levels for each FIPS 140-2 area.

Security Requirements Section	Level
Cryptographic Module Specification	3
Module Ports and Interfaces	2
Roles, Services and Authentication	2
Finite State Model	2
Physical Security	2
Operational Environment	N/A
Cryptographic Key Management	2
EMI/EMC	2
Self-Tests	2
Design Assurance	3
Mitigation of Other Attacks	N/A

Table 1 - FIPS 140-2 Security Levels

The CM implements a non-modifiable operational environment. FIPS 140-2 Area 6 Operational Environment requirements are not applicable.

The CM operates as a radio, in the sense that it implements 802.11 communications. The CM does not implement the APCO OTAR rekeying protocol described in [*FIPS 140-2*].

The CM does not implement mitigation of other attacks outside the scope of *[FIPS 140-2*].

Copyright Carefusion 2011. May be reproduced only in its original entirety [without revision].

The following figure depicts the CM. The CM's cryptographic boundary is the external housing, not including the IUI ports and battery pack.

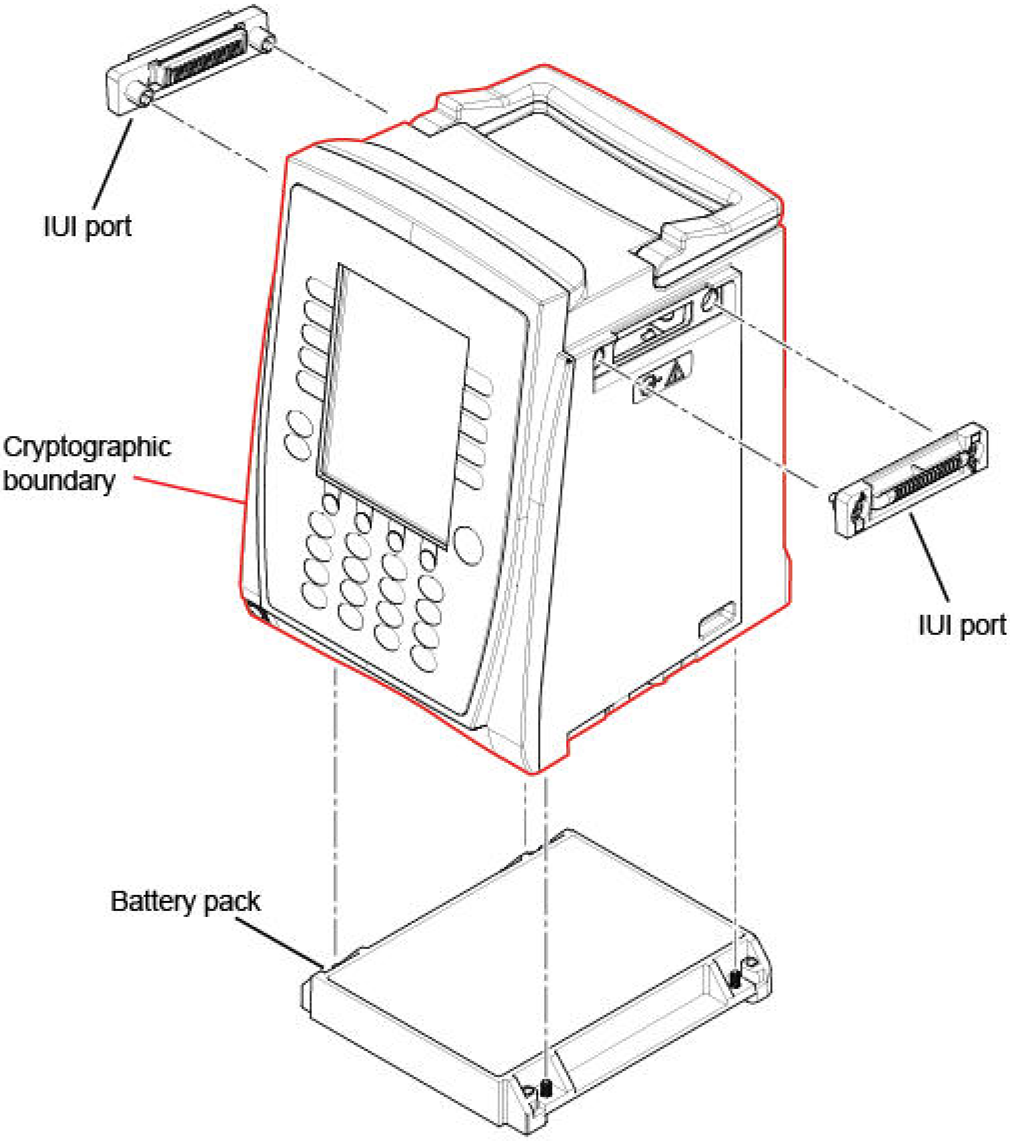


Figure 2 – CM Front and Side View

Copyright Carefusion 2011. May be reproduced only in its original entirety [without revision].

The following figure depicts a rear view of the CM.

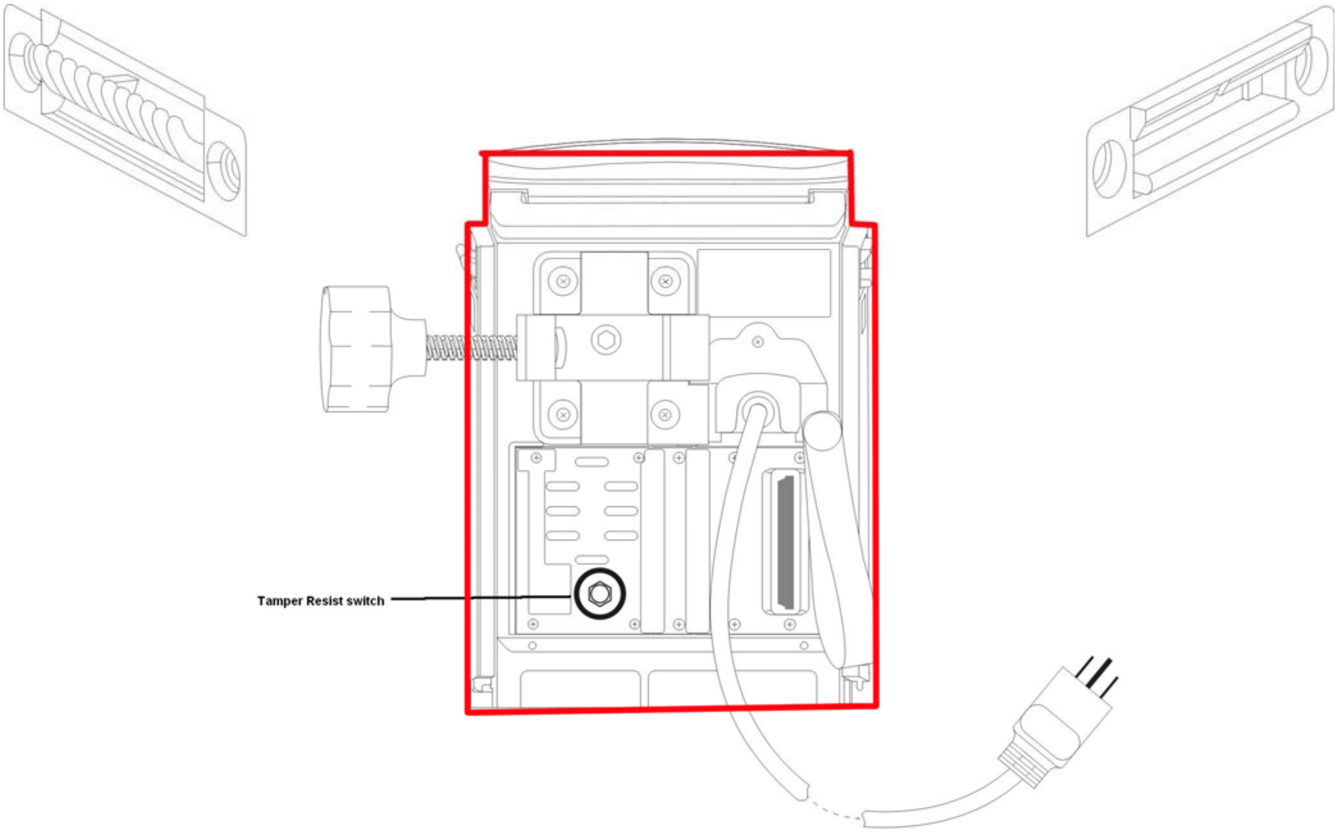


Figure 3 - CM Rear View

The Tamper Resist Switch is designed as a clinical feature and does not refer to FIPS 140-2 physical security requirements. This Tamper Resist Switch is used to inhibit a non-clinical person from making clinical changes to a programmed infusion.

Copyright Carefusion 2011. May be reproduced only in its original entirety [without revision].

The CM’s cryptographic boundary is indicated by the solid red line in the logical diagram in Figure 4.

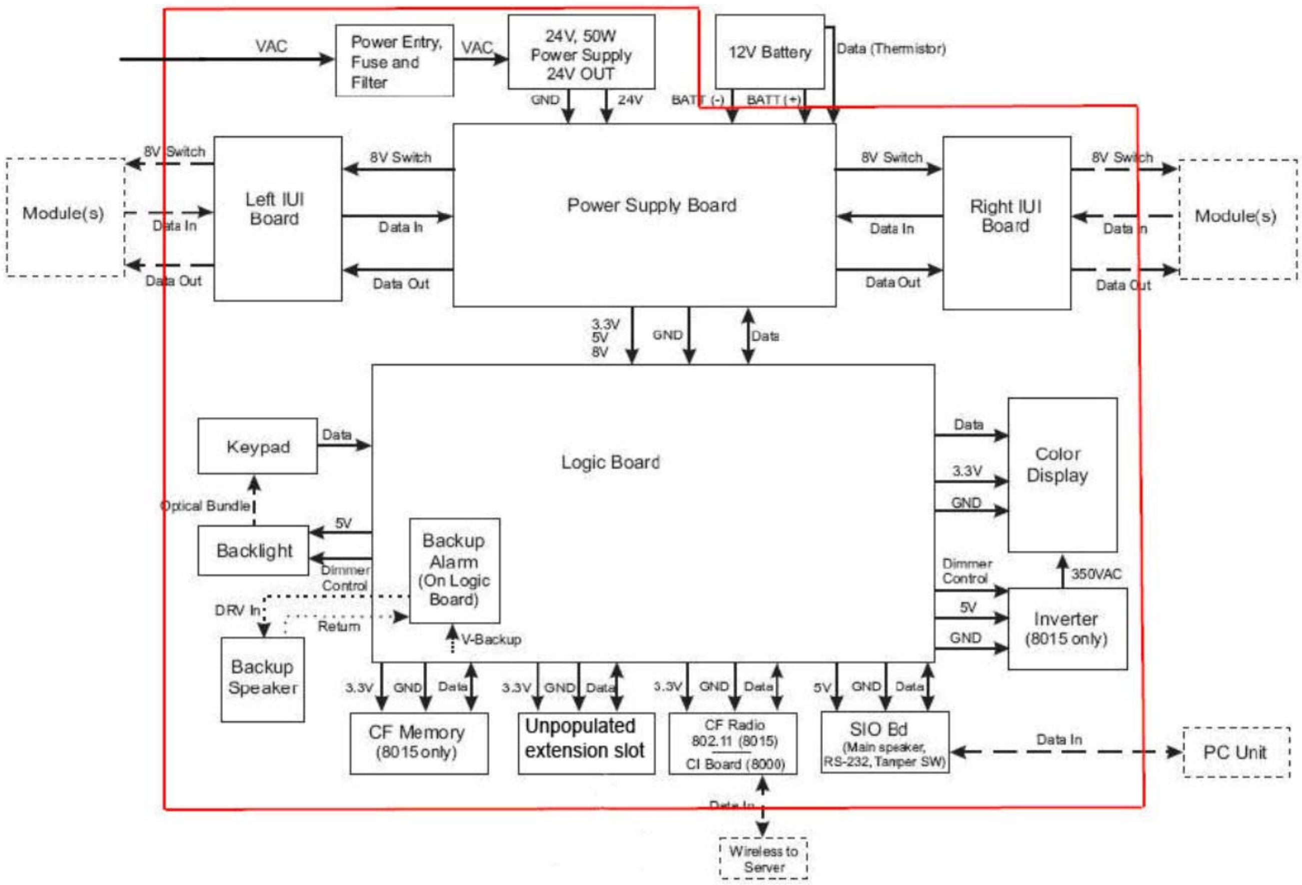


Figure 4 – Block diagram of CM logic

The CM comprises the components shown in the block diagram above.

- Power components: Power entry, fuse and filter; 24V power supply; 12V battery; Power Supply board (power conversion and distribution)
- Communications: Compact Flash Radio (802.11); Nurse Call (to alert nurses); Left and right IUI boards (communication with add-on clinical modules)
- Keypad, switches and annunciators: keypad, backlight, backup speaker, color display and inverter (display power); Tamper Resist Switch (used to lock keyboard from accidental key presses)
- Multi-function I/O board: SIO board, with serial communications to Alaris® System Maintenance (marked “PC Unit” in the diagram above)
- Processing and associated memory: Logic Board, with CPU, RAM and Flash memory; Compact Flash memory card

The battery pack and outer replaceable IUI connectors are not included in the cryptographic boundary. The IUI subsystem and battery subsystem do not implement any cryptographic function; they do not

Copyright Carefusion 2011. May be reproduced only in its original entirety [without revision].

provide any access to CSPs. The IUI connectors and battery pack are replaceable as part of routine maintenance; removal does not affect CM opacity or provide unprotected entry points for probing or other access.

