Manufacturer Disclosure Statement for Medical Device Security – MDS²

Manufacturer Disclosure Statement for Medical Device Security – MDS²

DEVICE DESCRIPTION

Device Category	Manufacturer	Document ID	Document Release Date
Point of Care Blood analysis Medical Device	**Epocal Inc.**	**51009991, Rev. 04**	**December 2019**

Device Model	Software Revision	Software Release Date
epoc Blood Analysis System	**epoc System v3.31.0** **epoc Host Software v3.31.3** **epoc Reader Firmware v2.2.12.1** **Sensor Configuration 35.3**	**October 2019**

	Company Name	Manufacturer Contact Information
Manufacturer or Representative Contact Information	**Siemens Healthcare Diagnostics Inc.**	**Epocal Inc.** **2060 Walkley Road** **Ottawa, ON K1G 3P5 Canada** **Tel.: +1-613-738-6192** **Fax: +1-613-738-6195**
	Representative Name/Position **Emergo Europe** **Prinsessegracht 20, 2514 AP** **The Hague, Netherlands** **service@emergogroup.com**	

Intended use of device in network-connected environment:

The **epoc Blood Analysis System** is a portable point-of-care blood analyzer used for quantitative in vitro diagnostic testing of whole-blood samples. The epoc system is intended to be used by trained medical professionals at a patient's bedside or in a laboratory or other clinical environment. The following are some of the epoc System's primary features:

- The epoc System measures blood gases, electrolytes, metabolites, and hematology using fresh whole blood at the patient's bedside in less than one minute after sample introduction.
- The epoc System can be customized to support various workflows in different clinical environments.
- The epoc System is wireless and can easily integrate with a data-management system to centrally manage devices across the entire institution and interface with the facility's LIS/HIS/EMR.

The epoc System comprises three major subsystems: epoc Host, epoc Reader, and epoc Test Cards.

epoc Reader:	The epoc Reader is a portable, battery-powered device used in conjunction with the epoc Host and Test Card to perform electrical measurements to produce blood test results.
epoc Host:	The epoc Host is a dedicated-use handheld mobile computer that runs the epoc Host software application. The epoc Host provides the primary user interface and calculates analytical values from sensor signals sent by the epoc Reader over a Bluetooth connection. The epoc Host runs specialized, user-friendly, highly configurable software that guides users through the testing process and can connect to a facility's existing wireless network to synchronize with a compatible data management
epoc Test Card:	The epoc Test Cards are single-use, individually wrapped devices that are used in conjunction with the epoc Reader and Host to produce blood test results. The Test Card contains electrochemical sensors, calibration fluid and fluidic channels, and an optical test chamber to accurately measure blood gas, electrolyte, metabolite, and hematology analyte concentrations in whole-blood samples.

Manufacturer Disclosure Statement for Medical Device Security – MDS²

MANAGEMENT OF PRIVATE DATA			
Refer to Section 2.3.2 of the standard Manufacturer Disclosure Statement for Medical Device Security (MDS²) issued by National Electrical Manufacturers Association and the Healthcare Information and Management Systems Society in 2013 for the proper interpretation of information requested in this form.		**Yes, No, N/A,** or **See Note**	**#**
A	Can this device display, transmit, or maintain private data (including electronic Protected Health Information [ePHI])?	**Yes**	
B	Types of private data elements that can be maintained by the device:		
B1	Demographic (e.g., name, address, location, unique identification number)?	**Yes**	
B2	Medical record (e.g., medical record #, account #, test or treatment date, device identification number)?	**Yes**	
B3	Diagnostic/therapeutic (e.g., photo/radiograph, test results, or physiologic data with identifying characteristics)?	**Yes**	
B4	Open, unstructured text entered by device user/operator?	**Yes**	
B5	Biometric data?	**No**	
B6	Personal financial information?	**No**	
C	Maintaining private data - Can the device:		
C1	Maintain private data temporarily in volatile memory (i.e., until cleared by power-off or reset)?	**Yes**	
C2	Store private data persistently on local media?	**Yes**	
C3	Import/export private data with other systems?	**Yes**	
C4	Maintain private data during power service interruptions?	**Yes**	
D	Mechanisms used for the transmitting, importing/exporting of private data – Can the device:		
D1	Display private data (e.g., video display, etc.)?	**Yes**	
D2	Generate hardcopy reports or images containing private data?	**Yes**	
D3	Retrieve private data from or record private data to removable media (e.g., disk, DVD, CD-ROM, tape, CF/SD card, memory stick, etc.)?	**No**	
D4	Transmit/receive or import/export private data via dedicated cable connection (e.g., IEEE 1073, serial port, USB, FireWire, etc.)?	**No**	
D5	Transmit/receive private data via a wired network connection (e.g., LAN, WAN, VPN, intranet, Internet, etc.)?	**No**	
D6	Transmit/receive private data via an integrated wireless network connection (e.g., WiFi, Bluetooth, infrared, etc.)?	**Yes**	
D7	Import private data via scanning?	**Yes**	
D8	Other?	**N/A**	
Management of Private Data Notes:			

