

# Manufacturer Disclosure Statement for Medical Device Security (MDS2)

For Ambu® aBox™ 2  
and aView™ 2 Advance  
with Software 2.4

**Ambu**



**MDS2 for Ambu A/S displaying and processing units with software version 2.4**

| Question ID | Question   | Displaying and processing unit  | Notes                             | IEC TR 80001-2-2: 2012 | NIST SP 800-53 Rev. 4 | ISO 27002: 2013 |
|-------------|--|---|-----------------------------------|------------------------|-----------------------|-----------------|
| DOC-1       | Manufacturer name  | AMBU A/S  | -                                 |                        |                       |                 |
| DOC-2       | Device description   | Non-sterile, reusable monitor, intended to display live imaging data from Ambu visualization devices.                 | -                                 |                        |                       |                 |
| DOC-3       | Device model   | aView 2 Advance and aBox 2 with software version 2.4  | -                                 |                        |                       |                 |
| DOC-4       | Document ID  | PUB-001997  | -                                 |                        |                       |                 |
| DOC-5       | Manufacturer contact information   | Phone: +45 7225 2000<br>Mail: ambu@ambu.com   | -                                 |                        |                       |                 |
| DOC-6       | Intended use of device in network-connected environment  | The device supports transferring images in PNG, JPG and DICOM, videos in MP4 and DICOM and data in clear text format. | -                                 |                        |                       |                 |
| DOC-7       | Document release date  | 2024-10-26  | -                                 |                        |                       |                 |
| DOC-8       | Coordinated Vulnerability Disclosure: Does the manufacturer have a vulnerability disclosure program for this device?                       | No  | -                                 |                        |                       |                 |
| DOC-9       | ISAO: Is the manufacturer part of an Information Sharing and Analysis Organization?  | No  | -                                 |                        |                       |                 |
| DOC-10      | Diagram: Is a network or data flow diagram available that indicates connections to other system components or expected external resources? | Yes   | Available upon request.           |                        |                       |                 |
| DOC-11      | SaMD: Is the device Software as a Medical Device (i.e. software-only, no hardware)?  | No  | It is SiMD.                       |                        |                       |                 |
| DOC-11.1    | Does the SaMD contain an operating system?   | N/A   | We deliver a whole system (SiMD). |                        |                       |                 |
| DOC-11.2    | Does the SaMD rely on an owner/operator provided operating system?   | N/A   | -                                 |                        |                       |                 |
| DOC-11.3    | Is the SaMD hosted by the manufacturer?  | N/A   | -                                 |                        |                       |                 |
| DOC-11.4    | Is the SaMD hosted by the customer?  | N/A   | -                                 |                        |                       |                 |

**MDS2 for Ambu A/S displaying and processing units with software version 2.4**

|          | <b>MANAGEMENT OF PERSONALLY IDENTIFIABLE INFORMATION</b>  | <b>Displaying and processing unit</b> | <b>Notes</b>   | <b>IEC TR 80001-2-2: 2012</b> | <b>NIST SP 800-53 Rev. 4</b> | <b>ISO 27002:2013</b> |
|----------|---|---------------------------------------|--|-------------------------------|------------------------------|-----------------------|
| MPII-1   | Can this device display, transmit, store, or modify personally identifiable information (e.g. electronic Protected Health Information (ePHI))?  | Yes                                   | The device can retrieve ePHI via a DICOM worklist and transfer it through DICOM export. The device can transfer ePHI to a SMB server.  |                               | AR-2                         | A.15.1.4              |
| MPII-2   | Does the device maintain personally identifiable information?   | Yes                                   | The device can retrieve ePHI via a DICOM worklist and transfer it through DICOM export. The device can transfer ePHI to a SMB server.<br><br>ePHI is used as data in use in program memory. ePHI is persisted as data at rest in a database. |                               | AR-2                         | A.15.1.4              |
| MPII-2.1 | Does the device maintain personally identifiable information temporarily in volatile memory (i.e., until cleared by power-off or reset)?  | Yes                                   |  |                               | AR-2                         | A.15.1.4              |
| MPII-2.2 | Does the device store personally identifiable information persistently on internal media?   | Yes                                   |  |                               |                              |                       |
| MPII-2.3 | Is personally identifiable information preserved in the device's non-volatile memory until explicitly erased?   | Yes                                   |  |                               |                              |                       |
| MPII-2.4 | Does the device store personally identifiable information in a database?  | Yes                                   |  |                               |                              |                       |
| MPII-2.5 | Does the device allow configuration to automatically delete local personally identifiable information after it is stored to a long term solution?   | Yes                                   | Configurable mechanism for moving to trash bin after 3d, 1w, 4w, 12w + never.<br><br>Configurable mechanism for moving removing from trash bin after 3d, 1w, 4w, 12 w + never.   |                               | AR-2                         | A.15.1.4              |
| MPII-2.6 | Does the device import/export personally identifiable information with other systems (e.g., a wearable monitoring device might export personally identifiable information to a server)?                                       | Yes                                   | ePHI is transmitted as data in transit via DICOM protocol.   |                               | AR-2                         | A.15.1.4              |
| MPII-2.7 | Does the device maintain personally identifiable information when powered off, or during power service interruptions?   | Yes                                   | ePHI is persisted as data at rest in a database.   |                               | AR-2                         | A.15.1.4              |
| MPII-2.8 | Does the device allow the internal media to be removed by a service technician (e.g., for separate destruction or customer retention)?  | Yes                                   | Internal SSD is on aBox 2 full disk encrypted and both aView 2 Advance and aBox 2 are ATA-locked. The SSD can be removed for destruction and retention.  |                               |                              |                       |
| MPII-2.9 | Does the device allow personally identifiable information records be stored in a separate location from the device's operating system (i.e. secondary internal drive, alternate drive partition, or remote storage location)? | Yes                                   | The ePHI is allowed to be stored on USB flash drives and on remote server via DICOM or SMB export.   |                               | AR-2                         | A.15.1.4              |

**MDS2 for Ambu A/S displaying and processing units with software version 2.4**

|                                   |  |     |   |  |      |          |
|-----------------------------------|--|-----|---|--|------|----------|
| MPII-3                            | Does the device have mechanisms used for the transmitting, importing/exporting of personally identifiable information?   | Yes | The device is able to retrieve worklists in DICOM format and export images/videos in DICOM format.  |  | AR-2 | A.15.1.4 |
| MPII-3.1                          | Does the device display personally identifiable information (e.g., video display, etc.)?   | Yes | ePHI is shown in internal and external screens.   |  | AR-2 | A.15.1.4 |
| MPII-3.2                          | Does the device generate hardcopy reports or images containing personally identifiable information?  | No  | –   |  | AR-2 | A.15.1.4 |
| MPII-3.3                          | Does the device retrieve personally identifiable information from or record personally identifiable information to removable media (e.g., removable-HDD, USB memory, DVD-R/RW, CD-R/RW, tape, CF/SD card, memory stick, etc.)? | No  | Recording is only to internal SSD.  |  | AR-2 | A.15.1.4 |
| MPII-3.4                          | Does the device transmit/receive or import/export personally identifiable information via dedicated cable connection (e.g., RS-232, RS-423, USB, FireWire, etc.)?  | Yes | ePHI is transmitted as data in transit via DICOM protocol over USB.   |  | AR-2 | A.15.1.4 |
| MPII-3.5                          | Does the device transmit/receive personally identifiable information via a wired network connection (e.g., RJ45, fiber optic, etc.)?   | Yes | ePHI is transmitted as data in transit over RJ-45 via DICOM protocol to PACS server or to SMB server.   |  | AR-2 | A.15.1.4 |
| MPII-3.6                          | Does the device transmit/receive personally identifiable information via a wireless network connection (e.g., WiFi, Bluetooth, NFC, infrared, cellular, etc.)?   | Yes | ePHI is transmitted as data in transit over Wi-Fi via DICOM protocol to PACS server or to SMB server.   |  | AR-2 | A.15.1.4 |
| MPII-3.7                          | Does the device transmit/receive personally identifiable information over an external network (e.g., Internet)?  | Yes | The protocols used for transmitting/receiving of personal identifiable information supports communication over external networks. The user is recommended to only use the DICOM and SMB on a private network. |  | AR-2 | A.15.1.4 |
| MPII-3.8                          | Does the device import personally identifiable information via scanning a document?  | No  | –   |  |      |          |
| MPII-3.9                          | Does the device transmit/receive personally identifiable information via a proprietary protocol?   | No  | –   |  |      |          |
| MPII-3.10                         | Does the device use any other mechanism to transmit, import or export personally identifiable information?   | No  | –   |  | AR-2 | A.15.1.4 |
| Management of Private Data notes: |  |     |   |  | AR-2 | A.15.1.4 |