2. Versions and Modes of Operation

The configuration of hardware and firmware for this validation is:

- Hardware: Model 8015
- Firmware: Version 9.7.0

Firmware version is displayed on Software Versions page. To display firmware version, from Main page, press Options button, followed by 'Page Down' softkey once to display the page titled 'System Options 2 of 3'. Select option 'Software Versions' and then press 'View' from the following page. Page 'Software Rev. Review' is displayed containing software versions of various components. The three most significant digits corresponding to 'Main processor' provides firmware version number of CM.

2.1. FIPS Approved Mode of Operation

The CM provides a FIPS Approved mode of operation, comprising all services described in the section Roles and Services.

The CM always performs all FIPS 140-2 required cryptographic self-tests at power up. The CM may perform Public Operator (unauthenticated) role services for the operation of the pump at any time following successful power on self-tests and configuration checks.

The CM becomes a FIPS 140-2 module when the following conditions are met:

- The cryptographic self-tests performed at power on passed.
- The tamper-evident seals (physical security) have been applied.
- CSPs have been installed on the CM.

The operator can verify that the module is in FIPS mode on the display page titled 'System Options 3 of 3'. To display FIPS mode from the Main Page: press the Options button, followed by the Page Down softkey twice. The page titled 'System Options 3 of 3', displays the FIPS 140-2 mode. The CM displays "FIPS 140-2 Mode Enabled" only if the FIPS mode is enabled. In all other cases, the FIPS 140-2 mode indicator will display "FIPS 140-2 Mode Disabled".

FIPS 140-2 mode is set using the ASM Enable FIPS Mode service. Once FIPS 140-2 mode is Enabled, it cannot be set back to Disabled without a Maintenance mode operation.

2.2. Maintenance Mode of Operation

The CM implements a maintenance mode of operation, to be used when performing hardware maintenance activities or bulk-loading of new firmware. The associated maintenance procedures require zeroization of CSPs prior to entering FIPS maintenance mode, and prior to exiting FIPS maintenance mode. New tamper seals should be applied prior to exiting the maintenance mode.

Maintenance activity may include firmware replacement, which can be performed only with tamper seals broken and the unit opened. The module is FIPS 140-2 compliant only when a FIPS 140-2 validated firmware is loaded in the module.

Copyright Carefusion 2011. May be reproduced only in its original entirety [without revision].

3. Ports and Interfaces

The CM implements the ports and interfaces shown in the following table.

Port	Name and Description	FIPS 140-2 Designation
LCD display	LCD display located on the front panel, used to provide visual feedback to public operator (unauthenticated user).	Status output
Alaris® System Maintenance Serial port	Rear panel RJ-45 connector used for administrative control of the CM.	• Data input • Data output • Control input • Status output
IUI ports	The IUI Right and IUI Left ports on the sides of the CM provide control over pump expansion devices. These interfaces provide no cryptographic function nor access to CSPs.	• Data input • Data output • Control input • Status output • Power/ground
802.11 card antenna	Wireless communications interface, enabling communications with external wireless access point devices.	• Data input • Data output • Control input • Status output
Tamper resist switch	Rear panel button used to deter casual changes to infusion pump settings by disabling the front panel buttons. Tamper resist in this context is not related to cryptographic functions. No CSPs are affected by this switch.	Control input
Status LEDs	• Front panel status LEDs: AC power, battery, and communications. • Rear panel: 802.11 card LED for 802.11 status. These LEDs have no cryptographic relevance.	Status output
Speakers	Audio status output to indicate alarm status.	Status output
Keypad	Front panel keypad for local control of the CM.	Control input
Power port	AC power input.	Power/ground
Battery port	Battery pack connector.	Power/ground

Table 2 - FIPS 140-2 Ports and Interfaces

The CM requires an external device (the Alaris® System Maintenance) for module administrative configuration, including CSP entry. All CSP entry is performed via the Alaris® System Maintenance Serial port. The Alaris® System Maintenance software connects only to the serial port depicted in Figure 4. No other connection port is used by the Alaris® System Maintenance software.

Copyright Carefusion 2011. May be reproduced only in its original entirety [without revision].

4. Cryptographic Functionality

The CM performs FIPS 140-2 Approved cryptography in two services:

- The authentication handshake between the CM and an Alaris® Systems Manager (Server), using SHA-256 and externally established shared secrets.
- Encryption and decryption of communications taking place over the network connection between the CM and the Alaris® Systems Manager (Server).

4.1. Approved and Allowed Algorithms

The CM supports the following FIPS Approved algorithms.

FIPS Approved Algorithm	CAVP Cert. #
AES (1) 128, 192, and 256-bit ECB encryption and decryption	1436
SHA-256	1301

Table 3 - FIPS Approved Algorithms

The CM implements a non-FIPS approved but allowed third-party supplied RNG to generate challenge values for CO authentication.

Copyright Carefusion 2011. May be reproduced only in its original entirety [without revision].

4.2. Non-FIPS Approved Algorithms

The CM includes an embedded off-the-shelf compact flash 802.11 card. The 802.11 card implements uncertified cryptographic algorithms to satisfy wireless communications protocols in the deployment environment; no FIPS 140-2 security claims are made for 802.11 communications cryptography. The compact flash radio card and the library used for the 802.11 communications contain the non-approved algorithm implementations listed below. None of these algorithm implementations are used by the module for any other purpose.

Non-FIPS Approved Algorithm
Uncertified cryptographic functions implemented by the 802.11 RF module: • AES (2) 128/192/256 (non-compliant) • RC4 • MD5 • SHA-1 (non-compliant) • SHA-256 (non-compliant) • RIPEMD • DES—ECB, CFB, CBC, & OFB modes • Triple DES—ECB, CFB, CBC & OFB modes (non-compliant) • RC2-CBC, RC2-ECB, RC2-CFB64, RC2-OFB64 • Blowfish • CAST • RSA (non-compliant) • DSA (non-compliant) • DH

Table 4 – Non-FIPS Approved Algorithms

Copyright Carefusion 2011. May be reproduced only in its original entirety [without revision].

4.3. Critical Security Parameters (CSPs)

The CM implements the CSPs listed in the following table:

CSP Name	Length and Type
ENC	AES 128-bit symmetric key used to encrypt and decrypt all traffic between the module and the Alaris® Systems Manager (Server) when the CM is in FIPS mode.
CU-AUTH	A 6-20 character string shared secret for CU authentication. A character string used in the CU authentication handshake with the Alaris® Systems Manager (Server) hashed by SHA-256 along with a nonce. The module supports eight instances of this CSP. A six-character minimum string length is enforced by the CM.
CM-AUTH	A 6-20 character shared secret for optional authentication of CM to the Alaris® Systems Manager (Server). A six-character minimum string length is enforced by the CM.
CO-AUTH	6-20 character string user name and password strings used in the CO authentication when communicating with the Alaris® System Maintenance over the Alaris® System Maintenance serial port for use in CSP-related transactions. A six-character minimum string length for user name and for password is enforced by the CM.

Table 5 - Critical Security Parameters

All CSPs are entered and output in plain text over the serial port by the CO using the Alaris® System Maintenance tool. The CSP entity association is the network configuration profile identifier; each network configuration profile includes host name and port. The ENC key, CO-AUTH, CM-AUTH, and CU-AUTH shared secret values are generated externally to the CM, then manually distributed, and entered into the CM electronically via the Alaris® System Maintenance.

The CM does not display or otherwise provide any user feedback of CSPs. The CM does not implement any form of electronic or automated key establishment. The CM does not generate any keys or output any intermediate key values

The CM does not implement any public keys.

Copyright Carefusion 2011. May be reproduced only in its original entirety [without revision].

5. Roles and Services

5.1. Identification and Authentication

The CM supports four distinct operator roles as described in Table 6.

ID	Role Description	Authentication Type	Authentication Data
CO	Cryptographic Officer: an Alaris® Systems Maintenance user authorized to load CSPs.	Role-based authentication. See Alaris® System Maintenance authentication in Table 7.	CO-AUTH
CU	Cryptographic User: the role used for communications between the module and the Alaris® Systems Manager (Server).	Role-based authentication See CU Authentication in Table 7.	CU-AUTH
PO	Public Operator: an implicit role for unauthenticated services	Not authenticated	N/A
M	Maintenance Operator: an implicit role for maintenance services	Not authenticated	N/A

Table 6 - Roles and Required Identification and Authentication

Two implicit roles are defined for the CM: Public Operator (PO) and Maintenance (M). The PO services are the clinical services accessible from the front panel operator, and the subset of services performed by an unauthenticated operator using the Alaris® Systems Maintenance tool via the serial port. The M services are performed to perform physical maintenance of the CM.

The CM enforces the separation of roles; the CO and CU roles require authentication and occur over different interfaces. The CO role is applicable to a subset of commands (see Table 8) invoked by the Alaris® Systems Maintenance tool. Each invocation of an authenticated service requires authentication of the CO (the Alaris® Systems Maintenance tool). For the CU role, a session is initiated when communication with an Alaris® Systems Manager (Server) is established. The session is destroyed when communication with Alaris® Systems Manager (Server) is terminated.

All authenticated sessions are terminated at the CM power-cycle. The CM does not retain authentication across a power-cycle.

A separate set of credentials is required for each authenticated role. The CM does not allow switching of authenticated roles, as these roles are available only using a specific interface of the CM.

The CM allows multiple concurrent operators; however, only one operator per role is allowed at a given instance. The Maintenance role is the role assumed to perform physical maintenance.

Copyright Carefusion 2011. May be reproduced only in its original entirety [without revision].

Each authentication mechanism implemented by the CM is listed in the following table, along with the FIPS 140-2 required strength of authentication rationale.

Authentication Mechanism	Strength of Mechanism
Alaris® System Maintenance Authentication (authentication of CO via the Alaris® System Maintenance Serial port)	CM implements a user name and password-based authentication mechanism to authenticate the CO. A valid password is a minimum of six characters in length and consists of a-zA-Z0-9_~@#%|&()-{} characters. These characters allow a minimum of 3.83E+57 possible combinations. The probability that a random attempt will succeed or a false acceptance will occur is 1/3.83E+57, or 2.61E-58. Based on Alaris® Systems Maintenance workflow, it is estimated that the number of maximum number of authentication attempts that can be made is less than 10/minute. The probability of successfully authenticating to the module within one minute is 2.61E-57.
CU Authentication (authentication of a remote Alaris® Systems Manager (Server) via a wireless network)	CM implements a shared passphrase-based CHAP mechanism to authenticate the CU. A valid passphrase is a minimum of six characters in length and consists of a-zA-Z0-9_~@#%|&()-{} characters. These characters allow a minimum of 3.83E+57 possible combinations. The probability that a random attempt will succeed or a false acceptance will occur is 2.61E-58. Based on the communication protocol used, it is estimated that the maximum number of authentication attempts that can be made is less than 10/minute. The probability of successfully authenticating to the module within one minute is 2.61E-57.

Table 7 - Strengths of Authentication Mechanisms

Copyright Carefusion 2011. May be reproduced only in its original entirety [without revision].

5.2. Services and Service Usage of CSPs

Table 8 lists all services performed by the CM, describing authorized roles and CSPs used for each service. The CM does not implement any service that outputs CSPs.

In the listing below:

- "executes using" means the CSP value is used when performing the service.
- "update" means a new CSP value is entered into the CM.
- "zeroization" means the CSP is overwritten with null values.

Service	Description	CO	CU	PO	M
Self-test	Perform power up self-tests; which are invoked by power cycling the module. Does not access any CSPs. KAT values are not CSPs.			X	
Enable FIPS mode	Deletes non-FIPS mode CSP values; put the CM into FIPS mode. Has no effect once the CM is in FIPS mode; FIPS mode cannot be disabled.			X	
System Manager Authenticate	Performs the authentication of Alaris® Systems Manager (Server) to the module (CU Role authentication); executes using CU-AUTH. Optionally performs authentication of the module to Alaris® Systems Manager (Server); executes using CM-AUTH.		X		
Secure communication	Encryption and decryption of data between the module and the Alaris® Systems Manager (Server). Executes using ENC.		X		
Update Alaris® System Maintenance login data	Change CO user name and password using the Alaris® System Maintenance. Updates and reads CO-AUTH and CM-AUTH, in plaintext.	X			
Server CSP Load	Updates and reads ENC, CM-AUTH and CU-AUTH in plaintext using the Alaris® System Maintenance as a key loader.	X			
Zeroize	Overwrite all CSPs with null values. Zeroize is not an authenticated command; it is available over the Alaris® Systems Maintenance (serial port) interface, but is not authenticated.			X	X
Local show status	Performed using the front panel interface within the network configuration function.			X	
Remote show status	Status/health test performed between the CM and the Alaris® Systems Manager (Server). Does not access any CSPs.		X		
Clinical device configuration and services	All clinical, non-cryptographic services provided by the CM. No CSPs are accessed by these services.			X	

Table 8 – Services and Service Usage of CSPs

Local show status and *Remote show status* information does not contain CSPs or sensitive data that if misused could lead to a compromise of the CM.

Copyright Carefusion 2011. May be reproduced only in its original entirety [without revision].