Manufacturer Disclosure Statement for Medical Device Security – MDS²

SECURITY CAPABILITIES			
Refer to Section 2.3.2 of the standard Manufacturer Disclosure Statement for Medical Device Security (MDS²) issued by National Electrical Manufacturers Association and the Healthcare Information and Management Systems Society in 2013 for the proper interpretation of information requested in this form.		**Yes, No, N/A,** or **See Note**	**#**
1	**AUTOMATIC LOGOFF (ALOF)** The device's ability to prevent access and misuse by unauthorized users if device is left idle for a period of time.		
1-1	Can the device be configured to force reauthorization of logged-in user(s) after a predetermined length of inactivity (e.g., auto-logoff, session lock, password protected screen saver)?	**Yes**	
	1-1.1. Is the length of inactivity time before auto-logoff/screen lock user or administrator configurable? (Indicate time [fixed or configurable range] in notes.)	**Yes, See Note**	**1**
	1-1.2. Can auto-logoff/screen lock be manually invoked (e.g., via a shortcut key or proximity sensor, etc.) by the user?	**Yes**	
ALOF Notes:	Note 1: epoc Host: **Yes** – Inactivity timeout is administrator-configurable (1-5min).		
2	**AUDIT CONTROLS (AUDT)** The ability to reliably audit activity on the device.		
2-1	Can the medical device create an audit trail?	**Yes**	
2-2	Indicate which of the following events are recorded in the audit log:		
	2-2.1. Login/logout	**Yes**	
	2-2.2. Display/presentation of data	**No**	
	2-2.3. Creation/modification/deletion of data	**Yes**	
	2-2.4. Import/export of data from removable media	**No**	
	2-2.5. Receipt/transmission of data from/to external (e.g., network) connection 2-2.5.1. Remote service activity	**Yes. See Note**	**2**
	2-2.6. Other events? (describe in the notes section)	**Yes. See Note**	**3**
2-3	Indicate what information is used to identify individual events recorded in the audit log:		
	2-3.1. User ID	**No**	
	2-3.2. Date/time	**Yes**	
AUDT Notes:	Note 2: When connecting to a compatible data management system. Note 3: Power notifications, barcode scanning, major system events, system errors.		
3	**AUTHORIZATION (AUTH)** The ability of the device to determine the authorization of users.		