**MDS2 for Ambu A/S displaying and processing units with software version 2.4**

| <b>AUTOMATIC LOGOFF (ALOF)</b>   |   | <b>Displaying and processing unit</b> | <b>Notes</b>   | <b>IEC TR 80001-2-2: 2012</b> | <b>NIST SP 800-53 Rev. 4</b> | <b>ISO 27002: 2013</b>                                  |
|--|---|---------------------------------------|--|-------------------------------|------------------------------|---|
| The device's ability to prevent access and misuse by unauthorized users if device is left idle for a period of time. |   |                                       |  |                               |                              |   |
| ALOF-1   | Can the device be configured to force reauthorization of logged-in user(s) after a predetermined length of inactivity (e.g., auto-logout, session lock, password protected screen saver)? | Yes                                   | Administrator can configure this from 10 min to never.       | Section 5.1, ALOF             | AC-12                        | None  |
| ALOF-2   | Is the length of inactivity time before auto-logout/ screen lock user or administrator configurable?  | Yes                                   |  | Section 5.1, ALOF             | AC-11                        | A.11.2.8, A.11.2.9                                      |
| <b>AUDIT CONTROLS (AUDT)</b>   |   | <b>Displaying and processing unit</b> | <b>Notes</b>   | <b>IEC TR 80001-2-2: 2012</b> | <b>NIST SP 800-53 Rev. 4</b> | <b>ISO 27002: 2013</b>                                  |
| The ability to reliably audit activity on the device.  |   |                                       |  |                               |                              |   |
| AUDT-1   | Can the medical device create additional audit logs or reports beyond standard operating system logs?   | No                                    | -  | Section 5.2, AUDT             | AU-1                         | A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2 |
| AUDT-1.1   | Does the audit log record a USER ID?  | No                                    | -  |                               |                              |   |
| AUDT-1.2   | Does other personally identifiable information exist in the audit trail?  | No                                    | -  | Section 5.2, AUDT             | AU-2                         | None  |
| AUDT-2   | Are events recorded in an audit log?<br>If yes, indicate which of the following events are recorded in the audit log  | No                                    | -  | Section 5.2, AUDT             | AU-2                         | None  |
| AUDT-2.1   | Successful login/logout attempts?   | Yes                                   | Extractable from the audit log.                              | Section 5.2, AUDT             | AU-2                         | None  |
| AUDT-2.2   | Unsuccessful login/logout attempts?   | N/A                                   |  | Section 5.2, AUDT             | AU-2                         | None  |
| AUDT-2.3   | Modification of user privileges?  | Yes                                   | Extractable from the audit log.                              | Section 5.2, AUDT             | AU-2                         | None  |
| AUDT-2.4   | Creation/modification/deletion of users?  | Yes                                   | Extractable from the audit log.                              | Section 5.2, AUDT             | AU-2                         | None  |
| AUDT-2.5   | Presentation of clinical or PII data (e.g. display, print)?   | N/A                                   | -  | Section 5.2, AUDT             | AU-2                         | None  |
| AUDT-2.6   | Creation/modification/deletion of data?   | N/A                                   | -  | Section 5.2, AUDT             | AU-2                         | None  |
| AUDT-2.7   | Import/export of data from removable media (e.g. USB drive, external hard drive, DVD)?  | No                                    | The event of USB insertion is extractable on the device log. | Section 5.2, AUDT             | AU-2                         | None  |

**MDS2 for Ambu A/S displaying and processing units with software version 2.4**

|            |   |  |  |                   |      |      |
|------------|---|--|--|-------------------|------|------|
| AUDT-2.8   | Receipt/transmission of data or commands over a network or point-to-point connection?       | N/A  | –  | Section 5.2, AUDT | AU-2 | None |
| AUDT-2.8.1 | Remote or on-site support?  | N/A  | –  | Section 5.2, AUDT | AU-2 | None |
| AUDT-2.8.2 | Application Programming Interface (API) and similar activity?                               | N/A  | –  | Section 5.2, AUDT | AU-2 | None |
| AUDT-2.9   | Emergency access?   | N/A  | –  | Section 5.2, AUDT | AU-2 | None |
| AUDT-2.10  | Other events (e.g., software updates)?  | Yes  | Extractable from the audit log.            | Section 5.2, AUDT | AU-2 | None |
| AUDT-2.11  | Is the audit capability documented in more detail?  | The capability is described in the IFU section "User activity log" | –  | Section 5.2, AUDT | AU-2 | None |
| AUDT-3     | Can the owner/operator define or select which events are recorded in the audit log?         | No   | –  | Section 5.2, AUDT | AU-2 | None |
| AUDT-4     | Is a list of data attributes that are captured in the audit log for an event available?     | No   | –  | Section 5.2, AUDT | AU-2 | None |
| AUDT-4.1   | Does the audit log record date/time?  | All entries are prefixed with a ISO-8601 timestamp.                | –  | Section 5.2, AUDT | AU-2 | None |
| AUDT-4.1.1 | Can date and time be synchronized by Network Time Protocol (NTP) or equivalent time source? | No   | –  | Section 5.2, AUDT | AU-2 | None |
| AUDT-5     | Can audit log content be exported?  | The audit log can be exported to a USB flash drives.               | –  | Section 5.2, AUDT | AU-2 | None |
| AUDT-5.1   | Via physical media?   | The audit log can be exported to a USB flash drives.               | –  |                   |      |      |
| AUDT-5.2   | Via IHE Audit Trail and Node Authentication (ATNA) profile to SIEM?                         | No   | –  |                   |      |      |
| AUDT-5.3   | Via Other communications (e.g., external service device, mobile application)?               | No   | –  |                   |      |      |
| AUDT-5.4   | Are audit logs encrypted in transit or on storage media.                                    | No   | –  |                   |      |      |
| AUDT-6     | Can audit logs be monitored/reviewed by owner/operator?                                     | No   | –  |                   |      |      |
| AUDT-7     | Are audit logs protected from modification?   | No   | Device log is protected from modification. | Section 5.2, AUDT | AU-2 | None |
| AUDT-7.1   | Are audit logs protected from access?   | No   |  |                   |      |      |
| AUDT-8     | Can audit logs be analyzed by the device?   | No   | –  | Section 5.2, AUDT | AU-2 | None |

