BIOFIRE Diagnostics, LLC Question ID	BIOFIRE® SPOTFIRE® SYSTEM	BFR0001-8102-03	Luc - 47th 2024
Question ID			June 17th 2024
	Question		San nata
DOC-1	Question Manufacturer Name	BIOFIRE Diagnostics, LLC	See note
		The BIOFIRE SPOTFIRE System is an automated <i>in vitro</i> diagnostic (IVD) device intended for use with compatible BioFire IVD Panels to detect multiple nucleic acid targets contained in patient specimens. The BIOFIRE SPOTFIRE System interacts with the reagent pouch to both purify nucleic acids and amplify targeted nucleic acid sequences using nested multiplex polymerase chain reaction (nmPCR) in a closed system. The resulting PCR products are evaluated using DNA melting analysis. The software automatically determines the results and provides a test report. The BIOFIRE SPOTFIRE instrument is composed of one to four SPOTFIRE Modules connected to one	
		SPOTFIRE Control Station running the SPOTFIRE Application Software. The first Module is placed on top of the Control Station running the SPOTFIRE Application Software. The first Module is placed on top of the Control Station, subsequent modules are added as desired (up to four). Each SPOTFIRE Module can be randomly and independently accessed to run a reagent pouch. The SPOTFIRE software (comprised of the following software components: Application Software, Panel Software, and Connectivity Software) facilitates the collection, analysis, and storage of data on the SPOTFIRE System.	
		The BIOFIRE SPOTFIRE System is designed to be used in ambulatory care and clinical acute care testing environments but is expected to be used in a variety of healthcare settings. SPOTFIRE software will be delivered as a single software installation image with multiple components including the SPOTFIRE Application Software, SPOTFIRE Panel Software, and SPOTFIRE Connectivity Software. All software will be delivered to the customer pre-installed on the control station.	
		The BIOFIRE SPOTFIRE System, hereafter referred to as the "System," is designed to run as a standalone device.	
DOC-2	Device Description		
DOC-3	Device Model	BIOFIRE® SPOTFIRE® SYSTEM	
DOC-4	Document ID	BFR0001-8102-03 BIOFIRE Technical Support	
		Email: BioFiresupport@biomerieux.com	
DOC-5	Manufacturer Contact Information	Phone: +1-801-736-6354, select Option 5 The System is supported in a network-connected environment for purposes such as printing or archiving data to a network location. In addition, the System includes the following connectivity software feature that can be enabled in a network-connected environment.	
		The System can be configured to unidirectionally or bidirectionally interface with a Data Manager (LIS, POCT DMS, middleware) to transfer test results and other associated data to/from the System using one of several supported communication protocols. Specific connectivity software features will vary depending on the configured protocol. This optional connectivity software feature requires a connection to the local area network (LAN) at the facility. The System can be configured to interface with an institution-specific cloud-based data management and the local representative of the policy of protocol configured.	
		portal, inclusive of encrypted outbound transfer of Test and System Data. This optional software feature requires an Internet connection to a pre-defined endpoint. The System can be configured to facilitate remote access for customer support activities. This optional	
DOC-6 DOC-7	Intended use of device in network-connected environment: Document Release Date	software feature requires an Internet connection to pre-defined endpoints. June 17th 2024	_
DOC-8	Coordinated Vulnerability Disclosure: Does the manufacturer have a vulnerability disclosure program for this device?	Yes	
	ISAO: Is the manufacturer part of an Information Sharing and		_
DOC-9	Analysis Organization? Diagram: Is a network or data flow diagram available that indicates	Yes	_