6. Physical Security Policy

6.1. Physical Security Mechanisms

The CM is a multichip standalone embodiment with an opaque covering and tamper-evident seals at all potential access points and seams.

See Appendix A for figures that show the placement of the physical tamper-evident seals. These seals are designed to provide tamper evidence and have been tested as a part of the FIPS 140-2 validation process.

6.2. Maintenance Access Interface

The CM is maintained by authorized clinical engineering staff, assuming the maintenance role and accessing the module via the maintenance access interface. CareFusion provides a detailed FIPS 140-2 maintenance procedure. The CM is in the maintenance state once the procedure is initiated and until the procedure is complete.

The maintenance access procedure requires zeroization of all CSPs using the Zeroize service prior to removal of tamper seals or enclosure covers. Tamper seals must be removed prior to removal of any enclosure cover. See Appendix A: FIPS 140-2 Physical Security Considerations and Tamper Seal Installation.

The front and rear panels are removable for maintenance/replacement of internal components. The device battery is also removable. Battery removal does not provide access to the inside of the device: the battery harness is protected by a tamper seal.

The maintenance procedure requires new seals to be applied and CSP zeroization before the CM exits the maintenance state. Once the CM is no longer in the maintenance state, the CO must authenticate using the default CO authentication value, and then re-initialize all CSPs .

Copyright Carefusion 2011. May be reproduced only in its original entirety [without revision].

6.3. Operator Required Actions

The following table outlines the inspection and testing of the physical security mechanisms.

Physical Security Mechanisms	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
Tamper-Evident Seals	Annual inspection of the device for tamper evidence. On initial deployment, devices are configured with tamper-evident seals and the device is placed into clinical use.	Processes for inspection of Physical Security can be found in the "FIPS 140-2 Compliance Instructions for the Alaris® PC Unit, Alaris® System Maintenance, and Alaris® Systems Manager." This process requires physical inspection of the tamper-evident seals to verify integrity and secure adhesion.

Table 9 – Inspection/Testing of Physical Security Mechanisms

Copyright Carefusion 2011. May be reproduced only in its original entirety [without revision].

7. Self-test

7.1. Power Up Cryptographic Algorithm Self-Tests and Software Integrity Test

The operator can command the CM to perform the power-up self-test by cycling power. Power-up self-tests execute without operator action. The CM performs the following self-tests at power up:

- Verification of all CM firmware for integrity using CRC-32
- Verification of AES algorithm function using AES encrypt and decrypt known answer tests
- Verification of SHA-256 algorithm function using a SHA-256 known answer test

7.2. Conditional Cryptographic Tests

The RNG is tested on each call for a “stuck-fault,” comparing the current RNG output to the previous value to ensure that the previous value has not been repeated.

7.3.Critical Functions Tests

The CM performs the following tests at power-up.

- Memory test
- Audio-speaker test
- Power-supply test
- Communications board test

In addition to the power-up tests, the CM performs continuous memory tests.

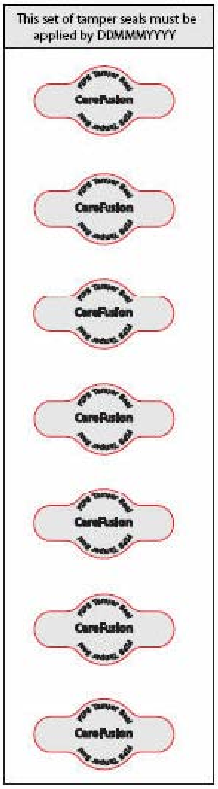
Copyright Carefusion 2011. May be reproduced only in its original entirety [without revision].

8. Appendix A—FIPS 140-2 Physical Security Considerations and Tamper Seal Installation

This procedure provides the steps for applying the tamper-evident seals on the Alaris® PCU Model 8015.

Part number	Description
11935165	FIPS Seal Kit (includes tamper-evident seals and orange stick)
11749252	Tamper-evident seals
10927242	Orange stick
N/A	Cotton tip applicator or soft cloth

The tamper-evident seals are provided in quantities of seven seals per sheet (Figure 1). When the tamper-evident seals are applied to the Alaris® PCU Model 8015, they are valid until removed, damaged, or compromised. The shelf life of the tamper-evident seals is printed on the sheet. When applied before the expiration date on the sheet, the seals are valid for intended use.



This set of tamper seals must be applied by DDMMMYYYY

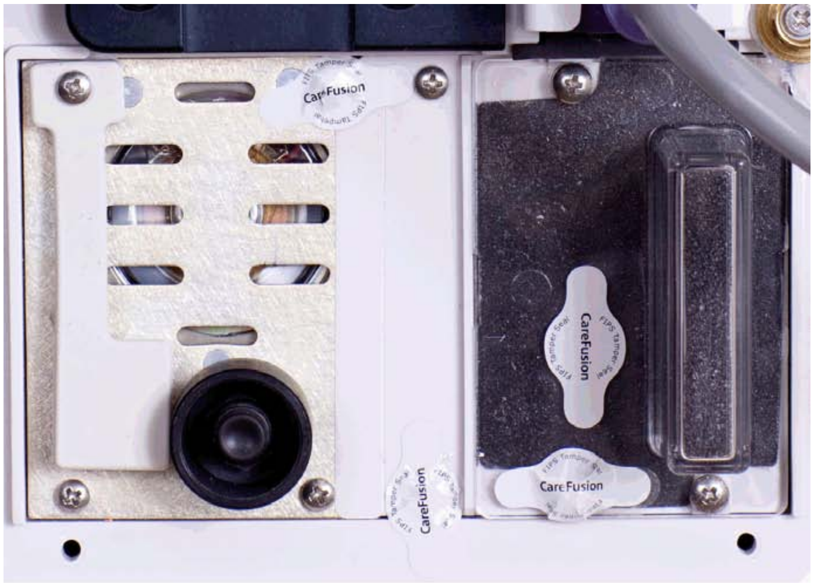
Figure 1 Tamper-Evident Labels sheet

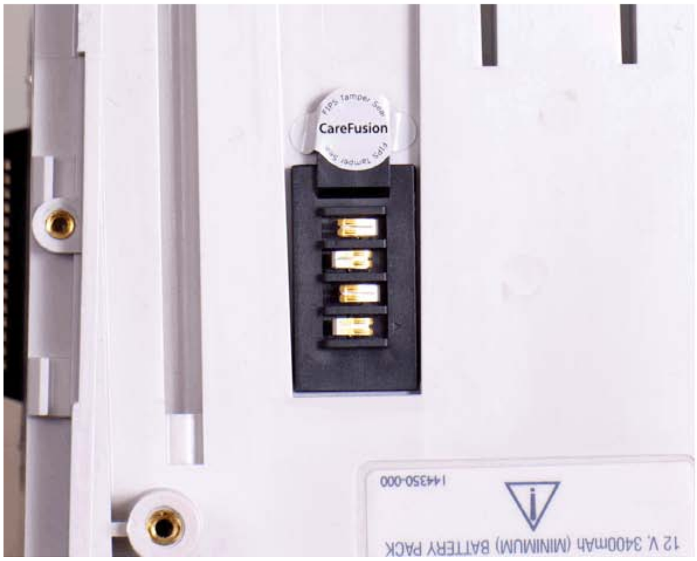
Copyright Carefusion 2011. May be reproduced only in its original entirety [without revision].

NOTE: After applying the tamper-evident seals, allow the seals to cure for 72 hours. Until the 72-hour curing process has occurred, the device is not compliant with recommended security practices. Hospital policy will determine if devices can be placed into clinical service during this curing time. CareFusion makes no claim as to the efficacy of tamper-evident seals that are not allowed to cure for 72 hours.

NOTE: It is recommended that the tamper-evident seals be replaced if applied incorrectly or if the seals show signs of wear and tear.

The following figures show the placement of four of the tamper-evident seals on the rear of the device, on the battery connector, and on the grooves on both sides of the device (Figure 2).





Copyright Carefusion 2011. May be reproduced only in its original entirety [without revision].

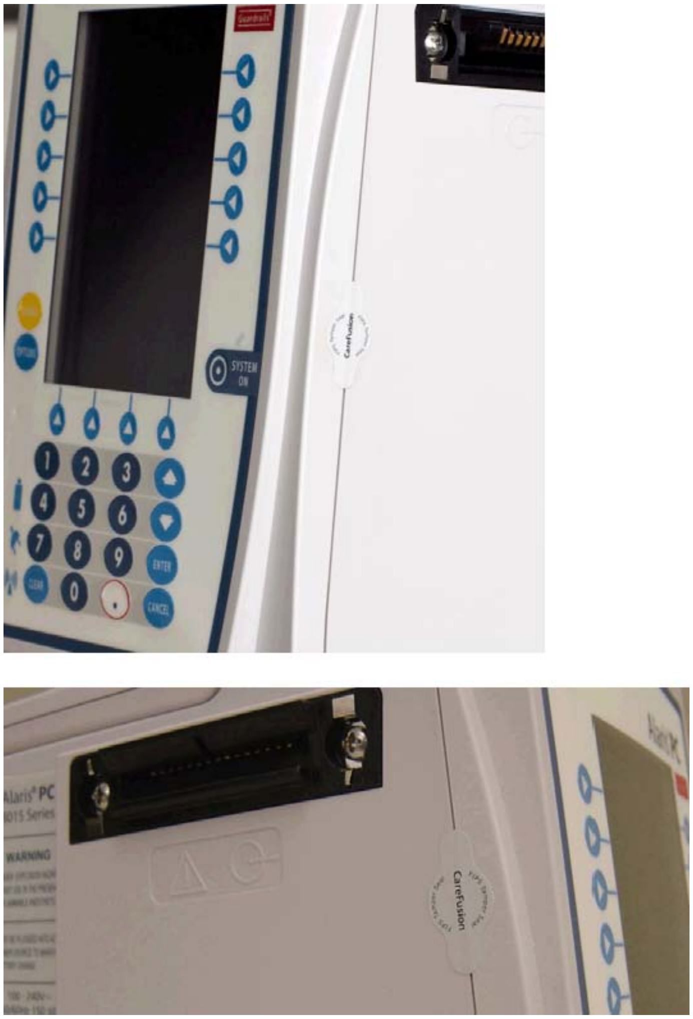


Figure 2 Location of seals on device

8.1. Applying tamper-evident seals

NOTE: Placing the device face-down on a work surface can result in damage to the operation panel. Lay a cloth down before placing the device on its front panel.

1. Before applying the tamper-evident seals, clean the surfaces where the labels will be applied with 70% isopropyl alcohol and allow the surface to dry.

2. Peel a tamper-evident seal from the sheet of seals.

Copyright Carefusion 2011. May be reproduced only in its original entirety [without revision].

3. Carefully center the tamper-evident seal over the middle screw in the row under the black area (Figure 3).

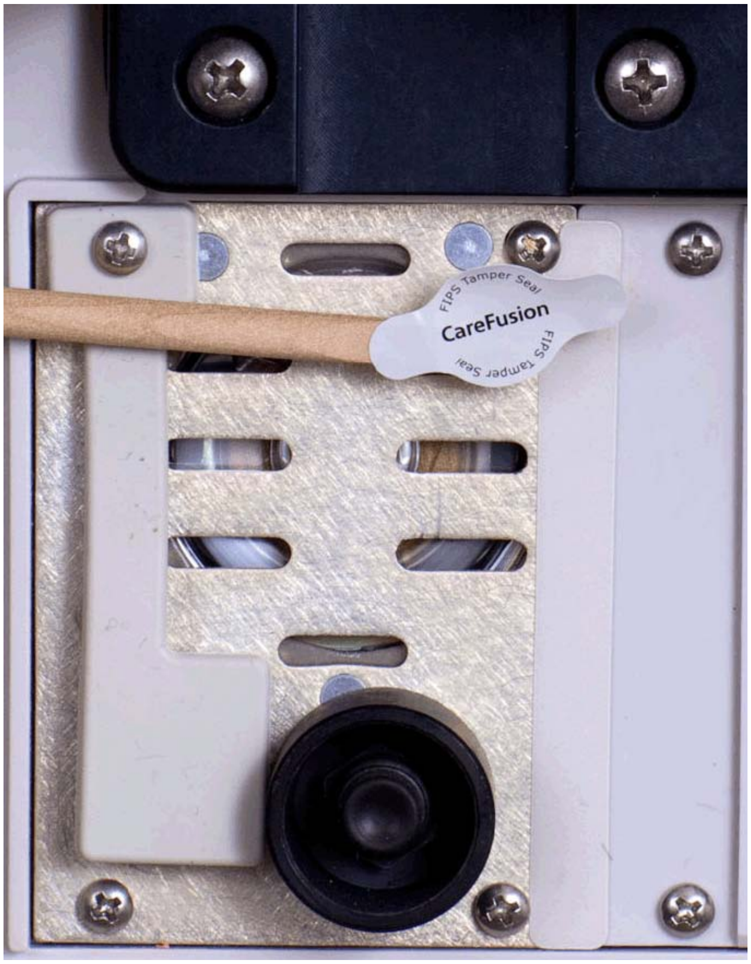


Figure 3 Center the seal over middle screw in row beneath black area

Copyright Carefusion 2011. May be reproduced only in its original entirety [without revision].

4. Ensure that the tamper-evident seal covers the entire head of the Phillips screw (Figure 4). An orange stick (P/N 10927242) can be used to conform the tamper-evident seal to the shape of the screw head.