**MDS2 for Ambu A/S displaying and processing units with software version 2.4**

|  | <b>AUTHORIZATION (AUTH)</b>   | <b>Displaying and processing unit</b> | <b>Notes</b>   | <b>IEC TR 80001-2-2: 2012</b> | <b>NIST SP 800-53 Rev. 4</b> | <b>ISO 27002: 2013</b> |
|--|---|---------------------------------------|--|-------------------------------|------------------------------|------------------------|
| The ability of the device to determine the authorization of users. |   |                                       |  |                               |                              |                        |
| AUTH-1   | Does the device prevent access to unauthorized users through user login requirements or other mechanism?  | Yes                                   | Role based access control by username and password.  | Section 5.3, AUTH             | IA-2                         | A.9.2.1                |
| AUTH-1.1   | Can the device be configured to use federated credentials management of users for authorization (e.g., LDAP, OAuth)?  | No                                    | This is not currently supported.   | Section 5.3, AUTH             | IA-2                         | A.9.2.1                |
| AUTH-1.2   | Can the customer push group policies to the device (e.g., Active Directory)?  | No                                    |  | Section 5.3, AUTH             | IA-2                         | A.9.2.1                |
| AUTH-1.3   | Are any special groups, organizational units, or group policies required?   | No                                    |  | Section 5.3, AUTH             | IA-2                         | A.9.2.1                |
| AUTH-2   | Can users be assigned different privilege levels based on 'role' (e.g., user, administrator, and/or service, etc.)?   | Yes                                   | There is two different user types:<br>Administrator and Service technicians (Premade types)<br>Non-privilege users can be created/modified by administrators.              | Section 5.3, AUTH             | IA-2                         | A.9.2.1                |
| AUTH-3   | Can the device owner/operator grant themselves unrestricted administrative privileges (e.g., access operating system or application via local root or administrator account)? | No                                    | Only pre-made accounts are assigned privilege.   | Section 5.3, AUTH             | IA-2                         | A.9.2.1                |
| AUTH-4   | Does the device authorize or control all API access requests?   | No                                    | –  | Section 5.3, AUTH             | IA-2                         | A.9.2.1                |
| AUTH-5   | Does the device run in a restricted access mode, or 'kiosk mode', by default?   | Yes                                   | The device's application runs in a kiosk mode, where it is the only application available to the user. The user does not have direct access to the operating system layer. |                               |                              |                        |

**MDS2 for Ambu A/S displaying and processing units with software version 2.4**

|  | <b>CYBER SECURITY PRODUCT UPGRADES (CSUP)</b>   | <b>Displaying and processing unit</b> | <b>Notes</b>   | <b>IEC TR 80001- 2-2: 2012</b> | <b>NIST SP 800-53 Rev. 4</b> | <b>ISO 27002: 2013</b> |
|--|---|---------------------------------------|--|--------------------------------|------------------------------|------------------------|
| The ability of on-site service staff, remote service staff, or authorized customer staff to install/upgrade device's security patches. |   |                                       |  |                                |                              |                        |
| CSUP-1   | Does the device contain any software or firmware which may require security updates during its operational life, either from the device manufacturer or from a third-party manufacturer of the software/firmware? If no, answer "N/A" to questions in this section. | Yes                                   | Software is always released as one self-contained bundle.  |                                |                              |                        |
| CSUP-2   | Does the device contain an Operating System? If yes, complete 2.1-2.4.  | Yes                                   | -  |                                |                              |                        |
| CSUP-2.1   | Does the device documentation provide instructions for owner/operator installation of patches or software updates?  | Yes                                   | All needed patches are controlled from Ambu, and released as one self-contained bundle.  |                                |                              |                        |
| CSUP-2.2   | Does the device require vendor or vendor-authorized service to install patches or software updates?   | Yes                                   | For the OTA it is required that the device is registered in order to be update/patched. For USB it is required that a signed update package is provided to the hospital from Ambu on a USB flash drives. This is contained in the self-contained bundle, see CSUP-1. |                                |                              |                        |
| CSUP-2.3   | Does the device have the capability to receive remote installation of patches or software updates?  | Yes                                   | Yes, the device can receive patches from the Ambu OTA service (pull only).   |                                |                              |                        |
| CSUP-2.4   | Does the medical device manufacturer allow security updates from any third-party manufacturers (e.g., Microsoft) to be installed without approval from the manufacturer?  | No                                    | -  |                                |                              |                        |
| CSUP-3   | Does the device contain Drivers and Firmware? If yes, complete 3.1-3.4.   | Yes                                   | Software is always released as one self-contained bundle.  |                                |                              |                        |
| CSUP-3.1   | Does the device documentation provide instructions for owner/operator installation of patches or software updates?  | No                                    | -  |                                |                              |                        |

**MDS2 for Ambu A/S displaying and processing units with software version 2.4**

|          |  |     |  |  |  |  |
|----------|--|-----|--|--|--|--|
| CSUP-3.2 | Does the device require vendor or vendor-authorized service to install patches or software updates?  | Yes | For the OTA it is required that the device is registered in order to be updated/ patched. For USB it is required that a signed update package is provided to the hospital from Ambu on a USB flash drives. This is contained in the self-contained bundle, see CSUP-1. |  |  |  |
| CSUP-3.3 | Does the device have the capability to receive remote installation of patches or software updates?   | Yes | Yes, the device can receive patches from the Ambu OTA service (pull only).   |  |  |  |
| CSUP-3.4 | Does the medical device manufacturer allow security updates from any third-party manufacturers (e.g., Microsoft) to be installed without approval from the manufacturer? | No  | -  |  |  |  |
| CSUP-4   | Does the device contain Anti-Malware Software? If yes, complete 4.1-4.4.   | No  | -  |  |  |  |
| CSUP-4.1 | Does the device documentation provide instructions for owner/operator installation of patches or software updates?   | N/A | -  |  |  |  |
| CSUP-4.2 | Does the device require vendor or vendor-authorized service to install patches or software updates?  | N/A | -  |  |  |  |
| CSUP-4.3 | Does the device have the capability to receive remote installation of patches or software updates?   | N/A | -  |  |  |  |
| CSUP-4.4 | Does the medical device manufacturer allow security updates from any third-party manufacturers (e.g., Microsoft) to be installed without approval from the manufacturer? | N/A | -  |  |  |  |
| CSUP-5   | Does the device contain Non-Operating System commercial off-the-shelf components? If yes, complete 5.1-5.4.  | Yes | Software is always released as one self-contained bundle.  |  |  |  |
| CSUP-5.1 | Does the device documentation provide instructions for owner/operator installation of patches or software updates?   | No  | -  |  |  |  |

**MDS2 for Ambu A/S displaying and processing units with software version 2.4**

|          |   |     |   |  |  |  |
|----------|---|-----|---|--|--|--|
| CSUP-5.2 | Does the device require vendor or vendor-authorized service to install patches or software updates?   | Yes | For the OTA it is required that the device is registered in order to be updated/patched. For USB it is required that a signed update package is provided to the hospital from Ambu on a USB flash drives. This is contained in the self-contained bundle, see CSUP-1. |  |  |  |
| CSUP-5.3 | Does the device have the capability to receive remote installation of patches or software updates?  | Yes | Yes, the device can receive patches from the Ambu OTA service (pull only).  |  |  |  |
| CSUP-5.4 | Does the medical device manufacturer allow security updates from any third-party manufacturers (e.g., Microsoft) to be installed without approval from the manufacturer?            | No  | -   |  |  |  |
| CSUP-6   | Does the device contain other software components (e.g., asset management software, license management)? If yes, please provide details or reference in notes and complete 6.1-6.4. | No  | -   |  |  |  |
| CSUP-6.1 | Does the device documentation provide instructions for owner/operator installation of patches or software updates?  | N/A | -   |  |  |  |
| CSUP-6.2 | Does the device require vendor or vendor-authorized service to install patches or software updates?   | N/A | -   |  |  |  |
| CSUP-6.3 | Does the device have the capability to receive remote installation of patches or software updates?  | N/A | -   |  |  |  |
| CSUP-6.4 | Does the medical device manufacturer allow security updates from any third-party manufacturers (e.g., Microsoft) to be installed without approval from the manufacturer?            | N/A | -   |  |  |  |
| CSUP-7   | Does the manufacturer notify the customer when updates are approved for installation?   | Yes | -   |  |  |  |
| CSUP-8   | Does the device perform automatic installation of software updates?   | No  | Pull only on operator initiative.   |  |  |  |
| CSUP-9   | Does the manufacturer have an approved list of third-party software that can be installed on the device?  | No  | -   |  |  |  |
| CSUP-10  | Can the owner/operator install manufacturer-approved third-party software on the device themselves?   | No  | -   |  |  |  |