DOC-10	connections to other system components or expected external resources?	Yes	_
DOC-11	SaMD: Is the device Software as a Medical Device (i.e. software- only, no hardware)?	No	
DOC-11.1	Does the SaMD contain an operating system? Does the SaMD rely on an owner/operator provided operating	N/A	
DOC-11.2	system?	N/A	_
DOC 11 3	Is the SaMD hosted by the manufacturer?	N/A	
DOC-11.3 DOC-11.4	Is the SaMD hosted by the customer?	N/A N/A	_
		Yes, No,	
		N/A, or See Note	Note #
	MANAGEMENT OF PERSONALLY IDENTIFIABLE INFORMATION		
MPII-1	Can this device display, transmit, store, or modify personally identifiable information (e.g. electronic Protected Health Information (ePHI))?	See Notes	Note 1
MPII-2	Does the device maintain personally identifiable information?	See Notes	
	Does the device maintain personally identifiable information temporarily in volatile memory (i.e., until cleared by power-off or		Note 2
MPII-2.1	reset)? Does the device store personally identifiable information	See Notes	Note 3
MPII-2.2	persistently on internal media? Is personally identifiable information preserved in the device's non-	See Notes	Note 4
MPII-2.3	volatile memory until explicitly erased? Does the device store personally identifiable information in a	See Notes	Note 5
	Lugge the device store personally identifiable information in a		
	database? Does the device allow configuration to automatically delete local	See Notes	Note 6

DIOCIDE D:	DIOCIDES CONTEIDES CYCTEA	PEROON 9103 03	luno 17th 2024
BIOFIRE Diagnostics, LLC	BIOFIRE® SPOTFIRE® SYSTEM	BFR0001-8102-03	June 17th 2024
	Does the device import/export personally identifiable information with other systems (e.g., a wearable monitoring device might export		
MPII-2.6	personally identifiable information to a server)?	See Notes	Note 8
-	Does the device maintain personally identifiable information when		
MPII-2.7	powered off, or during power service interruptions?	See Notes	Note 9
	Does the device allow the internal media to be removed by a service technician (e.g., for separate destruction or customer retention)?		
MPII-2.8		Yes	_
	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		
MPII-2.9	storage location)?	See Notes	Note 10
	Does the device have mechanisms used for the transmitting,		
MPII-3	importing/exporting of personally identifiable information? Does the device display personally identifiable information (e.g.,	See Notes	Note 11
MPII-3.1	video display, etc.)?	See Notes	Note 12
MPII-3.2	Does the device generate hardcopy reports or images containing personally identifiable information?	See Notes	Note 13
WII II 3.2		See Hotes	Note 15
	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		
MPII-3.3	card, memory stick, etc.)?	See Notes	Note 14
	Does the device transmit/receive or import/export personally		
	identifiable information via dedicated cable connection (e.g., RS-		
MPII-3.4	232, RS-423, USB, FireWire, etc.)?	See Notes	Note 15
	Does the device transmit/receive personally identifiable information		
MPII-3.5	via a wired network connection (e.g., RJ45, fiber optic, etc.)?	See Notes	Note 16
	Does the device transmit/receive personally identifiable information via a wireless network connection (e.g., WiFi, Bluetooth, NFC,		
MPII-3.6	infrared, cellular, etc.)? Does the device transmit/receive personally identifiable information	See Notes	Note 17
MPII-3.7	over an external network (e.g., Internet)?	No	_
	Does the device import personally identifiable information via		
MPII-3.8	scanning a document? Does the device transmit/receive personally identifiable information	No .	_
MPII-3.9	via a proprietary protocol?	No	_
MPII-3.10	Does the device use any other mechanism to transmit, import or export personally identifiable information?	No	
Management of Private Dat			
	AUTOMATIC LOGOFF (ALOF)		
	When do the fee follows he was a standard and a sta		
	The device's ability to prevent access and misuse by unauthorized users if device is left idle for a period of time.		