Manufacturer Disclosure Statement for Medical Device Security – MDS²

3-1	Can the device prevent access to unauthorized users through user login requirements or other mechanism?	**Yes**	
3-2	Can users be assigned different privilege levels within an application based on 'roles' (e.g., guests, regular users, power users, administrators, etc.)?	**Yes**	
3-3	Can the device owner/operator obtain unrestricted administrative privileges (e.g., access operating system or application via local root or admin account)?	**Yes. See Note**	**4**
AUTH Notes:	Note 4: Only the Host Administrator account can access the operating system and device configuration.		
4	**CONFIGURATION OF SECURITY FEATURES (CNFS)** The ability to configure/reconfigure device security capabilities to meet users' needs.		
4-1	Can the device owner/operator reconfigure product security capabilities?	**No**	
CNFS Notes:			
5	**CYBER SECURITY PRODUCT UPGRADES (CSUP)** The ability of on-site service staff, remote service staff, or authorized customer staff to install/upgrade device's security patches.		
5-1	Can relevant OS and device security patches be applied to the device as they become available?	**No**	
	5-1.1. Can security patches or other software be installed remotely?	**No. See Note**	**5**
CSUP Notes:	Note 5: Siemens Healthineers releases software for the epoc Blood Analysis System twice yearly. These updates include application updates and, if available, appropriate operating system updates..		
6	**HEALTH DATA DE-IDENTIFICATION (DIDT)** The ability of the device to directly remove information that allows identification of a person.		
6-1	Does the device provide an integral capability to de-identify private data?	**Yes. See Note.**	**6**
DIDT notes:	Note 6: The Device provides the ability to delete individual or all test records based on filtering criteria.		
7	**DATA BACKUP AND DISASTER RECOVERY (DTBK)** The ability to recover after damage or destruction of device data, hardware, or software.		
7-1	Does the device have an integral data backup capability (i.e., backup to remote storage or removable media such as tape, disk)?	**No. See Note**	**7**
DTBK Notes	Note 7: The epoc Host cannot back up to removable media but can transmit records to a compatible data management system for backup.		
8	**EMERGENCY ACCESS (EMRG)** The ability of device users to access private data in case of an emergency situation that requires immediate access to stored private data.		
8-1	Does the device incorporate an emergency access ("break-glass") feature?	**No**	
EMRG notes:			
9	**HEALTH DATA INTEGRITY AND AUTHENTICITY (IGAU)** How the device ensures that data processed by the device has not been altered or destroyed in an unauthorized manner and is from the originator.		
9-1	Does the device ensure the integrity of stored data with implicit or explicit error detection/correction technology?	**Yes**	
IGAU notes:			

Manufacturer Disclosure Statement for Medical Device Security – MDS²

10	**MALWARE DETECTION/PROTECTION (MLDP)** The ability of the device to effectively prevent, detect and remove malicious software (malware).		
10-1	Does the device support the use of anti-malware software (or other anti-malware mechanism)?	**No**	
	10-1.1. Can the user independently reconfigure antimalware settings?	**No**	
	10-1.2. Does notification of malware detection occur in the device user interface?	**No**	
	10-1.3. Can only manufacturer-authorized persons repair systems when malware has been detected?	**No**	
10-2	Can the device owner install or update anti-virus software?	**No**	
10-3	Can only manufacturer-authorized persons repair systems when malware has been detected?	**No**	
MLDP Notes:			
11	**NODE AUTHENTICATION (NAUT)** The ability of the device to authenticate communication partners/nodes.		
11-1	Does the device provide/support any means of node authentication that assures both the sender and the recipient of data are known to each other and are authorized to receive transferred information?	**No**	
NAUT Notes:			
12	**PERSON AUTHENTICATION (PAUT)** Ability of the device to authenticate users		
12-1	Does the device support user/operator-specific username(s) and password(s) for at least one user?	**Yes**	
	12-1.1. Does the device support unique user/operator-specific IDs and passwords for multiple users?	**Yes**	
12-2	Can the device be configured to authenticate users through an external authentication service (e.g., MS Active Directory, NDS, LDAP, etc.)?	**No**	
12-3	Can the device be configured to lock out a user after a certain number of unsuccessful logon attempts?	**Yes**	
12-4	Can default passwords be changed at/prior to installation?	**Yes**	
12-5	Are any shared user IDs used in this system?	**Yes**	
12-6	Can the device be configured to enforce creation of user account passwords that meet established complexity rules?	**Yes**	
12-7	Can the device be configured so that account passwords expire periodically?	**Yes**	
PAUT Notes:			
13	**PHYSICAL LOCKS (PLOK)** Physical locks can prevent unauthorized users with physical access to the device from compromising the integrity and confidentiality of private data stored on the device or on removable media.		
13-1	Are all device components maintaining private data (other than removable media) physically secure (i.e., cannot be removed without tools)?	**No, See Note**	**8**
PLOK Notes	Note 8: The epoc Host is a mobile device that is not physically secured.		
14	**ROADMAP FOR THIRD PARTY COMPONENTS IN DEVICE LIFE CYCLE (RDMP)** Manufacturer's plans for security support of 3rd party components within device life cycle.		