**MDS2 for Ambu A/S displaying and processing units with software version 2.4**

|   |   |                                       |  |                               |                              |                        |
|---|---|---------------------------------------|--|-------------------------------|------------------------------|------------------------|
| CSUP-10.1   | Does the system have mechanism in place to prevent installation of unapproved software?                                     | Yes                                   | Only accepts Ambu signed packages.   |                               |                              |                        |
| CSUP-11   | Does the manufacturer have a process in place to assess device vulnerabilities and updates?                                 | Yes                                   | Internal vulnerability management program.   |                               |                              |                        |
| CSUP-11.1   | Does the manufacturer provide customers with review and approval status of updates?   | No                                    | Internal Release Process according to IEC62304.  |                               |                              |                        |
| CSUP-11.2   | Is there an update review cycle for the device?   | Yes                                   | Internal Software Maintenance process according to IEC62304.   |                               |                              |                        |
|   | <b>HEALTH DATA DE-IDENTIFICATION (DIDT)</b>   | <b>Displaying and processing unit</b> | <b>Notes</b>   | <b>IEC TR 80001-2-2: 2012</b> | <b>NIST SP 800-53 Rev. 4</b> | <b>ISO 27002: 2013</b> |
| The ability of the device to directly remove information that allows identification of a person.                          |   |                                       |  |                               |                              |                        |
| DIDT-1  | Does the device provide an integral capability to de-identify personally identifiable information?                          | No                                    | –  | Section 5.6, DIDT             | None                         | ISO 27038              |
| DIDT-1.1  | Does the device support de-identification profiles that comply with the DICOM standard for de-identification?               | No                                    | –  | Section 5.6, DIDT             | None                         | ISO 27038              |
|   | <b>DATA BACKUP AND DISASTER RECOVERY (DTBK)</b>   | <b>Displaying and processing unit</b> | <b>Notes</b>   | <b>IEC TR 80001-2-2: 2012</b> | <b>NIST SP 800-53 Rev. 4</b> | <b>ISO 27002: 2013</b> |
| The ability to recover after damage or destruction of device data, hardware, software, or site configuration information. |   |                                       |  |                               |                              |                        |
| DTBK-1  | Does the device maintain long term primary storage of personally identifiable information/ patient information (e.g. PACS)? | Yes                                   | The device only stores DICOM-WL information in a database on the device.                             |                               |                              |                        |
| DTBK-2  | Does the device have a “factory reset” function to restore the original device settings as provided by the manufacturer?    | Yes                                   | The reset, resets all configurations, remove sensitive data and resets network settings.             | Section 5.7, DTBK             | CP-9                         | A.12.3.1               |
| DTBK-3  | Does the device have an integral data backup capability to removable media?   | No                                    | The device does not include a integral data backup. Manual backup through export to USB is possible. | Section 5.7, DTBK             | CP-9                         | A.12.3.1               |
| DTBK-4  | Does the device have an integral data backup capability to remote storage?  | No                                    | The device does not include a integral data backup. Export through DICOM and SMB is possible.        |                               |                              |                        |
| DTBK-5  | Does the device have a backup capability for system configuration information, patch restoration, and software restoration. | No                                    | –  |                               |                              |                        |
| DTBK-6  | Does the device provide the capability to check the integrity and authenticity of a backup?                                 | N/A                                   | –  | Section 5.7, DTBK             | CP-9                         | A.12.3.1               |

**MDS2 for Ambu A/S displaying and processing units with software version 2.4**

|   | <b>EMERGENCY ACCESS (EMRG)</b>  | <b>Displaying and processing unit</b> | <b>Notes</b>   | <b>IEC TR 80001-2-2: 2012</b> | <b>NIST SP 800-53 Rev. 4</b> | <b>ISO 27002: 2013</b> |
|---|---|---------------------------------------|--|-------------------------------|------------------------------|------------------------|
| The ability of the device user to access personally identifiable information in case of a medical emergency situation that requires immediate access to stored personally identifiable information. |   |                                       |  |                               |                              |                        |
| EMRG-1  | Does the device incorporate an emergency access (i.e. "break-glass") feature? | Yes                                   | Primary use functions for the current procedure is available without login, but are restricted to the current procedure, can not export or modify the configuration of the device. | Section 5.8, EMRG             | SI-17                        | None                   |

|  | <b>HEALTH DATA INTEGRITY AND AUTHENTICITY (IGAU)</b>  | <b>Displaying and processing unit</b> | <b>Notes</b> | <b>IEC TR 80001-2-2: 2012</b> | <b>NIST SP 800-53 Rev. 4</b> | <b>ISO 27002: 2013</b> |
|--|---|---------------------------------------|--------------|-------------------------------|------------------------------|------------------------|
| How the device ensures that the stored data on the device has not been altered or destroyed in a non-authorized manner and is from the originator. |   |                                       |              |                               |                              |                        |
| IGAU-1   | Does the device provide data integrity checking mechanisms of stored health data (e.g., hash or digital signature)? | No                                    | -            | Section 5.9, IGAU             | SC-28                        | A.18.1.3               |
| IGAU-2   | Does the device provide error/failure protection and recovery mechanisms for stored health data (e.g., RAID-5)?     | No                                    | -            | Section 5.9, IGAU             | SC-28                        | A.18.1.3               |

|   | <b>MALWARE DETECTION/PROTECTION (MLDP)</b>   | <b>Displaying and processing unit</b> | <b>Notes</b>  | <b>IEC TR 80001-2-2: 2012</b> | <b>NIST SP 800-53 Rev. 4</b> | <b>ISO 27002: 2013</b>                         |
|---|--|---------------------------------------|---|-------------------------------|------------------------------|--|
| The ability of the device to effectively prevent, detect and remove malicious software (malware). |  |                                       |   |                               |                              |  |
| MLDP-1  | Does the device capable of hosting executable software?  | No                                    | The jailed GUI is unable to execute arbitrary software. | Section 5.10, MLDP            |                              |  |
| MLDP-2  | Does the device support the use of anti-malware software (or other anti-malware mechanism)? Provide details or reference in notes. | No                                    | -   | Section 5.10, MLDP            | SI-3                         | A.12.2.1                                       |
| MLDP-2.1  | Does the device include anti-malware software by default?  | N/A                                   | -   | Section 5.10, MLDP            | CM-5                         | A.9.2.3, A.9.4.5, A.12.1.2, A.12.1.4, A.12.5.1 |
| MLDP-2.2  | Does the device have anti-malware software available as an option?   | N/A                                   | -   | Section 5.10, MLDP            | AU-6                         | A.12.4.1, A.16.1.2, A.16.1.4                   |
| MLDP-2.3  | Does the device documentation allow the owner/operator to install or update anti-malware software?                                 | N/A                                   | -   | Section 5.10, MLDP            | CP-10                        | A.17.1.2                                       |
| MLDP-2.4  | Can the device owner/operator independently (re-) configure anti-malware settings?   | N/A                                   | -   | Section 5.10, MLDP            | AU-2                         | None   |