	Can the device he configured to force requite extention of larged in		
	Can the device be configured to force reauthorization of logged-in user(s) after a predetermined length of inactivity (e.g., auto-logoff,		
ALOF-1	session lock, password protected screen saver)?	Yes	_
ALOF-2	Is the length of inactivity time before auto-logoff/screen lock user or administrator configurable?	Yes	
	-		
	AUDIT CONTROLS (AUDT)		
	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?	Yes	
AUDT-1.1	Does the audit log record a USER ID?	Yes	_
AUDT-1.2	Does other personally identifiable information exist in the audit trail?	Yes	
7.031 1.2			
AUDT-2	Are events recorded in an audit log? If yes, indicate which of the following events are recorded in the audit log:	Yes	
AUDT-2.1	Successful login/logout attempts?	Yes Yes	
AUDT-2.2	Unsuccessful login/logout attempts?	Yes	_
AUDT-2.3 AUDT-2.4	Modification of user privileges? Creation/modification/deletion of users?	Yes Yes	_
AUDT-2.5	Presentation of clinical or PII data (e.g. display, print)?	No	
AUDT-2.6	Creation/modification/deletion of data?	Yes	_
AUDT-2.7	Import/export of data from removable media (e.g. USB drive, external hard drive, DVD)?	Yes	
	Receipt/transmission of data or commands over a network or point-		
AUDT-2.8 AUDT-2.8.1	to-point connection? Remote or on-site support?	Yes See Notes	Note 18
AUDT-2.8.2 AUDT-2.9	Application Programming Interface (API) and similar activity? Emergency access?	No No	
AUDT-2.10	Other events (e.g., software updates)?	Yes	_
AUDT-2.11	Is the audit capability documented in more detail? Can the owner/operator define or select which events are recorded	Yes	_
AUDT-3	in the audit log?	No	
AUDT-4	Is a list of data attributes that are captured in the audit log for an event available?	No	
AUDT-4.1	Does the audit log record date/time?	Yes	
	Can date and time be synchronized by Network Time Protocol (NTP)	See Notes	Note 10
AUDT-4.1.1 AUDT-5	or equivalent time source? Can audit log content be exported?	See Notes Yes	Note 19
AUDT-5.1	Via physical media?	Yes	
AUDT-5.2	Via IHE Audit Trail and Node Authentication (ATNA) profile to SIEM?	No	
			I—

	T		
BIOFIRE Diagnostics, LLC	BIOFIRE® SPOTFIRE® SYSTEM	BFR0001-8102-03	June 17th 2024
	Via Other communications (e.g., external service device, mobile		
AUDT-5.3 AUDT-5.4	applications)?	No No	_
AUD1-5.4	Are audit logs encrypted in transit or on storage media?	No .	_
AUDT-6	Can audit logs be monitored/reviewed by owner/operator?	Yes	_
AUDT-7 AUDT-7.1	Are audit logs protected from modification? Are audit logs protected from access?	Yes Yes	_
AUDT-8	Can audit logs be analyzed by the device?	No	_
	AUTHORIZATION (AUTH)		
	The ability of the device to determine the authorization of users. Does the device prevent access to unauthorized users through user		
AUTH-1	login requirements or other mechanism?	See Notes	Note 20
	Can the device be configured to use federated credentials		
AUTH-1.1	management of users for authorization (e.g., LDAP, OAuth)?	See Notes	Note 21
AUTH-1.2	Can the customer push group policies to the device (e.g., Active Directory)?	No	
A0111 1.2	Are any special groups, organizational units, or group policies	110	
AUTH-1.3	required?	No	_
AUTH-2	Can users be assigned different privilege levels based on 'role' (e.g., user, administrator, and/or service, etc.)?	See Notes	Note 22
	Can the device owner/operator grant themselves unrestricted administrative privileges (e.g., access operating system or		
AUTH-3	application via local root or administrator account)?	See Notes	Note 23
AUTH-4	Does the device authorize or control all API access requests?	Yes	
	Does the device run in a restricted access mode, or 'kiosk mode', by		_
AUTH-5	default?	Yes	_
 			
	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.		