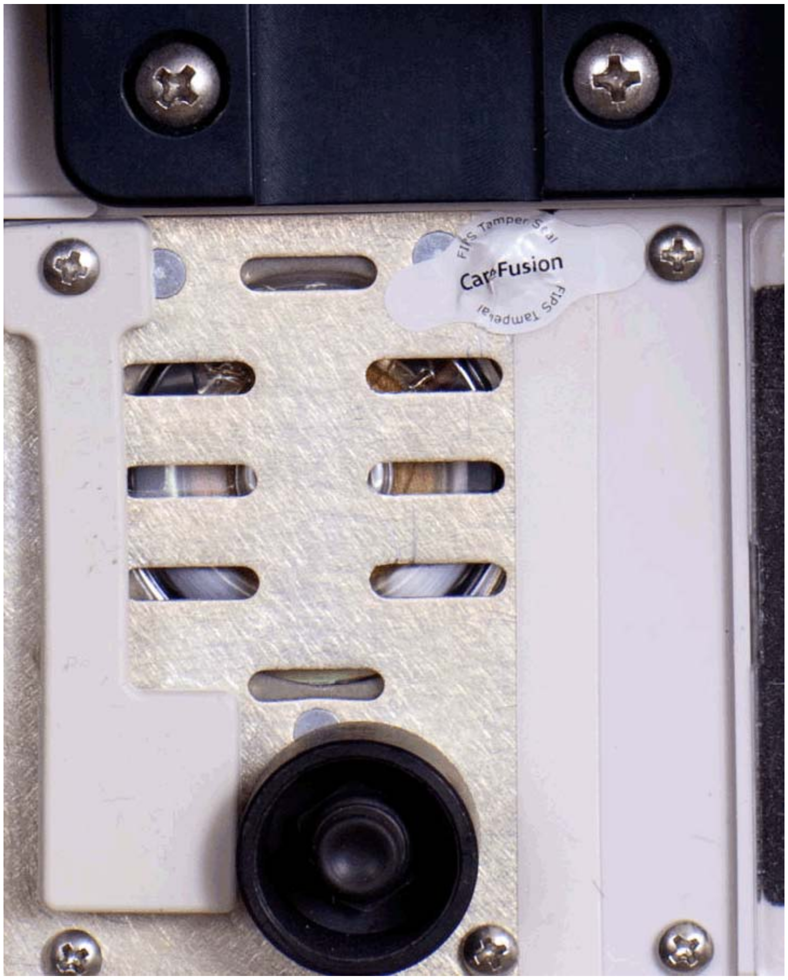


Figure 4 Seal must cover entire head of screw

Copyright Carefusion 2011. May be reproduced only in its original entirety [without revision].

Incorrect application below (Figure 5)—Notice how the tamper-evident seal is incorrectly placed offset from the screw head. The screw head should not be visible.

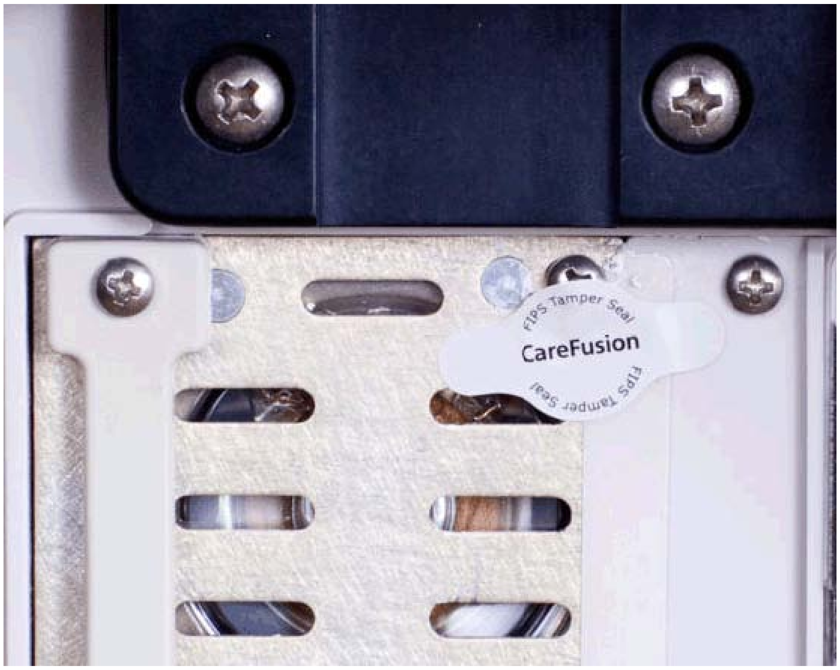


Figure 5 Incorrect seal application

5. Carefully center and affix the tamper-evident seal over the viewing hole (not an actual hole, but a small circle where the cover is not opaque) on the wireless card cover in location 2 (Figure 6).

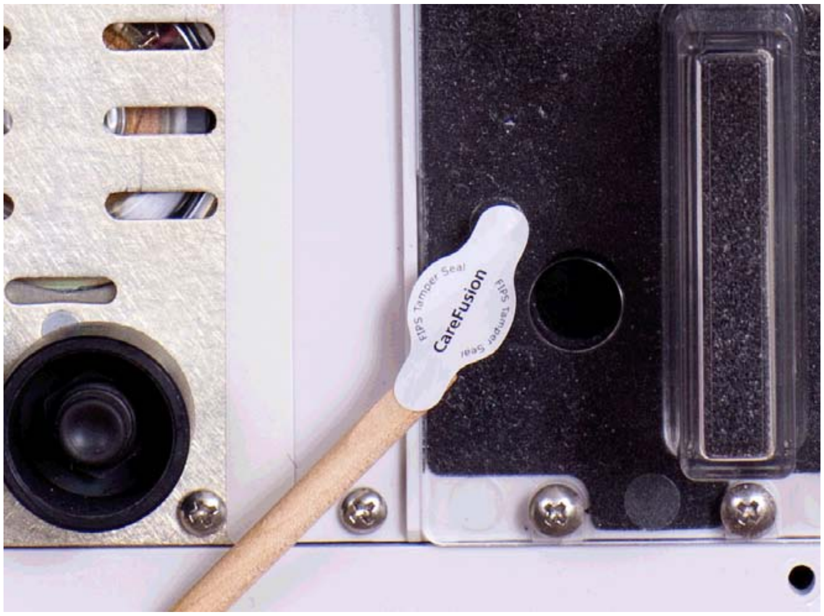


Figure 6 Affix seal over hole in wireless card

6. Ensure that the tamper-evident seal covers the entire hole (Figure 7).

Copyright Carefusion 2011. May be reproduced only in its original entirety [without revision].

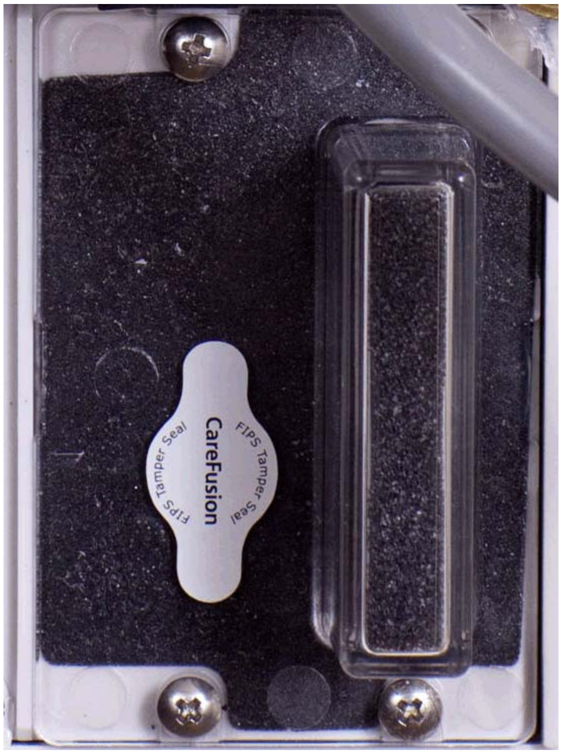


Figure 7 Ensure seal covers entire viewing hole

Incorrect application below (Figure 8)—Notice that the tamper-evident seal was incorrectly placed so that a portion of the hole is visible. The entire hole must be covered so that no part of it is visible.

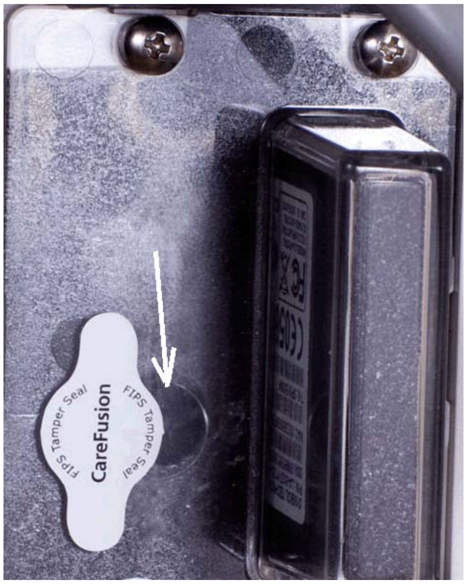


Figure 8 Incorrect application

Copyright Carefusion 2011. May be reproduced only in its original entirety [without revision].

7. Carefully center and affix the tamper-evident seal over the bottom screw as indicated by the arrow (see Figure 9).

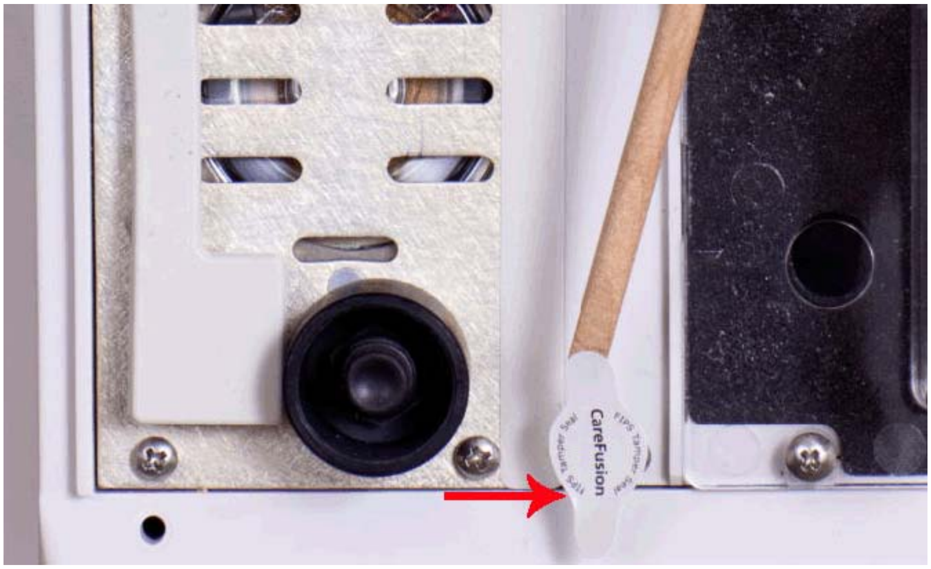


Figure 9 Affix seal over bottom screw

8. Ensure that the tamper-evident seal covers the entire head of the Phillips screw (Figure 10).

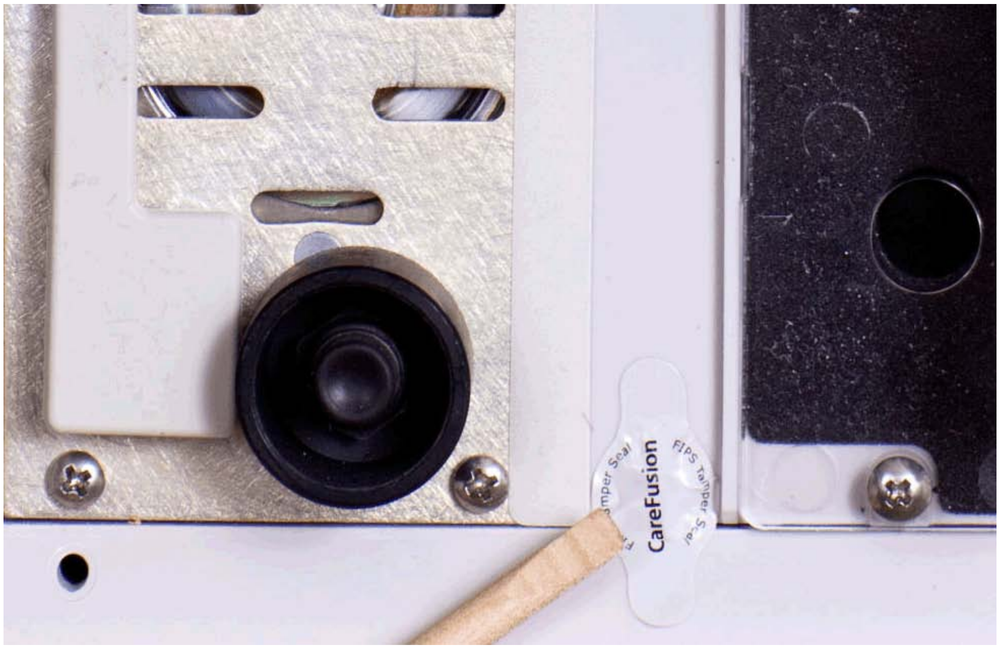


Figure 10 Ensure seal covers entire head of screw

Incorrect application below (Figure 11)—Notice that the tamper-evident seal was not placed over the entire Phillips screw. The entire screw head must be covered by the tamper-evident seal so that no portion of it is visible.