**MDS2 for Ambu A/S displaying and processing units with software version 2.4**

|   |  |                                       |  |                                |                              |  |
|---|--|---------------------------------------|--|--------------------------------|------------------------------|--|
| MLDP-2.5  | Does notification of malware detection occur in the device user interface?   | N/A                                   | –  |                                |                              |  |
| MLDP-2.6  | Can only manufacturer-authorized persons repair systems when malware has been detected?  | N/A                                   | –  |                                |                              |  |
| MLDP-2.7  | Are malware notifications written to a log?  | N/A                                   | –  |                                |                              |  |
| MLDP-2.8  | Are there any restrictions on anti-malware (e.g., purchase, installation, configuration, scheduling)?  | N/A                                   | –  |                                |                              |  |
| MLDP-3  | If the answer to MLDP-2 is NO, and anti-malware cannot be installed on the device, are other compensating controls in place or available?  | Yes                                   | <ul style="list-style-type: none"> <li>• Jailed GUI application</li> <li>• Update bundles are authenticated and signed by Ambu</li> <li>• Linux OS configured with least required modules installed</li> <li>• Device acts as client for both SMB and DICOM.</li> <li>• Firewall only allow system initiated connections and ICMP responses</li> </ul> | Section 5.10, MLDP             | SI-2                         | A.12.6.1, A.14.2.2, A.14.2.3, A.16.1.3 |
| MLDP-4  | Does the device employ application whitelisting that restricts the software and services that are permitted to be run on the device?   | No                                    | –  | Section 5.10, MLDP             | SI-3                         | A.12.2.1                               |
| MLDP-5  | Does the device employ a host-based intrusion detection/prevention system?   | No                                    | –  | Section 5.10, MLDP             | SI-4                         | None                                   |
| MLDP-5.1  | Can the host-based intrusion detection/prevention system be configured by the customer?  | N/A                                   | –  | Section 5.10, MLDP             | CM-7                         | A.12.5.1                               |
| MLDP-5.2  | Can a host-based intrusion detection/prevention system be installed by the customer?   | N/A                                   | –  | Section 5.10, MLDP             |                              |  |
|   | <b>NODE AUTHENTICATION (NAUT)</b>  | <b>Displaying and processing unit</b> | <b>Notes</b>   | <b>IEC TR 80001- 2-2: 2012</b> | <b>NIST SP 800-53 Rev. 4</b> | <b>ISO 27002: 2013</b>                 |
| The ability of the device to authenticate communication partners/nodes. |  |                                       |  |                                |                              |  |
| NAUT-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 (e.g. Web APIs, SMTP, SNMP)? | Yes                                   | The OTA update service, uses role based authentication and authorization. The upgrade bundle is authenticated using a X.509 certificate.   | Section 5.11, NAUT             | SC-23                        | None                                   |
| NAUT-2  | Are the network access control mechanisms supported (E.g., does the device have an internal firewall, or use a network connection white list)?   | Yes                                   | Internal firewall.   | Section 5.11, NAUT             | SC-7                         | A.13.1.1, A.13.1.3, A.13.2.1, A.14.1.3 |
| NAUT-2.1  | Is the firewall ruleset documented and available for review?   | No                                    | –  |                                |                              |  |

**MDS2 for Ambu A/S displaying and processing units with software version 2.4**

|  |  |                                       |   |                                |                              |                        |
|--|--|---------------------------------------|---|--------------------------------|------------------------------|------------------------|
| NAUT-3   | Does the device use certificate-based network connection authentication?                     | Yes                                   | The device uses TLS authentication for OTA, with a CA signed certificate. The authentication of the TLS session is maintained by a OAUTH2 token.<br><br>DICOM-TLS is supported, supporting certificate-based authentication (one-way/anonymous TLS) |                                |                              |                        |
|  | <b>CONNECTIVITY CAPABILITIES (CONN)</b>  | <b>Displaying and processing unit</b> | <b>Notes</b>  | <b>IEC TR 80001- 2-2: 2012</b> | <b>NIST SP 800-53 Rev. 4</b> | <b>ISO 27002: 2013</b> |
| All network and removable media connections must be considered in determining appropriate security controls. This section lists connectivity capabilities that may be present on the device. |  |                                       |   |                                |                              |                        |
| CONN-1   | Does the device have hardware connectivity capabilities?                                     | Yes                                   | -   |                                |                              |                        |
| CONN-1.1   | Does the device support wireless connections?  | Yes                                   | -   |                                |                              |                        |
| CONN-1.1.2   | Does the device support Wi-Fi?   | Yes                                   | -   |                                |                              |                        |
| CONN-1.1.3   | Does the device support Bluetooth?   | No                                    | -   |                                |                              |                        |
| CONN-1.1.4   | Does the device support other wireless network connectivity (e.g. LTE, Zigbee, proprietary)? | No                                    | -   |                                |                              |                        |
| CONN-1.2   | Does the device support physical connections?  | Yes                                   | -   |                                |                              |                        |
| CONN-1.2.1   | Does the device have available RJ45 Ethernet ports?  | Yes                                   | -   |                                |                              |                        |
| CONN-1.2.2   | Does the device have available USB ports?  | Yes                                   | -   |                                |                              |                        |
| CONN-1.2.3   | Does the device require, use, or support removable memory devices?                           | Yes                                   | -   |                                |                              |                        |
| CONN-1.2.4   | Does the device support other physical connectivity?   | Yes                                   | aBox 2 has video output (SDI/VDI) and trigger signal options (mini jack/D-SUB9) and USB input/output.<br><br>aView 2 Advance has video output (HDMI/SDI) and USB input/output   |                                |                              |                        |

**MDS2 for Ambu A/S displaying and processing units with software version 2.4**

|          |   |     |   |  |  |  |
|----------|---|-----|---|--|--|--|
| CONN-2   | Does the manufacturer provide a list of network ports and protocols that are used or may be used on the device? | No  | -   |  |  |  |
| CONN-3   | Can the device communicate with other systems within the customer environment?                                  | Yes | The devices can retrieve worklist and export data to system utilizing the DICOM protocol.<br><br>See DICOM conformance statement for more. The device can export videos and images to a network storage server using SMB. |  |  |  |
| CONN-4   | Can the device communicate with other systems external to the customer environment (e.g., a service host)?      | Yes | The "Over the Air" (OTA) software update service uses HTTPS over TLS to make remote request. All requests are initiated by a user of the display unit.  |  |  |  |
| CONN-5   | Does the device make or receive API calls?  | Yes | The OTA (Ambu update service) make API requests to a Ambu specific update solution. All requests are initiated by a user of the display unit.   |  |  |  |
| CONN-6   | Does the device require an internet connection for its intended use?  | No  | OTA (Ambu update service) requires a internet uplink.   |  |  |  |
| CONN-7   | Does the device support Transport Layer Security (TLS)?   | Yes | OTA uses HTTP over TLS. DICOM-TLS is supported. SMBv3 supports TLS.   |  |  |  |
| CONN-7.1 | Is TLS configurable?  | No  | DICOM-TLS and SMB are only top-level configurable, cipher-suites cannot be choosen, but mode of operation can.<br><br>See Note 1 below about DICOM-TLS Security profiles.   |  |  |  |
| CONN-8   | Does the device provide operator control functionality from a separate device (e.g., telemedicine)?             | No  | -   |  |  |  |