	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		
CSUP-1	section. Does the device contain an Operating System? If yes, complete 2.1-	Yes	_
CSUP-2	2.4.	Yes	_
	Describe de la descripción del		
CSUP-2.1	Does the device documentation provide instructions for owner/operator installation of patches or software updates?	See Notes	Note 24
	Does the device require vendor or vendor-authorized service to		
CSUP-2.2	install patches or software updates? Does the device have the capability to receive remote installation of	No	_
CSUP-2.3	patches or software updates?	No	_
	Does the medical device manufacturer allow security updates from		
	any third-party manufacturers (e.g., Microsoft) to be installed		
CSUP-2.4	without approval from the manufacturer? Does the device contain Drivers and Firmware? If yes, complete 3.1-	See Notes	Note 25
CSUP-3	3.4.	Yes	
	Does the device desumentation remitted by the form		
CSUP-3.1	Does the device documentation provide instructions for owner/operator installation of patches or software updates?	Yes	
	Does the device require vendor or vendor-authorized service to		
CSUP-3.2	install patches or software updates? Does the device have the capability to receive remote installation of	See Notes	Note 26
CSUP-3.3	patches or software updates?	No	_
	Does the medical device manufacturer allow security updates from		
	any third-party manufacturers (e.g., Microsoft) to be installed		
CSUP-3.4	without approval from the manufacturer?	See Notes	Note 27
CSUP-4	Does the device contain Anti-Malware Software? If yes, complete 4.1-4.4.	Yes	
CSUP-4.1	Does the device documentation provide instructions for owner/operator installation of patches or software updates?	See Notes	Note 28
5501 7.1			20
•	Does the device require vendor or vendor-authorized service to		
CSUP-4.2	Does the device require vendor or vendor-authorized service to install patches or software updates?	No .	_
CSUP-4.2	Does the device require vendor or vendor-authorized service to		
	Does the device require vendor or vendor-authorized service to install patches or software updates? Does the device have the capability to receive remote installation of patches or software updates?	No	
	Does the device require vendor or vendor-authorized service to install patches or software updates? Does the device have the capability to receive remote installation of patches or software updates? Does the medical device manufacturer allow security updates from	No	
	Does the device require vendor or vendor-authorized service to install patches or software updates? Does the device have the capability to receive remote installation of patches or software updates?	No	
CSUP-4.3	Does the device require vendor or vendor-authorized service to install patches or software updates? Does the device have the capability to receive remote installation of patches or software updates? 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-4.3	Does the device require vendor or vendor-authorized service to install patches or software updates? Does the device have the capability to receive remote installation of patches or software updates? Does the medical device manufacturer allow security updates from any third-party manufacturers (e.g., Microsoft) to be installed	No	 Note 29
CSUP-4.3	Does the device require vendor or vendor-authorized service to install patches or software updates? Does the device have the capability to receive remote installation of patches or software updates? Does the medical device manufacturer allow security updates from any third-party manufacturers (e.g., Microsoft) to be installed without approval from the manufacturer? Does the device contain Non-Operating System commercial off-the-shelf components? If yes, complete 5.1-5.4.	No No See Notes	Note 29
CSUP-4.4 CSUP-5	Does the device require vendor or vendor-authorized service to install patches or software updates? Does the device have the capability to receive remote installation of patches or software updates? Does the medical device manufacturer allow security updates from any third-party manufacturers (e.g., Microsoft) to be installed without approval from the manufacturer? Does the device contain Non-Operating System commercial off-the-shelf components? If yes, complete 5.1-5.4. Does the device documentation provide instructions for	No No See Notes	Note 29
CSUP-4.4 CSUP-5 CSUP-5.1	Does the device require vendor or vendor-authorized service to install patches or software updates? Does the device have the capability to receive remote installation of patches or software updates? Does the medical device manufacturer allow security updates from any third-party manufacturers (e.g., Microsoft) to be installed without approval from the manufacturer? Does the device contain Non-Operating System commercial off-the-shelf components? If yes, complete 5.1-5.4. Does the device documentation provide instructions for owner/operator installation of patches or software updates? Does the device require vendor or vendor-authorized service to	No No See Notes Yes	Note 29