Manufacturer Disclosure Statement for Medical Device Security – MDS²

14-1	In the notes section, list the provided or required (separately purchased and/or delivered) operating system(s) - including version number(s).	**See Note**	**9**
14-2	Is a list of other third party applications provided by the manufacturer available?	**Yes**	
RDMP notes:	Note 9: Microsoft Embedded Handheld v6.5 Zebra Wireless Fusion v3.00		
15	**SYSTEM AND APPLICATION HARDENING (SAHD)** The device's resistance to cyber attacks and malware.		
15-1	Does the device employ any hardening measures? Please indicate in the notes the level of conformance to any industry-recognized hardening standards.	**No**	
15-2	Does the device employ any mechanism (e.g., release-specific hash key, checksums, etc.) to ensure the installed program/update is the manufacturer-authorized program or software update?	**Yes**	
15-3	Does the device have external communication capability (e.g., network, modem, etc.)?	**Yes**	
15-4	Does the file system allow the implementation of file-level access controls (e.g., New Technology File System (NTFS) for MS Windows platforms)?	**No**	
15-5	Are all accounts which are not required for the intended use of the device disabled or deleted, for both users and applications?	**Yes**	
15-6	Are all shared resources (e.g., file shares) which are not required for the intended use of the device, disabled?	**See Note**	**10**
15-7	Are all communication ports which are not required for the intended use of the device closed/disabled?	**See Note**	**10**
15-8	Are all services (e.g., telnet, file transfer protocol [FTP], internet information server [IIS], etc.), which are not required for the intended use of the device deleted/disabled?	**See Note**	**10**
15-9	Are all applications (COTS applications as well as OS-included applications, e.g., MS Internet Explorer, etc.) which are not required for the intended use of the device deleted/disabled?	**See Note**	**10**
15-10	Can the device boot from uncontrolled or removable media (i.e., a source other than an internal drive or memory component)?	**No**	
15-11	Can software or hardware not authorized by the device manufacturer be installed on the device without the use of tools?	**No**	
SAHD Notes:	Note 10: Host Operators are restricted and cannot access the Operating System or other unnecessary resources. Only Host Administrators can access the Operating System and its resources.		
16	**SECURITY GUIDANCE (SGUD)** The availability of security guidance for operator and administrator of the system and manufacturer sales and service.		
16-1	Are security-related features documented for the device user?	**Yes**	
16-2	Are instructions available for device/media sanitization (i.e., instructions for how to achieve the permanent deletion of personal or other sensitive data)?	**Yes.** **See Note**	**11**
SGUD notes:	Note 11: Refer to epoc System Manual.		
17	**HEALTH DATA STORAGE CONFIDENTIALITY (STCF)** The ability of the device to ensure unauthorized access does not compromise the integrity and confidentiality of private data stored on device or removable media.		
17-1	Can the device encrypt data at rest?	**Yes**	
STCF Notes:			

Manufacturer Disclosure Statement for Medical Device Security – MDS²

18	**TRANSMISSION CONFIDENTIALITY (TXCF)** The ability of the device to ensure the confidentiality of transmitted private data.		
18-1	Can private data be transmitted only via a point-to-point dedicated cable?	**No**	
18-2	Is private data encrypted prior to transmission via a network or removable media? (If yes, indicate in the notes which encryption standard is implemented.)	**No**	
18-3	Is private data transmission restricted to a fixed list of network destinations?	**Yes**	
TXCF Notes:			
19	**TRANSMISSION INTEGRITY (TXIG)** The ability of the device to ensure the integrity of transmitted private data.		
19-1	Does the device support any mechanism intended to ensure data is not modified during transmission? (If yes, describe in the notes section how this is achieved.)	**No**	
TXIG Notes:			
20	**OTHER SECURITY CONSIDERATIONS (OTHR)** Additional security considerations/notes regarding medical device security.		
20-1	Can the device be serviced remotely?	**No**	
20-2	Can the device restrict remote access to/from specified devices or users or network locations (e.g., specific IP addresses)?	**Yes**	
	20-2.1. Can the device be configured to require the local user to accept or initiate remote access?	**N/A. See Note**	**12**
OTHR Notes:	Note 12: The epoc System does not support remote access.		

Questions

If you have any questions, please contact Siemens Healthineers Remote Services Center or your local Siemens technical support representative.

Manufactured by:
Epocal Inc.
2060 Walkley Rd.
Ottawa, ON K1G 3P5 Canada
Tel.: +1-613-738-6192
Fax: +1-613-738-6195
siemens.com/epoc

Authorized Representative:
Emergo Europe
Prinsessegracht 20, 2514 AP
The Hague, Netherlands
service@emergogroup.com

51009991 Rev.: 04 2019-12