**MDS2 for Ambu A/S displaying and processing units with software version 2.4**

|  | <b>PERSON AUTHENTICATION (PAUT)</b>  | <b>Displaying and processing unit</b> | <b>Notes</b>   | <b>IEC TR 80001- 2-2: 2012</b> | <b>NIST SP 800-53 Rev. 4</b> | <b>ISO 27002: 2013</b>                 |
|--|--|---------------------------------------|--|--------------------------------|------------------------------|--|
| The ability to configure the device to authenticate users. |  |                                       |  |                                |                              |  |
| PAUT-1   | Does the device support and enforce unique IDs and passwords for all users and roles (including service accounts)?                               | No                                    | The device does not support enforcing of password policies for users/roles. The device supports user creation and password changing. | Section 5.12, PAUT             | IA-2                         | A.9.2.1                                |
| PAUT-1.1   | Does the device enforce authentication of unique IDs and passwords for all users and roles (including service accounts)?                         | No                                    | IFU recommend password policies, but the device does not enforce it.   | Section 5.12, PAUT             | IA-2                         | A.9.2.1                                |
| PAUT-2   | Is the device configurable to authenticate users through an external authentication service (e.g., MS Active Directory, NDS, LDAP, OAuth, etc.)? | No                                    | –  | Section 5.12, PAUT             | IA-5                         | A.9.2.1                                |
| PAUT-3   | Is the device configurable to lock out a user after a certain number of unsuccessful logon attempts?   | No                                    | –  | Section 5.12, PAUT             | IA-2                         | A.9.2.1                                |
| PAUT-4   | Are all default accounts (e.g., technician service accounts, administrator accounts) listed in the documentation?                                | Yes                                   | Access levels are documented in the IFU.   | Section 5.12, PAUT             | SA-4(5)                      | A.14.1.1, A.14.2.7, A.14.2.9, A.15.1.2 |
| PAUT-5   | Can all passwords be changed?  | Yes                                   | –  | Section 5.12, PAUT             |                              |  |
| PAUT-6   | Is the device configurable to enforce creation of user account passwords that meet established (organization specific) complexity rules?         | No                                    | –  | Section 5.12, PAUT             | IA-2                         | A.9.2.1                                |
| PAUT-7   | Does the device support account passwords that expire periodically?  | No                                    | –  |                                |                              |  |
| PAUT-8   | Does the device support multi-factor authentication?   | No                                    | –  |                                |                              |  |
| PAUT-9   | Does the device support single sign-on (SSO)?  | No                                    | –  | Section 5.12, PAUT             | IA-2                         | A.9.2.1                                |
| PAUT-10  | Can user accounts be disabled/locked on the device?  | Yes                                   | Administrator can disable accounts.  | Section 5.12, PAUT             | IA-2                         | A.9.2.1                                |
| PAUT-11  | Does the device support biometric controls?  | No                                    | –  | Section 5.12, PAUT             | IA-2                         | A.9.2.1                                |
| PAUT-12  | Does the device support physical tokens (e.g. badge access)?   | No                                    | –  |                                |                              |  |
| PAUT-13  | Does the device support group authentication (e.g. hospital teams)?  | No                                    | –  |                                |                              |  |
| PAUT-14  | Does the application or device store or manage authentication credentials?   | Yes                                   | X.509 Certificate used for update package authentication. Encryption key is stored for use in OTA authentication.                    |                                |                              |  |

**MDS2 for Ambu A/S displaying and processing units with software version 2.4**

|  |  |                                       |   |                                |                              |                              |
|--|--|---------------------------------------|---|--------------------------------|------------------------------|------------------------------|
| PAUT-14.1  | Are credentials stored using a secure method?  | Yes                                   | The keys are stored in GPG keystore.  |                                |                              |                              |
|  | <b>PHYSICAL LOCKS (PLOK)</b>   | <b>Displaying and processing unit</b> | <b>Notes</b>  | <b>IEC TR 80001- 2-2: 2012</b> | <b>NIST SP 800-53 Rev. 4</b> | <b>ISO 27002: 2013</b>       |
| Physical locks can prevent unauthorized users with physical access to the device from compromising the integrity and confidentiality of personally identifiable information stored on the device or on removable media |  |                                       |   |                                |                              |                              |
| PLOK-1   | Is the device software only? If yes, answer "N/A" to remaining questions in this section.  | No                                    | –   | Section 5.13, PLOK             | PE-3(4)                      | A.11.1.1, A.11.1.2, A.11.1.3 |
| PLOK-2   | Are all device components maintaining personally identifiable information (other than removable media) physically secure (i.e., cannot remove without tools)?          | Yes                                   | No data storage component can be removed without opening the case (Special tools are needed).   | Section 5.13, PLOK             | PE-3(4)                      | A.11.1.1, A.11.1.2, A.11.1.3 |
| PLOK-3   | Are all device components maintaining personally identifiable information (other than removable media) physically secured behind an individually keyed locking device? | No                                    | –   | Section 5.13, PLOK             | PE-3(4)                      | A.11.1.1, A.11.1.2, A.11.1.3 |
| PLOK-4   | Does the device have an option for the customer to attach a physical lock to restrict access to removable media?   | No                                    | –   | Section 5.13, PLOK             | PE-3(4)                      | A.11.1.1, A.11.1.2, A.11.1.3 |
|  | <b>ROADMAP FOR THIRD PARTY COMPONENTS IN DEVICE LIFE CYCLE (RDMP)</b>  | <b>Displaying and processing unit</b> | <b>Notes</b>  | <b>IEC TR 80001- 2-2: 2012</b> | <b>NIST SP 800-53 Rev. 4</b> | <b>ISO 27002: 2013</b>       |
| Manufacturer's plans for security support of third-party components within the device's life cycle.  |  |                                       |   |                                |                              |                              |
| RDMP-1   | Was a secure software development process, such as ISO/IEC 27034 or IEC 62304, followed during product development?  | Yes                                   | –   | Section 5.14, RDMP             | CM-2                         | None                         |
| RDMP-2   | Does the manufacturer evaluate third-party applications and software components included in the device for secure development practices?                               | Yes                                   | Internal reviews of selected third-party components has been conducted. Internal vulnerability management program monitors the third-party component security. The device has been subject to external pentest. | Section 5.14, RDMP             | CM-8                         | A.8.1.1, A.8.1.2             |
| RDMP-3   | Does the manufacturer maintain a web page or other source of information on software support dates and updates?  | No                                    | –   | Section 5.14, RDMP             | CM-8                         | A.8.1.1, A.8.1.2             |
| RDMP-4   | Does the manufacturer have a plan for managing third-party component end-of-life?  | Yes                                   | –   | Section 5.14, RDMP             | CM-8                         | A.8.1.1, A.8.1.2             |