CSUP-4.4 CSUP-5	Does the device require vendor or vendor-authorized service to install patches or software updates? Does the device have the capability to receive remote installation of patches or software updates? Does the medical device manufacturer allow security updates from any third-party manufacturers (e.g., Microsoft) to be installed without approval from the manufacturer? Does the device contain Non-Operating System commercial off-the-shelf components? If yes, complete 5.1-5.4. Does the device documentation provide instructions for owner/operator installation of patches or software updates? Does the device require vendor or vendor-authorized service to install patches or software updates?	No See Notes Yes	Note 29
CSUP-4.4 CSUP-5 CSUP-5.1	Does the device require vendor or vendor-authorized service to install patches or software updates? Does the device have the capability to receive remote installation of patches or software updates? Does the medical device manufacturer allow security updates from any third-party manufacturers (e.g., Microsoft) to be installed without approval from the manufacturer? Does the device contain Non-Operating System commercial off-the-shelf components? If yes, complete 5.1-5.4. Does the device documentation provide instructions for owner/operator installation of patches or software updates? Does the device require vendor or vendor-authorized service to	No No See Notes Yes	Note 29
CSUP-4.4 CSUP-5 CSUP-5.1 CSUP-5.2	Does the device require vendor or vendor-authorized service to install patches or software updates? Does the device have the capability to receive remote installation of patches or software updates? Does the medical device manufacturer allow security updates from any third-party manufacturers (e.g., Microsoft) to be installed without approval from the manufacturer? Does the device contain Non-Operating System commercial off-the-shelf components? If yes, complete 5.1-5.4. Does the device documentation provide instructions for owner/operator installation of patches or software updates? Does the device require vendor or vendor-authorized service to install patches or software updates? Does the device have the capability to receive remote installation of patches or software updates?	No No See Notes Yes No Yes	Note 29
CSUP-4.4 CSUP-5 CSUP-5.1 CSUP-5.2	Does the device require vendor or vendor-authorized service to install patches or software updates? Does the device have the capability to receive remote installation of patches or software updates? Does the medical device manufacturer allow security updates from any third-party manufacturers (e.g., Microsoft) to be installed without approval from the manufacturer? Does the device contain Non-Operating System commercial off-the-shelf components? If yes, complete 5.1-5.4. Does the device documentation provide instructions for owner/operator installation of patches or software updates? Does the device require vendor or vendor-authorized service to install patches or software updates? Does the device have the capability to receive remote installation of	No No See Notes Yes No Yes	Note 29

BIOFIRE Diagnostics, LLC	BIOFIRE® SPOTFIRE® SYSTEM	BFR0001-8102-03	June 17th 2024
	Does the device contain other software components (e.g., asset		
CSUP-6	management software, license management)? If yes, please provide details or reference in notes and complete 6.1-6.4.	No	
	Does the device documentation provide instructions for		
CSUP-6.1	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	
	Does the device have the capability to receive remote installation of		
CSUP-6.3	patches or software updates?	N/A	
	Does the medical device manufacturer allow security updates from		
CSUP-6.4	any third-party manufacturers (e.g., Microsoft) to be installed without approval from the manufacturer?	N/A	
	Does the manufacturer notify the customer when updates are		
CSUP-7	approved for installation? Does the device perform automatic installation of software	Yes	_
CSUP-8	updates?	See Notes	Note 30
CSUP-9	Does the manufacturer have an approved list of third-party software that can be installed on the device?	No	
	Can the owner/operator install manufacturer-approved third-party	N/A	
CSUP-10	software on the device themselves? Does the system have mechanism in place to prevent installation of	N/A	_
CSUP-10.1	unapproved software?	N/A	_
CSUP-11	Does the manufacturer have a process in place to assess device vulnerabilities and updates?	Yes	_
	Does the manufacturer provide customers with review and approval		
CSUP-11.1 CSUP-11.2	status of updates? Is there an update review cycle for the device?	No Yes	
	HEALTH DATA DE IDEAL SE		
	HEALTH DATA DE-IDENTIFICATION (DIDT) 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?	See Notes	Note 31
	Does the device support de-identification profiles that comply with		
DIDT-1.1	the DICOM standard for de-identification?	N/A	_
	DATA DAGUUD AND DIG		
	DATA BACKUP AND DISASTER RECOVERY (DTBK)		
	The ability to recover after damage or destruction of device data,		
	hardware, software, or site configuration information.		