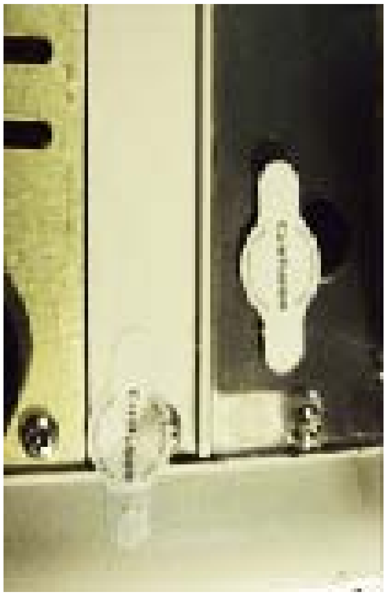


Figure 11 Incorrect application

9. Carefully center and affix the tamper-evident seal over the bottom screw of the wireless card cover (Figure 12).

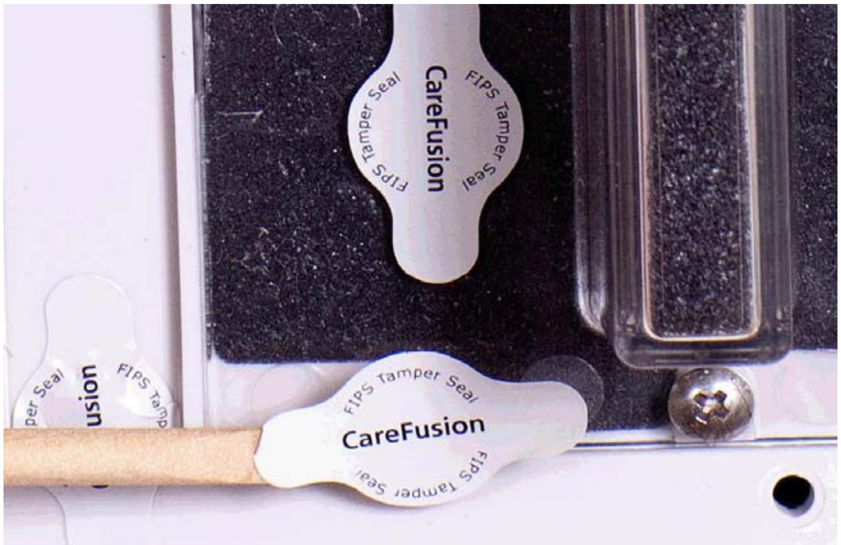


Figure 12 Affix seal over bottom screw of wireless card cover

Copyright Carefusion 2011. May be reproduced only in its original entirety [without revision].

Incorrect application below (Figure 13)—Notice that the tamper-evident seal was not placed over the entire Phillips screw. The screw head must be covered entirely so no part of it is visible.

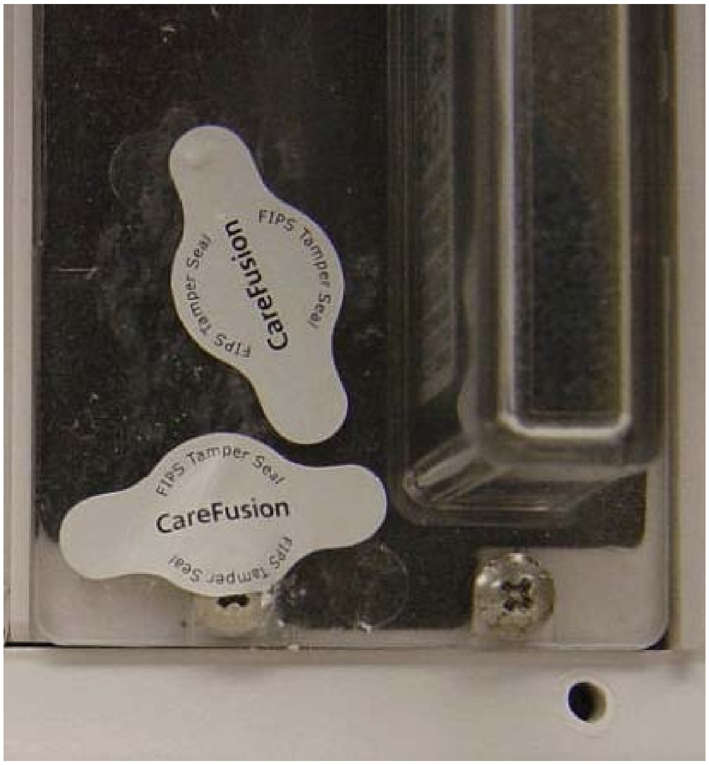


Figure 13 Incorrect application

Copyright Carefusion 2011. May be reproduced only in its original entirety [without revision].

10. On the underside of the device with the battery removed, carefully center and affix the tamper-evident seal over the battery connector screw (Figure 14).

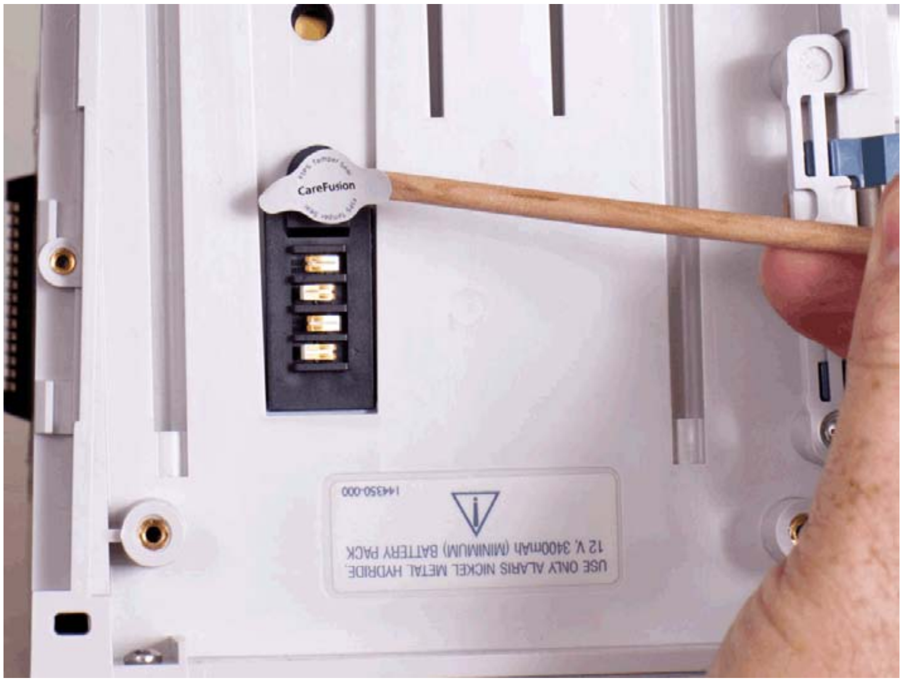

FIPS Tamper Seal
CareFusion
144350-000
12 V, 3400mAh (MINIMUM) BATTERY PACK
USE ONLY ALARIS NICKEL METAL HYDRIDE

Figure 14 Affix seal over battery connector screw

11. Ensure that the tamper-evident seal covers the entire head of the Phillips screw (Figure 15).

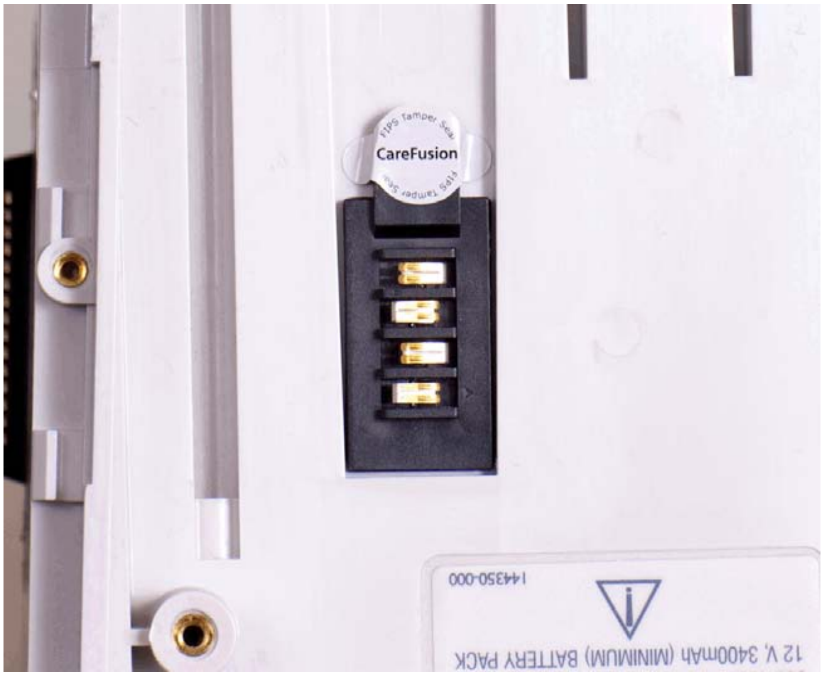


Figure 15 Ensure seal covers entire head of screw

Copyright Carefusion 2011. May be reproduced only in its original entirety [without revision].

Incorrect application below (Figure 16)—Notice that the tamper-evident seal was not placed over the entire Phillips screw. The screw head must be covered entirely so no part of it is visible.

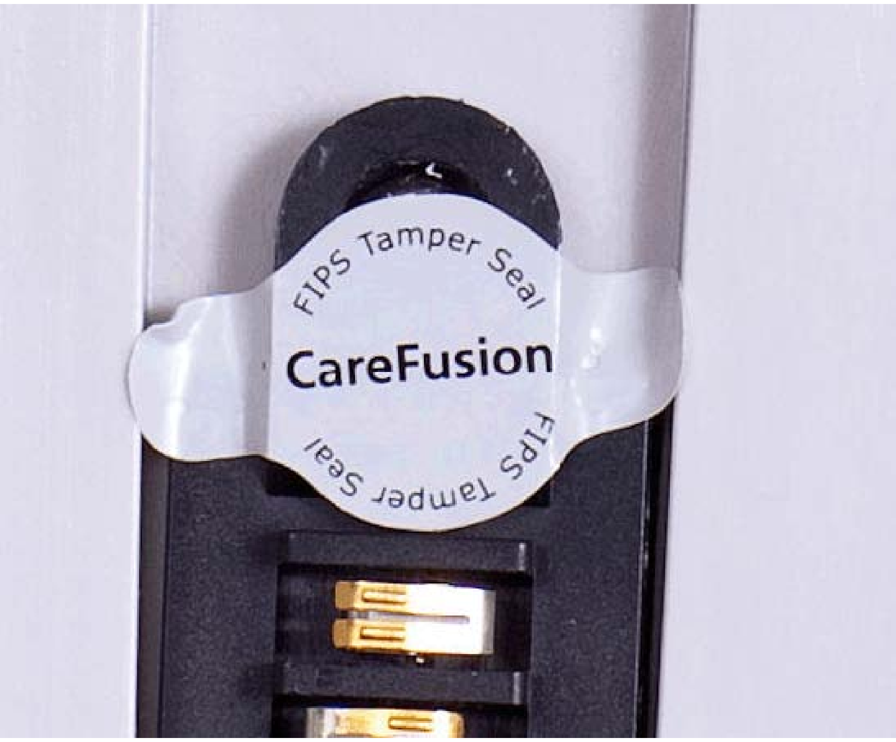


Figure 16 Incorrect application

Copyright Carefusion 2011. May be reproduced only in its original entirety [without revision].

12. Carefully center and affix a tamper-evident seal on the each side of the device, on the groove between the rear and front cases (Figure 17). Apply one tamper-evident seal on the left side and one on the right side of the device.