**MDS2 for Ambu A/S displaying and processing units with software version 2.4**

|   | <b>SOFTWARE BILL OF MATERIALS (SBoM)</b>   | <b>Displaying and processing unit</b>   | <b>Notes</b>  | <b>IEC TR 80001- 2-2: 2012</b> | <b>NIST SP 800-53 Rev. 4</b> | <b>ISO 27002: 2013</b>                              |
|---|--|---|---|--------------------------------|------------------------------|---|
| A Software Bill of Material (SBoM) lists all the software components that are incorporated into the device being described for the purpose of operational security planning by the healthcare delivery organization. This section support |  |   |   |                                |                              |   |
| SBOM-1  | Is the SBoM for this product available?  | Yes   | The SBOM is available on ambu.com.  |                                |                              |   |
| SBOM-2  | Does the SBoM follow a standard or common method in describing software components?  | The new eSBOMs are provided in CycloneDX and SPDX formats which are standardized formats. | -   |                                |                              |   |
| SBOM-2.1  | Are the software components identified?  | Yes   | -   |                                |                              |   |
| SBOM-2.1  | Are the developers/manufacturers of the software components identified?  | Yes   | -   |                                |                              |   |
| SBOM-2.3  | Are the major version numbers of the software components identified?   | Yes   | -   |                                |                              |   |
| SBOM-2.4  | Are any additional descriptive elements identified?  | Yes   | End of Support dates and Unique IDs.  |                                |                              |   |
| SBOM-3  | Does the device include a command or process method available to generate a list of software components installed on the device? | Yes   | Licenses and software can be displayed on the system on request.  |                                |                              |   |
| SBOM-4  | Is there an update process for the SBoM?   | No  | -   |                                |                              |   |
|   | <b>SYSTEM AND APPLICATION HARDENING (SAHD)</b>   | <b>Displaying and processing unit</b>   | <b>Notes</b>  | <b>IEC TR 80001- 2-2: 2012</b> | <b>NIST SP 800-53 Rev. 4</b> | <b>ISO 27002: 2013</b>                              |
| The device's inherent resistance to cyber attacks and malware.  |  |   |   |                                |                              |   |
| SAHD-1  | Is the device hardened in accordance with any industry standards?  | No  | The device software has been hardened by: <ul style="list-style-type: none"> <li>Using a firewall that drops all traffic other than system-initiated connections and ICMP responses</li> <li>Jailing the GUI application</li> <li>Configuring the Linux operating system using a least required principle</li> <li>Supporting WPA3 and WPA 2/3 enterprise</li> <li>Supporting DICOM TLS and using HTTP over TLS for OTA</li> <li>Only supporting SMBv3</li> </ul> | Section 5.15, SAHD             | AC-17(2)/ IA-3               | A.6.2.1, A.6.2.2, A.13.1.1, A.13.2.1, A.14.1.2/None |
| SAHD-2  | Has the device received any cybersecurity certifications?  | No  | -   | Section 5.15, SAHD             | SA-12(10)                    | A.14.2.7, A.15.1.1, A.15.1.2, A.15.1.3              |

**MDS2 for Ambu A/S displaying and processing units with software version 2.4**

|          |  |     |  |                    |       |   |
|----------|--|-----|--|--------------------|-------|---|
| SAHD-3   | Does the device employ any mechanisms for software integrity checking  | No  |  |                    |       |   |
| SAHD-3.1 | Does the device employ any mechanism (e.g., release-specific hash key, checksums, digital signature, etc.) to ensure the installed software is manufacturer-authorized?            | Yes | Update package has been digitally signed using RSA key.  |                    |       |   |
| SAHD-3.2 | Does the device employ any mechanism (e.g., release-specific hash key, checksums, digital signature, etc.) to ensure the software updates are the manufacturer-authorized updates? | Yes |  | Section 5.15, SAHD | CM-8  | A.8.1.1, A.8.1.2  |
| SAHD-4   | Can the owner/operator perform software integrity checks (i.e., verify that the system has not been modified or tampered with)?  | No  | The operator can see the verification of update packages.  | Section 5.15, SAHD | AC-3  | A.6.2.2, A.9.1.2, A.9.4.1, A.9.4.4, A.9.4.5, A.13.1.1, A.14.1.2, A.14.1.3, A.18.1.3 |
| SAHD-5   | Is the system configurable to allow the implementation of file-level, patient level, or other types of access controls?  | Yes | Only the Administrator has full access to the displaying unit's settings and functions, including the creation of new users. | Section 5.15, SAHD | CM-7  | A.12.5.1*   |
| SAHD-5.1 | Does the device provide role-based access controls?  | Yes | Role-based access control has been enforced on the application layer of the device.  | Section 5.15, SAHD | CM-7  | A.12.5.1*   |
| SAHD-6   | Are any system or user accounts restricted or disabled by the manufacturer at system delivery?   | Yes | Administrator and Service accounts are immutable and can only be modified at compile time (except password).                 | Section 5.15, SAHD | CM-8  | A.8.1.1, A.8.1.2  |
| SAHD-6.1 | Are any system or user accounts configurable by the end user after initial configuration?  | No  | –  | Section 5.15, SAHD | CM-7  | A.12.5.1*   |
| SAHD-6.2 | Does this include restricting certain system or user accounts, such as service technicians, to least privileged access?  | Yes | –  | Section 5.15, SAHD | CM-7  | A.12.5.1*   |
| SAHD-7   | Are all shared resources (e.g., file shares) which are not required for the intended use of the device disabled?   | Yes | Application layer accounts are jailed and access to resources are role based restricted.                                     | Section 5.15, SAHD | CM-7  | A.12.5.1*   |
| SAHD-8   | Are all communication ports and protocols that are not required for the intended use of the device disabled?   | Yes | Specifically verified during verification.   | Section 5.15, SAHD | SA-18 | None  |
| SAHD-9   | Are all devices (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? | Yes |  | Section 5.15, SAHD | CM-6  | None  |

**MDS2 for Ambu A/S displaying and processing units with software version 2.4**

|           |  |     |   |                    |      |  |
|-----------|--|-----|---|--------------------|------|--|
| SAHD-10   | 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? | Yes | The OS is custom built for the device. The OS implements the least required.  | Section 5.15, SAHD | SI-2 | A.12.6.1, A.14.2.2, A.14.2.3, A.16.1.3 |
| SAHD-11   | Can the device prohibit boot from uncontrolled or removable media (i.e., a source other than an internal drive or memory component)?   | Yes | The BIOS password is required to boot from removable media. The BIOS password is unique to every device and only known to legal manufacturer.                     |                    |      |  |
| SAHD-12   | Can unauthorized software or hardware be installed on the device without the use of physical tools?  | No  | –   |                    |      |  |
| SAHD-13   | Does the product documentation include information on operational network security scanning by users?  | No  | –   |                    |      |  |
| SAHD-14   | Can the device be hardened beyond the default provided state?  | Yes | Disabling of critical components is possible, e.g Wi-Fi, Internet uplink and USB. Automatic logout and session policies, can be hardened beyond default settings. |                    |      |  |
| SAHD-14.1 | Are instructions available from vendor for increased hardening?  | Yes | Instructions for hardening beyond defaults, are provided in the IFU.  |                    |      |  |
| SAHD-15   | Can the system prevent access to BIOS or other bootloaders during boot?  | Yes | aBox2 uses full disk encryption and ATA-locking. aView 2 Advance uses ATA-locking of the disk. Both devices uses a per device unique BIOS password.               |                    |      |  |
| SAHD-16   | Have additional hardening methods not included in 2.3.19 been used to harden the device?   | No  | –   |                    |      |  |

