Manufacturer Disclosure Statement for Medical Device Security – MDS²

SECTION 1

Device Category	Manufacturer	Document ID	Document Release Date
	Beckman Coulter		
Device Model: DXC700AU	Software Revision: 1.07	Software Release Date: 5-Feb-18	

Manufacturer or Representative Contact Information:	Company Name: Beckman Coulter	Manufacturer Contact Information
	Representative Name/Position	Beckman Coulter Japan 454-32 Higashino, Nagaizumi-cho, Sunto-gun Sgizuoka 411-0931, Japan

MANAGEMENT OF ELECTRONIC PROTECTED HEALTH INFORMATION (ePHI)	Yes No N/A	Note #
1. Can this device transmit or maintain electronic Protected Health Information (ePHI)?	Yes	__#1_
2. Types of ePHI data elements that can be maintained by the device:		
a. Demographic (e.g., name, address, location, unique identification number)?	Yes	__#1_
b. Medical record (e.g., medical record #, account #, test or treatment date, device identification number)?	Yes	__#1_
c. Diagnostic/therapeutic (e.g., photo/radiograph, test results, or physiologic data with identifying characteristics)?	Yes	__#1_
d. Open, unstructured text entered by device user/operator?	Yes	__#1_
3. Maintaining ePHI - Can the device		
a. Maintain ePHI temporarily in volatile memory (i.e., until cleared on by power-off or reset)?	No	_____
b. Store ePHI persistently on local media?	Yes	__#1_
c. Import/export ePHI with other systems?	Yes	__#1_
4. Mechanisms used for the transmitting, importing/exporting of ePHI – Can the device		
a. Display ePHI (e.g., video display)?	Yes	__#1_
b. Generate hardcopy reports or images containing ePHI?	Yes	__#1_
c. Retrieve ePHI from or record ePHI to removable media (e.g., disk, DVD, CD-ROM, tape, CF/SD card, memory stick)?	Yes	__#1_
d. Transmit/receive or import/export ePHI via dedicated cable connection (e.g., IEEE 1073, serial port, USB, FireWire)?	Yes	__#1_
e. Transmit/receive ePHI via a network connection (e.g., LAN, WAN, VPN, intranet, Internet)?	Yes	__#1_
f. Transmit/receive ePHI via an integrated wireless connection (e.g. WiFi, Bluetooth, infrared)?	No	_____
g. Other? _____		

ADMINISTRATIVE SAFEGUARDS	Yes No N/A	Note #
5. Does manufacturer offer operator and technical support training or documentation on device security features?	Yes	_____
6. What underlying operating system(s) (including version number) are used by the device? Windows 7	Yes	_____

PHYSICAL SAFEGUARDS	Yes No N/A	Note #
7. Are all device components maintaining ePHI (other than removable media) physically secure (i.e. cannot remove without tools)?	No	_____
8. Does the device have an integral data backup capability (i.e., backup onto removable media like tape, disk)?	No	_____
9. Can the device boot from uncontrolled or removable media (i.e., a source other than an internal drive or memory component)?	Yes	_____

TECHNICAL SAFEGUARDS	Yes No N/A	Note #
10. Can software or hardware not authorized by the device manufacturer be installed on the device without the use of tools?	Yes	_____
11. Can the device be serviced remotely (i.e., maintenance activities performed by service person via network or remote connection)?		_____
a. Can the device restrict remote access to specific devices or network locations (e.g., specific IP addresses)?	Yes	_____
b. Can the device provide an audit trail of remote-service activity?	No	_____
c. Can security patches or other software be installed remotely?	No	_____
12. Level of owner/operator service access to device operating system: Can the device owner/operator		
a. Apply device manufacturer-validated security patches?	No	_____
b. Install or update antivirus software?	No	__#2_
c. Update virus definitions on manufacturer-installed antivirus software?	No	__#2_
d. Obtain administrative privileges (e.g. access operating system or application via local root or admin account)?	No	_____
13. Does the device support user/operator specific username and password?	Yes	__#3_
14. Does the system force reauthorization after a predetermined length of inactivity (e.g., auto logoff, session lock)?	Yes	_____

© Copyright 2008 by the National Electrical Manufacturers Association and
the Healthcare Information and Management Systems Society.

Manufacturer Disclosure Statement for Medical Device Security – MDS²

SECTION 1

Device Category	Manufacturer	Document ID	Document Release Date
	Beckman Coulter		
Device Model DXC700AU	Software Revision 1.07	Software Release Date	5-Feb-18

Manufacturer or Representative Contact Information:	Company Name Beckman Coulter	Manufacturer Contact Information
	Representative Name/Position	

15. Events recorded in device audit trail (e.g., user, date/time, action taken): Can the audit trail record.....		
a. Login and logout by users/operators?.....	Yes	_____
b. Viewing of ePHI?.....	No	_____
c. Creation, modification or deletion of ePHI?.....	Yes	_____
d. Import/export or transmittal/receipt of ePHI?.....	No	_____
16. Does the device incorporate an emergency access (“break-glass”) feature that is logged?.....	No	_____
17. Can the device maintain ePHI during power service interruptions?.....	Yes	_____
18. Controls when exchanging ePHI with other devices:.....		
a. Transmitted only via a point-to-point dedicated cable?.....	No	_____
b. Encrypted prior to transmission via a network or removable media?.....	No	_____
c. Restricted to a fixed list of network destinations.....	No	_____
19. Does the device ensure the integrity of the ePHI data with implicit or explicit error detection/correction technology?.....	No	_____

Other Security Considerations

© Copyright 2008 by the National Electrical Manufacturers Association and
the Healthcare Information and Management Systems Society.

Manufacturer Disclosure Statement for Medical Device Security – MDS²

SECTION 1

Device Category		Manufacturer		Document ID	Document Release Date
		Beckman Coulter			
Device Model	DXC700AU	Software Revision	1.07	Software Release Date	5-Feb-18

Manufacturer or Representative Contact Information:	Company Name Beckman Coulter	Manufacturer Contact Information
	Representative Name/Position	

SECTION 2

EXPLANATORY NOTES (from questions 1 - 19)

IMPORTANT: Refer to Section 2.2.2 of this standard for the proper interpretation of information requested in this form

Note #1: The DxC 700 AU instrument operates using "Sample ID" and associates test results with the Sample ID. If patient demographic data is transmitted to the DxC 700 AU instrument from LIS, then that demographic data is available to view on the DxC 700 AU user interface and to print on patient reports. Patient reports can be exported to removable media. The Patient Information Record consists of the following demographic information: Sample ID, Sex, Age, and free comment. The DxC 700 AU instrument doesn't have the treatment date, it only has the test analyzed date.

Note #2: McAfee's Application Control (Whitelisting) prevents any malicious software from executing. Only field service engineers can install or update ant-virus software.

Note #3: Only a single configurable password is available for the administrative function (Administrative password is required for the following operations: Service functions.).

© Copyright 2008 by the National Electrical Manufacturers Association and
the Healthcare Information and Management Systems Society.