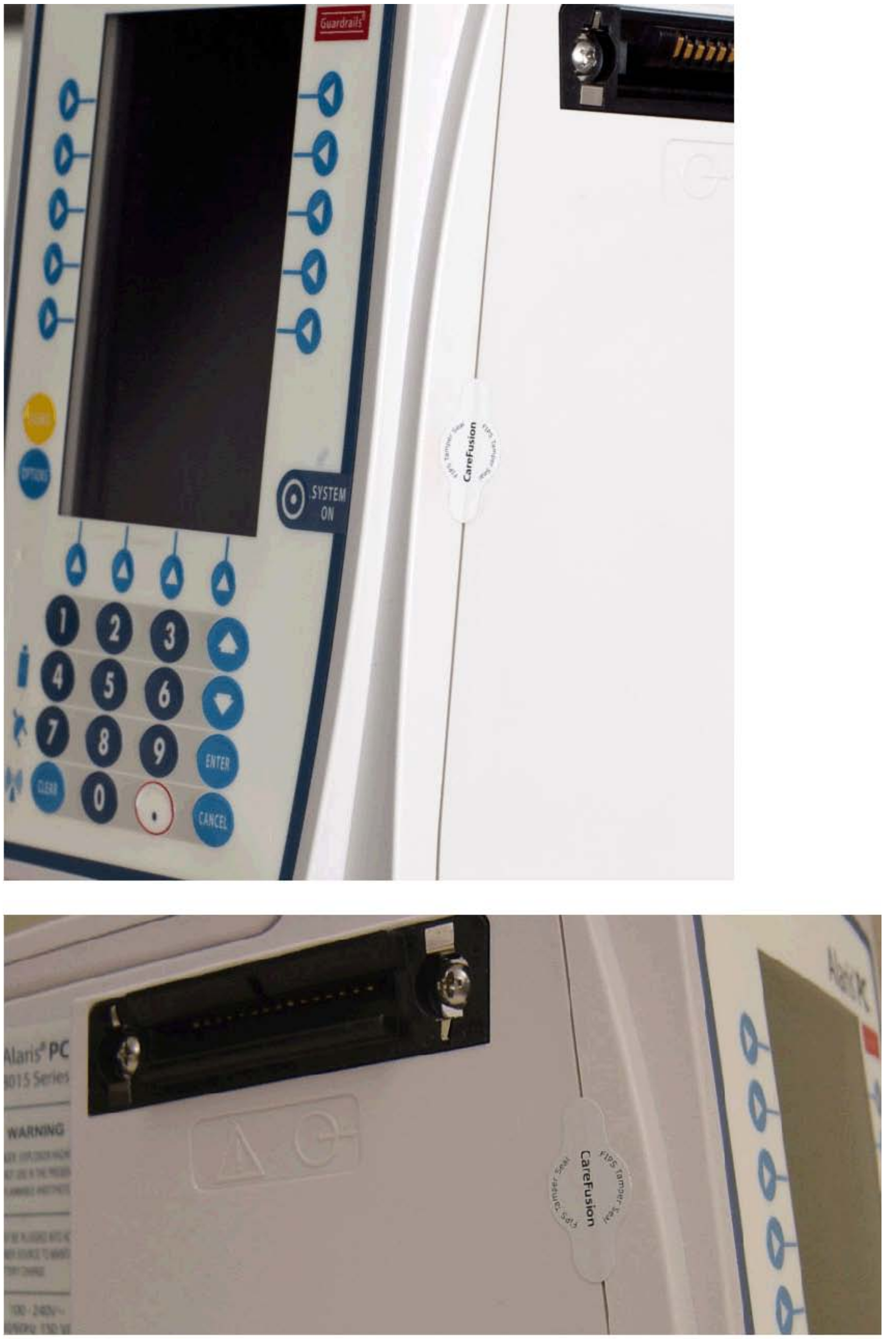


Figure 17 Affix a seal on each side of the device

Copyright Carefusion 2011. May be reproduced only in its original entirety [without revision].

13. Ensure that the tamper-evident seal is centered over the groove where the two case halves meet (Figure 18).

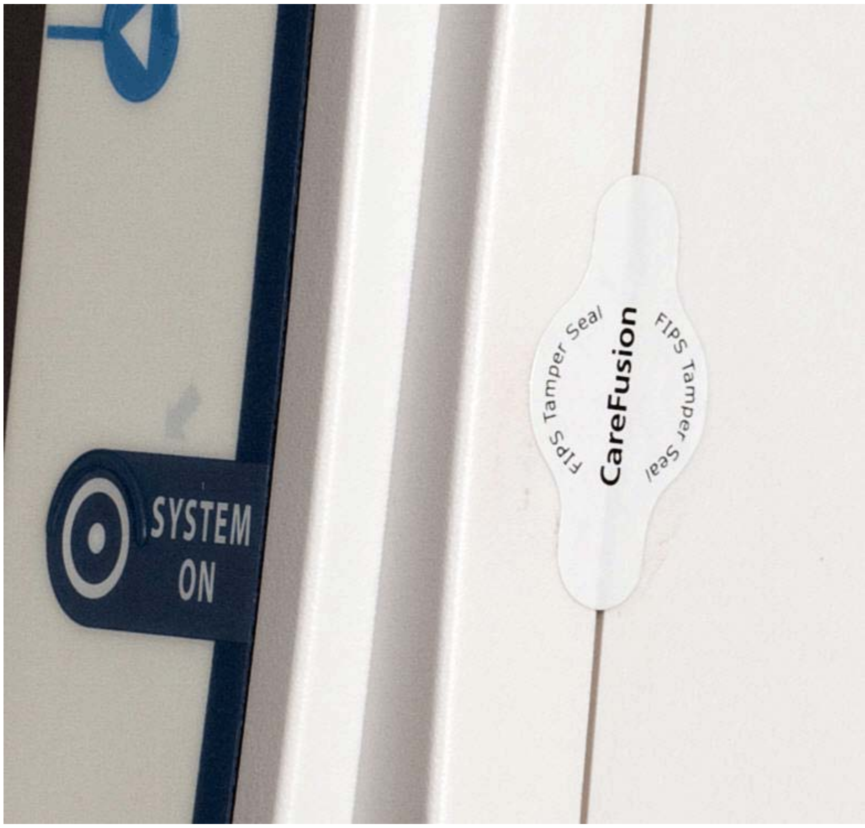


Figure 18 Ensure seal is centered between grooves

Copyright Carefusion 2011. May be reproduced only in its original entirety [without revision].

Incorrect application below (Figure 19)—In this image, the tamper-evident seal was not centered over the groove where the two case halves meet. Be sure to center the seal over the groove where the two case halves meet.

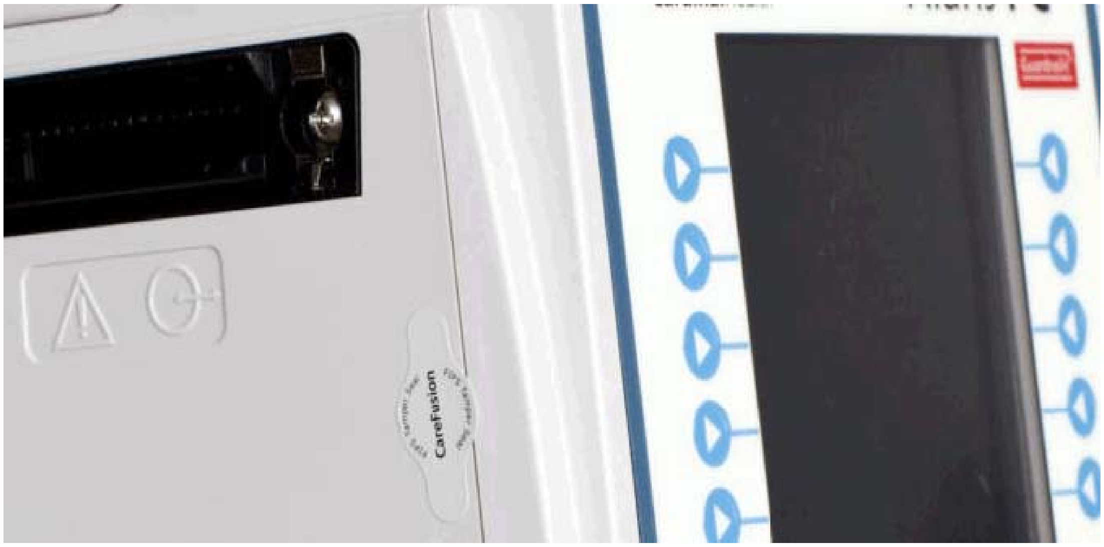


Figure 19 Incorrect application

8.2. Removing the tamper-evident seals

NOTE: CareFusion cannot guarantee the performance of the tamper-evident seals if new seals are placed on top of old seals or if residue or remains of previous seals are not properly removed before the application of new seals.

NOTE: Do not use a tool that may scratch the surface of the device.

NOTE: When the tamper-evident seals are applied to the device, it is up to your facility to decide when to replace the seals. They do not need to be replaced unless they show signs of wear and tear and/or tampering. Removal of the tamper-evident seals is also done whenever the device needs physical maintenance. The seals are destroyed when removed and cannot be reused.

8.2.1. Cleaning Products recommended by CareFusion

CareFusion recommends the use of 70% isopropyl alcohol (IPA) on the Alaris® PCU to clean the residue left behind when the tamper-evident seals are removed.

For more cleaning agents, see the following link:
https://inside.carefusion.com/myteam/irs/infusion/marketingresources/Alaris%20System%20Version%209/Alaris%20System%20Cleaning%20Products.pdf

Copyright Carefusion 2011. May be reproduced only in its original entirety [without revision].

8.2.2. To remove the tamper-evident seals

The following images show the location of the tamper-evident seals on the rear of the device, on the battery connector, and on the grooves on both sides of the device (Figure 20).

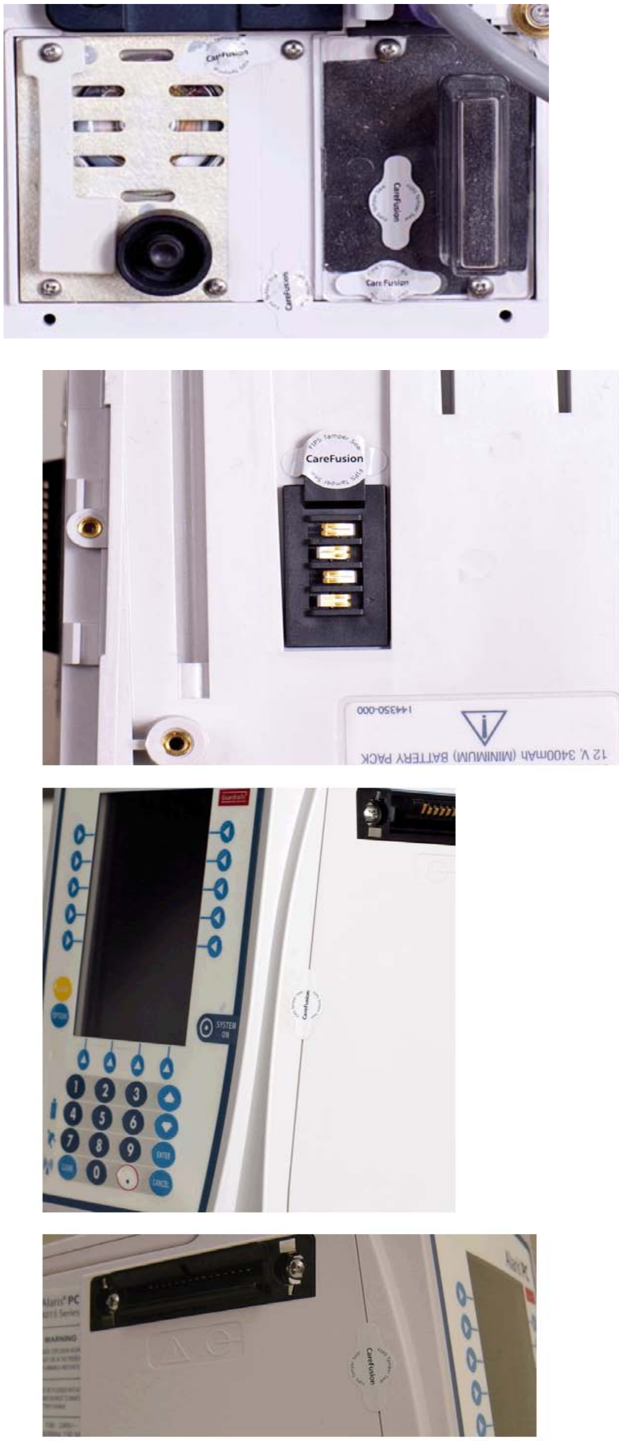


Figure 20 Location of each seal

Copyright Carefusion 2011. May be reproduced only in its original entirety [without revision].

1. Remove each of the seals. For the tamper-evident seals that cover a screw head, begin by removing the screws first (Figure 21).

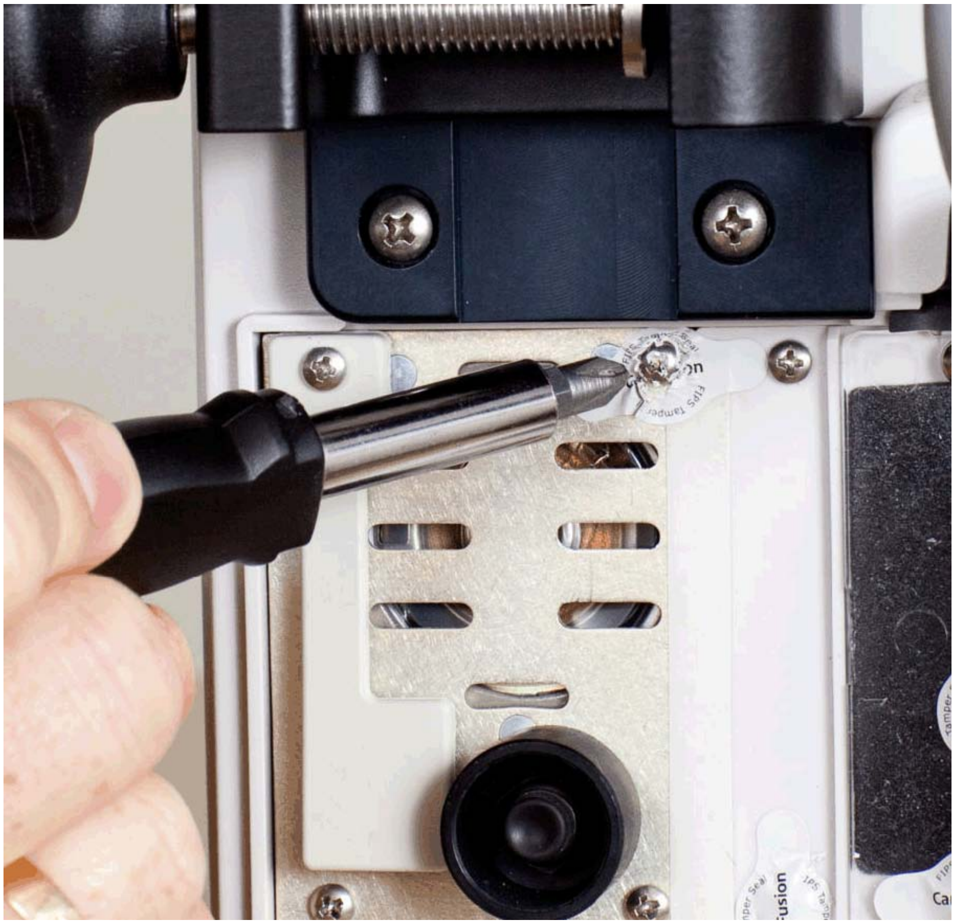


Figure 21 Remove seals

2. Use the orange stick to remove the remaining debris from the back of the Alaris® PCU rear case, leaving no portion of the tamper-evident seal present (Figure 22).