**MDS2 for Ambu A/S displaying and processing units with software version 2.4**

|   | <b>SECURITY GUIDANCE (SGUD)</b>   | <b>Displaying and processing unit</b> | <b>Notes</b>  | <b>IEC TR 80001-2-2: 2012</b> | <b>NIST SP 800-53 Rev. 4</b> | <b>ISO 27002: 2013</b>                     |
|---|---|---------------------------------------|---|-------------------------------|------------------------------|--|
| Availability of security guidance for operator and administrator of the device and manufacturer sales and service.  |   |                                       |   |                               |                              |  |
| SGUD-1  | Does the device include security documentation for the owner/operator?  | Yes                                   | Basic operational security information is provided in the IFU. Additional cybersecurity information can be provided on request by Ambu. | Section 5.16, SGUD            | AT-2/PL-2                    | A.7.2.2, A.12.2.1/A.14.1.1                 |
| SGUD-2  | Does the device have the capability, and provide instructions, for the permanent deletion of data from the device or media? | Yes                                   | See IFU.  | Section 5.16, SGUD            | MP-6                         | A.8.2.3, A.8.3.1, A.8.3.2, A.11.2.7        |
| SGUD-3  | Are all access accounts documented?   | Yes                                   | –   | Section 5.16, SGUD            | AC-6, IA-2                   | A.9.1.2, A.9.2.3, A.9.4.4, A.9.4.5/A.9.2.1 |
| SGUD-3.1  | Can the owner/operator manage password control for all accounts?  | Yes                                   | –   |                               |                              |  |
| SGUD-4  | Does the product include documentation on recommended compensating controls for the device?                                 | Yes                                   | The IFU includes information for: DICOM setup on private networks and for Wi-Fi setup.  |                               |                              |  |
|   | <b>HEALTH DATA STORAGE CONFIDENTIALITY (STCF)</b>   | <b>Displaying and processing unit</b> | <b>Notes</b>  | <b>IEC TR 80001-2-2: 2012</b> | <b>NIST SP 800-53 Rev. 4</b> | <b>ISO 27002: 2013</b>                     |
| The ability of the device to ensure unauthorized access does not compromise the integrity and confidentiality of personally identifiable information stored on the device or removable media. |   |                                       |   |                               |                              |  |
| STCF-1  | Can the device encrypt data at rest?  | Yes                                   | aBox2 offers full disk encryption. aView 2 Advance uses ATA-locking of the disk.  | Section 5.17, STCF            | SC-28                        | A.8.2.3                                    |
| STCF-1.1  | Is all data encrypted or otherwise protected?   | Yes                                   |   |                               |                              |  |
| STCF-1.2  | Is the data encryption capability configured by default?  | Yes                                   |   |                               |                              |  |
| STCF-1.3  | Are instructions available to the customer to configure encryption?   | No                                    |   |                               |                              |  |
| STCF-2  | Can the encryption keys be changed or configured?   | No                                    |   | Section 5.17, STCF            | SC-28                        | A.8.2.3                                    |
| STCF-3  | Is the data stored in a database located on the device?   | Yes                                   | –   |                               |                              |  |
| STCF-4  | Is the data external in a database located on the device?   | No                                    | Manual export to DICOM PACS is possible.  |                               |                              |  |

**MDS2 for Ambu A/S displaying and processing units with software version 2.4**

|   | <b>TRANSMISSION CONFIDENTIALITY (TXCF)</b>  | <b>Displaying and processing unit</b> | <b>Notes</b>  | <b>IEC TR 80001-2-2: 2012</b> | <b>NIST SP 800-53 Rev. 4</b> | <b>ISO 27002: 2013</b>                                    |
|---|---|---------------------------------------|---|-------------------------------|------------------------------|---|
| The ability of the device to ensure the confidentiality of transmitted personally identifiable information.                               |   |                                       |   |                               |                              |   |
| TXCF-1  | Can personally identifiable information be transmitted only via a point-to-point dedicated cable?                             | No                                    | –   | Section 5.18, TXCF            | CM-7                         | A.12.5.1  |
| TXCF-2  | Is personally identifiable information encrypted prior to transmission via a network or removable media?                      | No                                    | The device support DICOM TLS and SMBv3 which includes encryption.   | Section 5.18, TXCF            | CM-7                         | A.12.5.1  |
| TXCF-2.1  | If data is not encrypted by default, can the customer configure encryption options?   | No                                    | –   |                               |                              |   |
| TXCF-3  | Is personally identifiable information transmission restricted to a fixed list of network destinations?                       | Yes                                   | Transmission of data to either SMB server or PACS server in DICOM must be configured by end-user. All transmissions are user initiated. | Section 5.18, TXCF            | CM-7                         | A.12.5.1  |
| TXCF-4  | Annexations limited to authenticated systems?   | No                                    | –   | Section 5.18, TXCF            | CM-7                         | A.12.5.1  |
| TXCF-5  | Are secure transmission methods supported/ implemented (DICOM, HL7, IEEE 11073)?  | Yes                                   | DICOM-TLS support.  |                               |                              |   |
|   | <b>TRANSMISSION INTEGRITY (TXIG)</b>  | <b>Displaying and processing unit</b> | <b>Notes</b>  | <b>IEC TR 80001-2-2: 2012</b> | <b>NIST SP 800-53 Rev. 4</b> | <b>ISO 27002: 2013</b>                                    |
| The ability of the device to ensure the integrity of transmitted data.  |   |                                       |   |                               |                              |   |
| TXIG-1  | Does the device support any mechanism (e.g., digital signatures) intended to ensure data is not modified during transmission? | Yes                                   | Upgrade provided by OTA, the integrity is maintained by a digital signature.  | Section 5.19, TXIG            | SC-8                         | A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3 |
| TXIG-2  | Does the device include multiple sub-components connected by external cables?   | No                                    | –   |                               |                              |   |
|   | <b>REMOTE SERVICE (RMOT)</b>  | <b>Displaying and processing unit</b> | <b>Notes</b>  | <b>IEC TR 80001-2-2: 2012</b> | <b>NIST SP 800-53 Rev. 4</b> | <b>ISO 27002: 2013</b>                                    |
| Remote service refers to all kinds of device maintenance activities performed by a service person via network or other remote connection. |   |                                       |   |                               |                              |   |
| RMOT-1  | Does the device permit remote service connections for device analysis or repair?  | No                                    | –   |                               | AC-17                        | A.6.2.1, A.6.2.2, A.13.1.1, A.13.2.1, A.14.1.2            |
| RMOT-1.1  | Does the device allow the owner/operator to initiative remote service sessions for device analysis or repair?                 | N/A                                   | –   |                               |                              |   |
| RMOT-1.2  | Is there an indicator for an enabled and active remote session?   | N/A                                   | –   |                               |                              |   |

| MDS2 for Ambu A/S displaying and processing units with software version 2.4 |  |                                       |  |                               |                              |  |
|---|--|---------------------------------------|--|-------------------------------|------------------------------|--|
| RMOT-1.3  | Can patient data be accessed or viewed from the device during the remote session?                          | N/A                                   | -  |                               | AC-17                        | A.6.2.1, A.6.2.2, A.13.1.1, A.13.2.1, A.14.1.2 |
| RMOT-2  | Does the device permit or use remote service connections for predictive maintenance data?                  | No                                    | -  |                               |                              |  |
| RMOT-3  | Does the device have any other remotely accessible functionality (e.g. software updates, remote training)? | Yes                                   | OTA service uses HTTP over TLS for updating the device. Updates must be initiated by healthcare organisation' Admin or Service Technician. Ambu cannot push an update automatically to the device for updating the device. |                               |                              |  |
|   | <b>OTHER SECURITY CONSIDERATIONS (OTHR)</b>  | <b>Displaying and processing unit</b> | <b>Notes</b>   | <b>IEC TR 80001-2-2: 2012</b> | <b>NIST SP 800-53 Rev. 4</b> | <b>ISO 27002: 2013</b>                         |
|   | None   |                                       |  |                               |                              |  |
| OTHR-1  | Does the remote upgrade mechanism support a fallback to local?   | Yes                                   | -  |                               |                              |  |
| OTHR-1.1  | Does the device permit a local operator to disable the remote connection                                   | Yes                                   | -  |                               |                              |  |
| OTHR-1.2  | Is the device still capable to be updated without the remote upgrade mechanism                             | Yes                                   | -  |                               |                              |  |
| OTHR-1.3  | Can the vendor modify the uploaded packages for remote availability?                                       | No                                    | Upgrade package is authenticated through a digital signature.  |                               |                              |  |
| OTHR-2  | Are the operating system designed with least requirements in mind?   | Yes                                   | The Linux system is custom built to only support the minimal required components.  |                               |                              |  |

**Note-1:**

DICOM-TLS Security Profiles as defined in DICOM P3.15 on TLS-based security:

1. Disable, many customers may not be able to support DICOM-TLS server-side on their PACS.
2. Enable, non-downgrading TLS Secure profile.
3. Enable - allow downgrade, TLS but it allows downgrading of versions + ciphers as per BCP-195 requirement.

# Ambu



Ambu A/S  
Baltorpbakken 13  
DK-2750 Ballerup  
Denmark  
T +45 72 25 20 00  
ambu.com