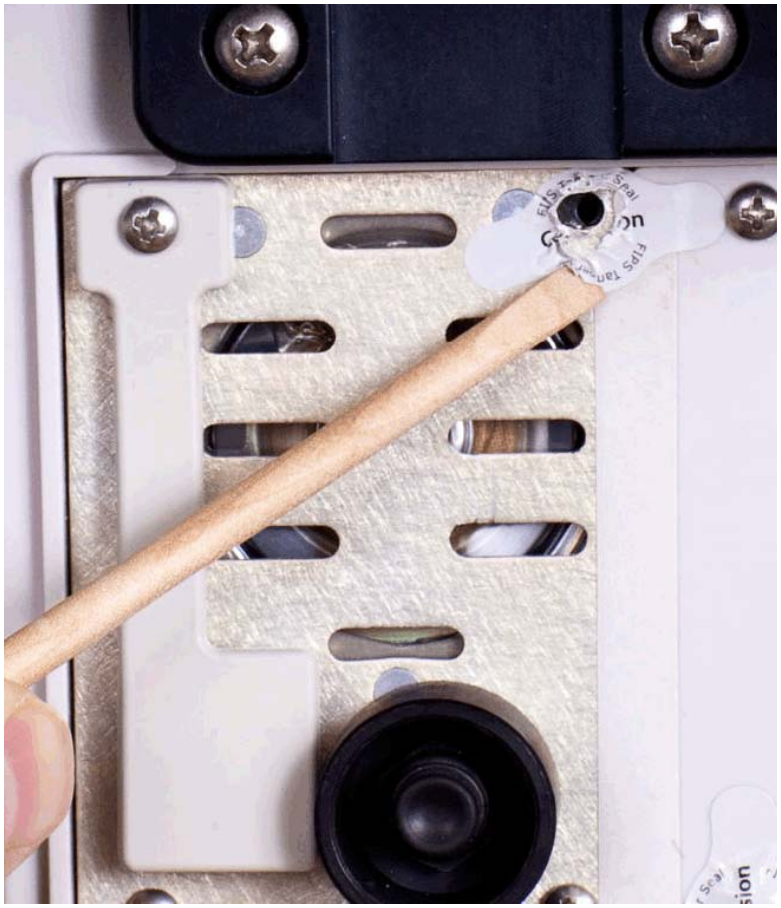


Figure 22 Use orange stick to remove debris

Copyright Carefusion 2011. May be reproduced only in its original entirety [without revision].

3. Remove the remaining debris from the head of the uninstalled screw with tweezers, a fingernail, or a soft cloth. Wipe clean with a soft cloth or a cotton tip applicator dampened with 70% IPA (Figure 23).

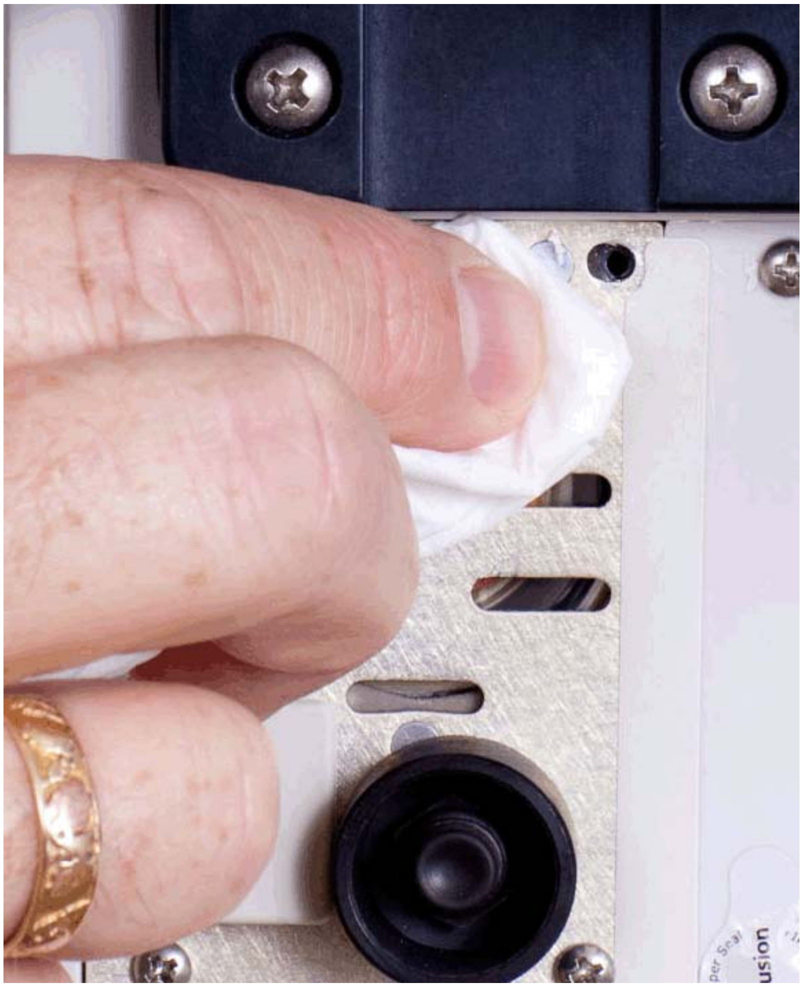


Figure 23 Removing remaining debris

NOTE: Prior to reinstalling the tamper evident seals, make sure that the screws on the rear panel of the Alaris® PCU are properly torqued to 6 in/lb according to the *Alaris® Technical Service Manual*.

Copyright Carefusion 2011. May be reproduced only in its original entirety [without revision].

4. Remove the screw that holds the battery in place, and remove the tamper-evident seal from the battery connector (Figure 24). Remove remaining adhesive residue with a soft cloth. Wipe clean with a soft cloth or a cotton tip applicator dampened with 70% IPA.

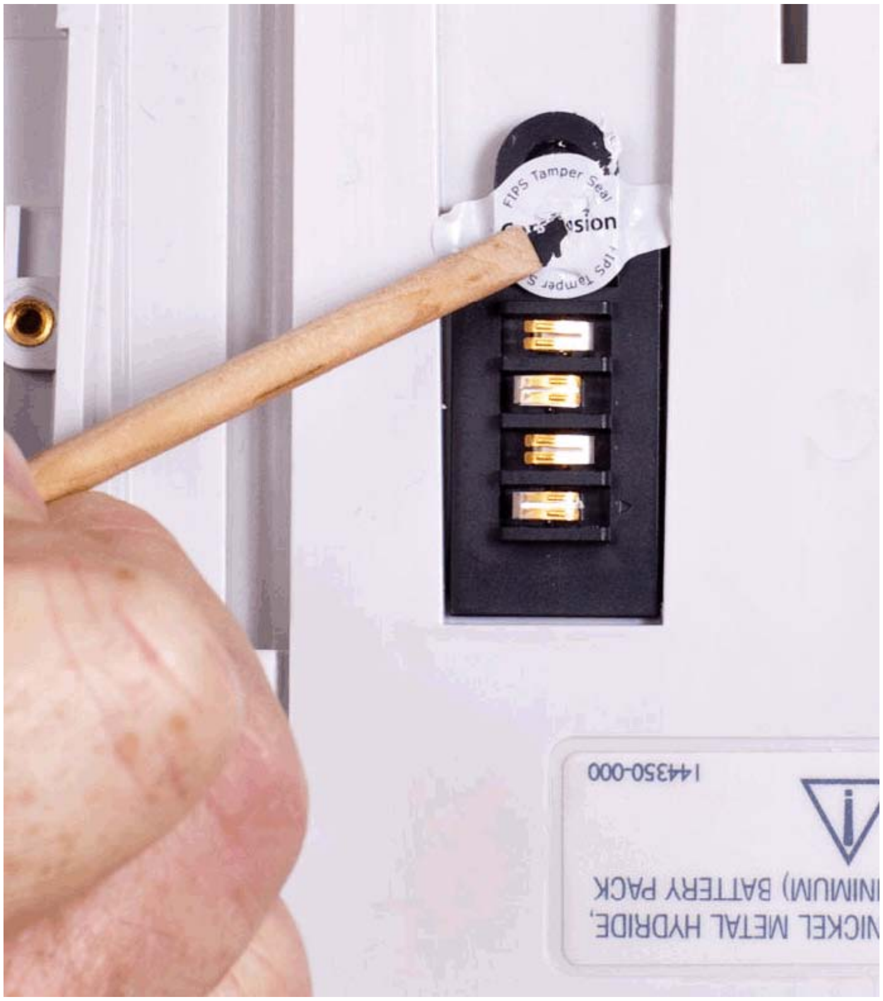


Figure 24 Remove seal over battery connector screw

5. Scrape off any of the remaining seals that are on the flat surfaces using the orange stick, leaving no portion of the tamper-evident seal present (Figure 25).

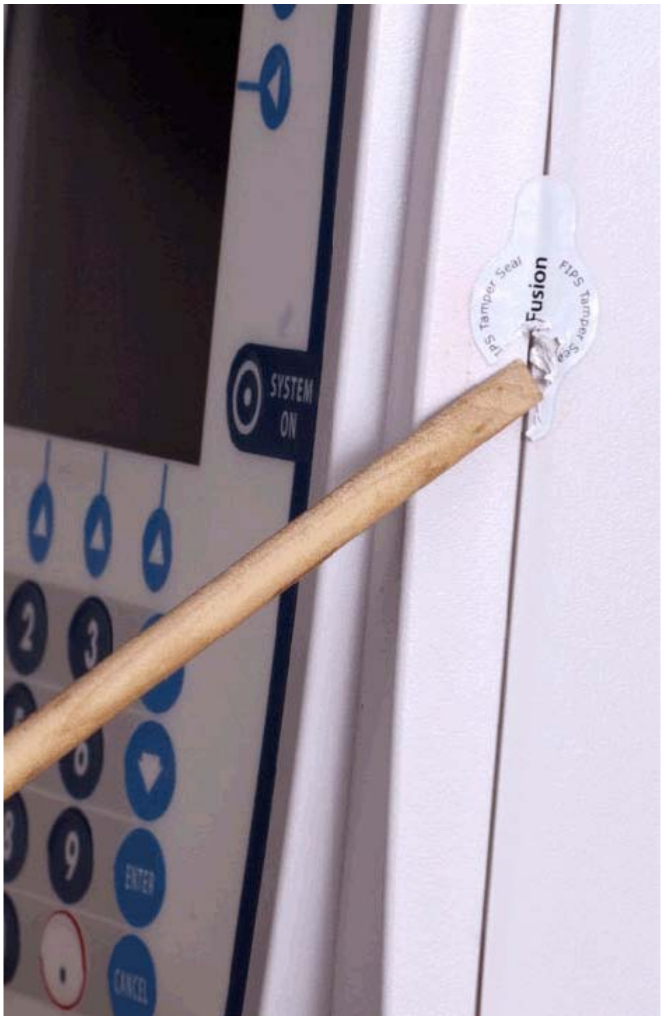


Figure 25 Leave no portion of seal remaining

Copyright Carefusion 2011. May be reproduced only in its original entirety [without revision].

6. Clean adhesive residue from the areas where the seals were removed with a soft cloth. Wipe clean with a soft cloth or a cotton tip applicator dampened with 70% IPA (Figure 26).

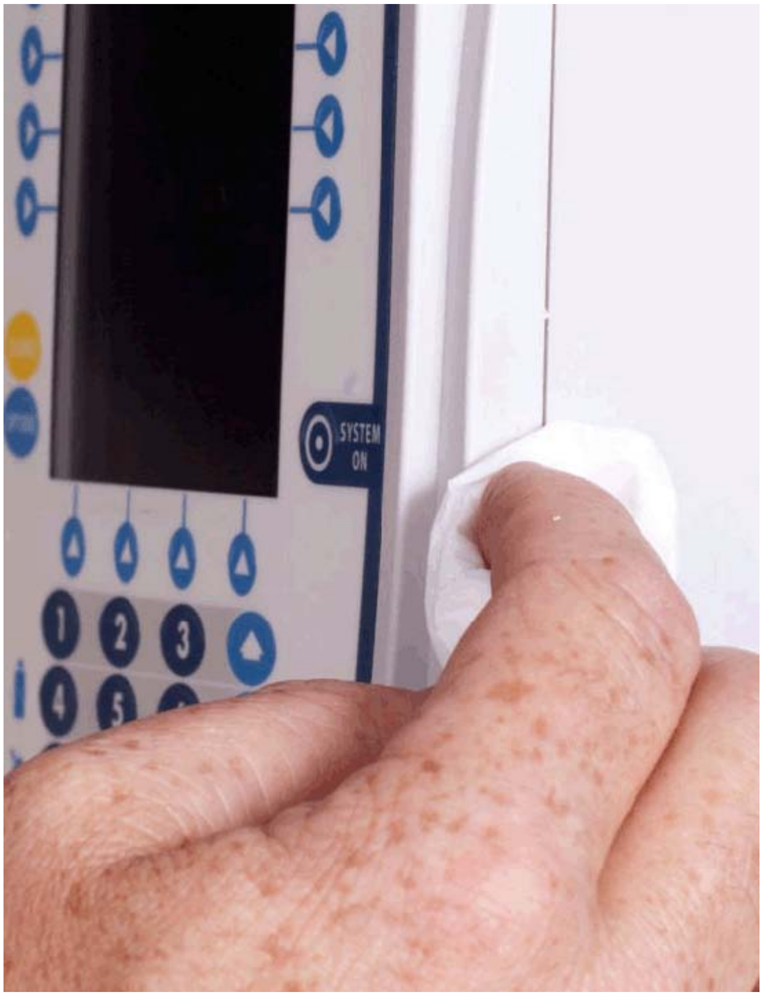


Figure 26 Clean residue with a soft cloth

NOTE: This concludes the tamper-evident seal removal process. Any remaining alcohol should be allowed to dry before new tamper-evident seals are applied.

Copyright Carefusion 2011. May be reproduced only in its original entirety [without revision].

8.3. Signs of Tampered Seals

The Alaris® PCU should be inspected on a regularly scheduled basis determined by the security officer of your hospital. If an Alaris® PCU has been verified as tampered with, the hospital security officer should be alerted to the situation. Because hospital network configurations may vary, this breach of security should be evaluated by the security officer and appropriate action should be taken. For assistance with CSP reconfiguration on the Alaris® System, please consult with CareFusion technical support.

Below are some examples of tampered seals.

- The tamper-evident seal has been sliced through the groove with a razor or other sharp object (Figure 27).

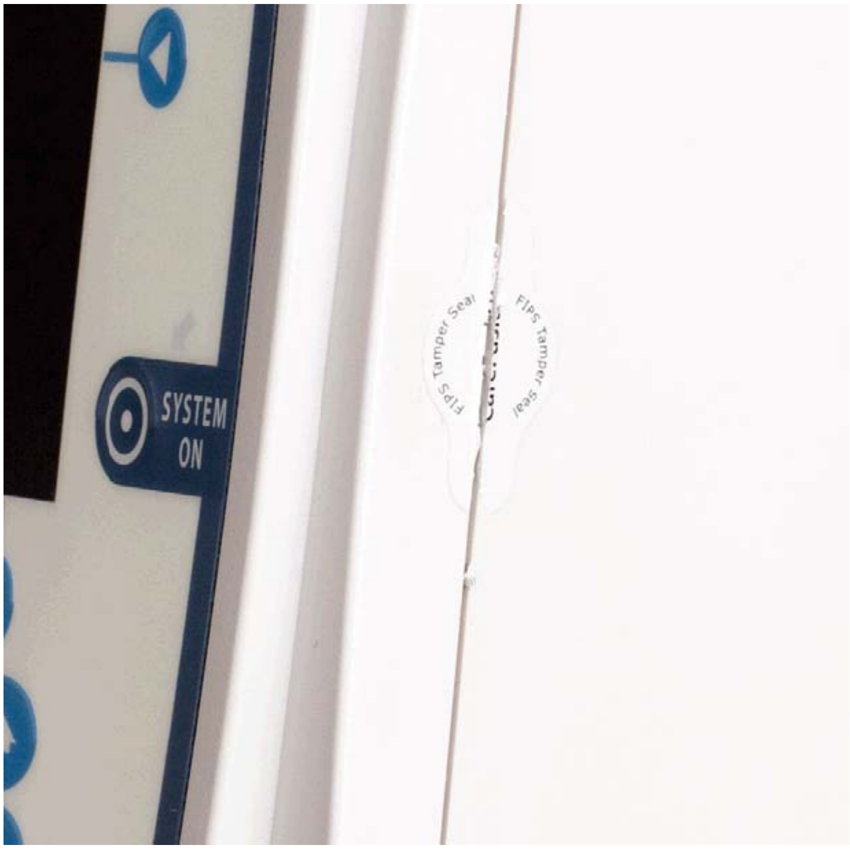


Figure 27 Seal has been sliced through

Copyright Carefusion 2011. May be reproduced only in its original entirety [without revision].

- The tamper-evident seal has been gouged out and pieces of it have been removed from the screw head (Figure 28).

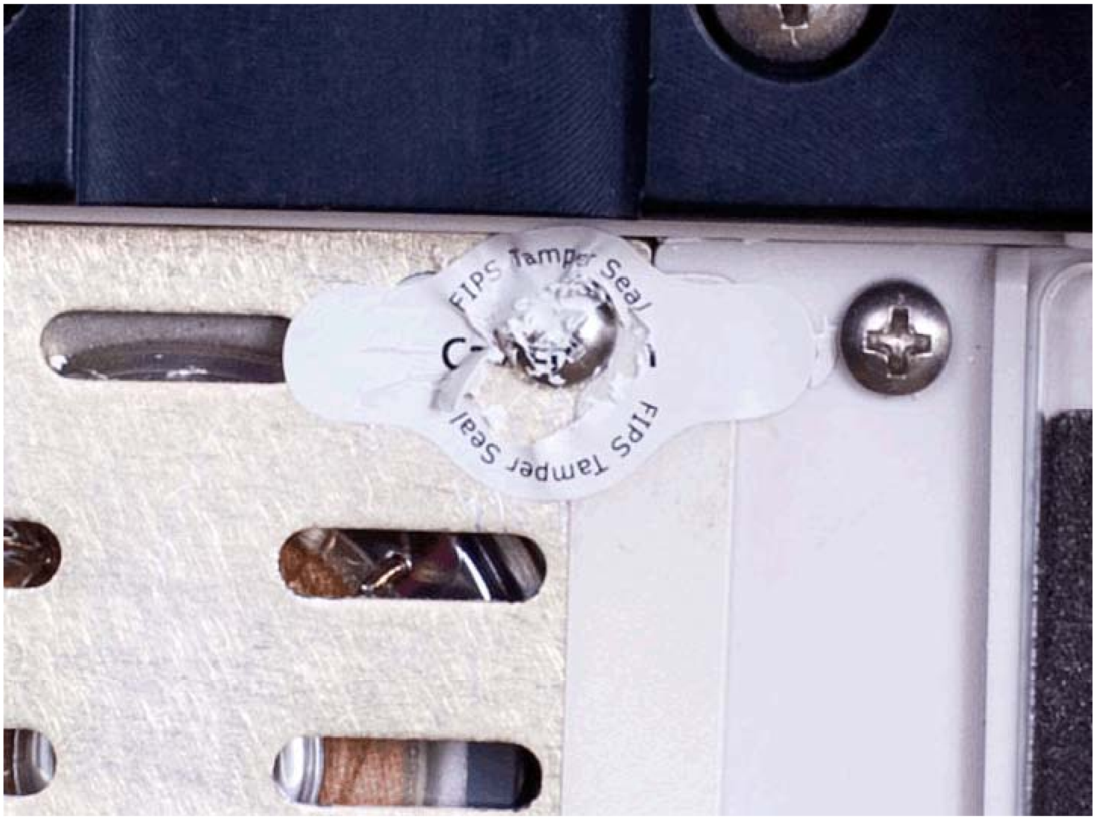


Figure 28 Seal has been gouged out

Copyright Carefusion 2011. May be reproduced only in its original entirety [without revision].

- The tamper-evident seal is showing signs that attempts to peel it off have occurred (Figure 29).

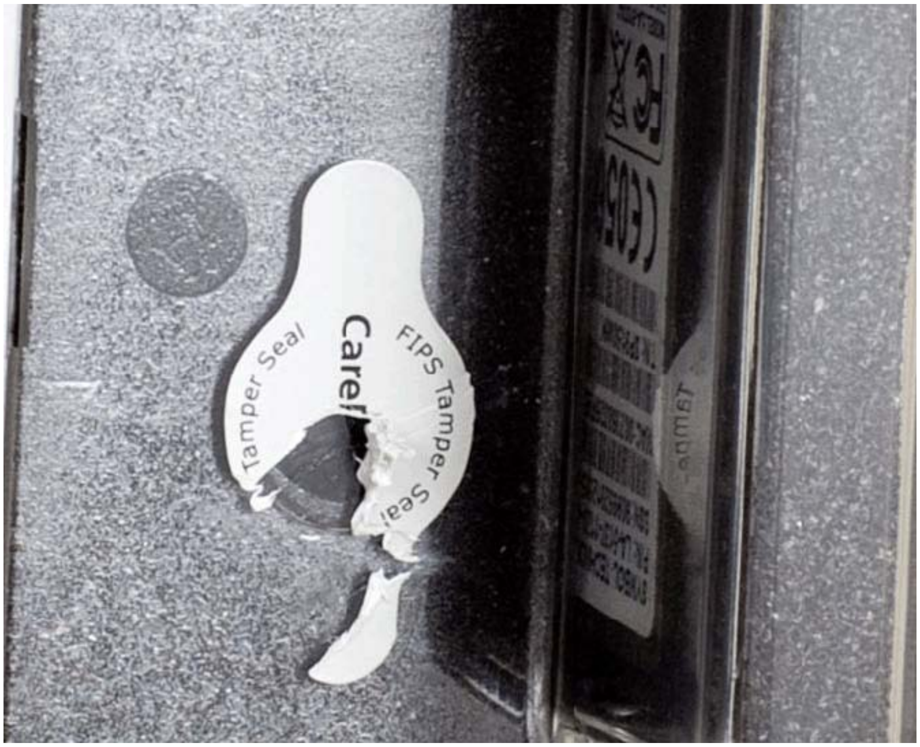


Figure 29 Seal has been partially peeled off from the device

- The tamper-evident seal has not been applied correctly and is not FIPS compliant (Figure 30). It is necessary that an incorrectly applied tamper-evident seal be removed and a new one be applied correctly. The device needs to be zeroized anytime a tamper-evident seal is replaced.

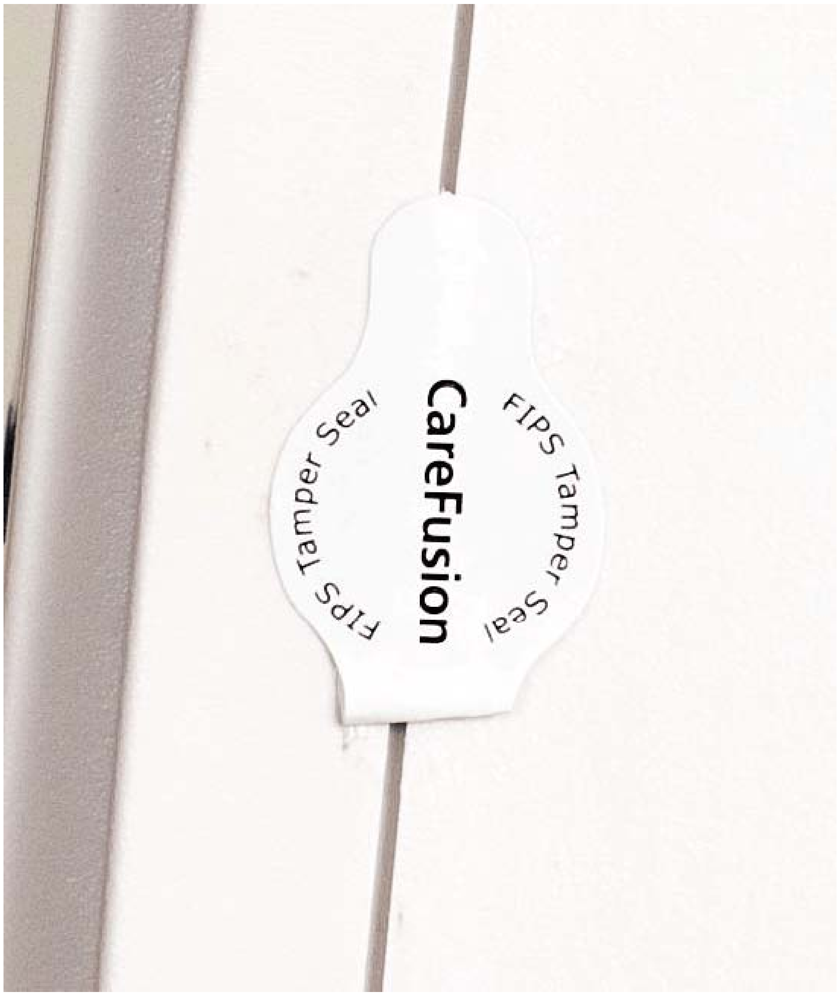


Figure 30 Seal has not been applied correctly; not FIPS compliant

Copyright Carefusion 2011. May be reproduced only in its original entirety [without revision].