	hardware, software, or site configuration information. Does the device maintain long term primary storage of personally		
DTBK-1	Does the device maintain long term primary storage of personally identifiable information / patient information (e.g. PACS)?	See Notes	Note 32
	Does the device maintain long term primary storage of personally	See Notes Yes	Note 32
DTBK-1 DTBK-2	Does the device maintain long term primary storage of personally identifiable information / patient information (e.g. PACS)? Does the device have a "factory reset" function to restore the original device settings as provided by the manufacturer? Does the device have an integral data backup capability to	Yes	Note 32
DTBK-1 DTBK-2 DTBK-3	Does the device maintain long term primary storage of personally identifiable information / patient information (e.g. PACS)? Does the device have a "factory reset" function to restore the original device settings as provided by the manufacturer? Does the device have an integral data backup capability to removable media? Does the device have an integral data backup capability to remote	Yes Yes	Note 32
DTBK-1 DTBK-2	Does the device maintain long term primary storage of personally identifiable information / patient information (e.g. PACS)? Does the device have a "factory reset" function to restore the original device settings as provided by the manufacturer? Does the device have an integral data backup capability to removable media?	Yes	Note 32
DTBK-1 DTBK-2 DTBK-3	Does the device maintain long term primary storage of personally identifiable information / patient information (e.g. PACS)? Does the device have a "factory reset" function to restore the original device settings as provided by the manufacturer? Does the device have an integral data backup capability to removable media? Does the device have an integral data backup capability to remote	Yes Yes	Note 32
DTBK-1 DTBK-2 DTBK-3	Does the device maintain long term primary storage of personally identifiable information / patient information (e.g. PACS)? Does the device have a "factory reset" function to restore the original device settings as provided by the manufacturer? Does the device have an integral data backup capability to removable media? Does the device have an integral data backup capability to remove storage? Does the device have a backup capability for system configuration information, patch restoration, and software restoration?	Yes Yes	Note 32
DTBK-2 DTBK-3 DTBK-4	Does the device maintain long term primary storage of personally identifiable information / patient information (e.g. PACS)? Does the device have a "factory reset" function to restore the original device settings as provided by the manufacturer? Does the device have an integral data backup capability to removable media? Does the device have an integral data backup capability to remote storage? Does the device have an integral data backup capability to remote storage?	Yes Yes Yes	Note 32
DTBK-1 DTBK-2 DTBK-3 DTBK-4 DTBK-5	Does the device maintain long term primary storage of personally identifiable information / patient information (e.g. PACS)? Does the device have a "factory reset" function to restore the original device settings as provided by the manufacturer? Does the device have an integral data backup capability to removable media? Does the device have an integral data backup capability to removable media? Does the device have an integral data backup capability to remote storage? Does the device have a backup capability for system configuration information, patch restoration, and software restoration? Does the device provide the capability to check the integrity and	Yes Yes No	Note 32
DTBK-1 DTBK-2 DTBK-3 DTBK-4 DTBK-5	Does the device maintain long term primary storage of personally identifiable information / patient information (e.g. PACS)? Does the device have a "factory reset" function to restore the original device settings as provided by the manufacturer? Does the device have an integral data backup capability to removable media? Does the device have an integral data backup capability to removable media? Does the device have an integral data backup capability to remote storage? Does the device have a backup capability for system configuration information, patch restoration, and software restoration? Does the device provide the capability to check the integrity and	Yes Yes No	Note 32
DTBK-1 DTBK-2 DTBK-3 DTBK-4 DTBK-5	Does the device maintain long term primary storage of personally identifiable information / patient information (e.g. PACS)? Does the device have a "factory reset" function to restore the original device settings as provided by the manufacturer? Does the device have an integral data backup capability to removable media? Does the device have an integral data backup capability to removable media? Does the device have an integral data backup capability to remote storage? Does the device have a backup capability for system configuration information, patch restoration, and software restoration? Does the device provide the capability to check the integrity and authenticity of a backup? EMERGENCY ACCESS (EMRG)	Yes Yes No	Note 32
DTBK-1 DTBK-2 DTBK-3 DTBK-4 DTBK-5	Does the device maintain long term primary storage of personally identifiable information / patient information (e.g. PACS)? Does the device have a "factory reset" function to restore the original device settings as provided by the manufacturer? Does the device have an integral data backup capability to removable media? Does the device have an integral data backup capability to removable media? Does the device have an integral data backup capability to remote storage? Does the device have a backup capability for system configuration information, patch restoration, and software restoration? Does the device provide the capability to check the integrity and authenticity of a backup? EMERGENCY ACCESS [EMRG] The ability of the device user to access personally identifiable information in case of a medical emergency situation that requires	Yes Yes No	Note 32
DTBK-1 DTBK-2 DTBK-3 DTBK-4 DTBK-5	Does the device maintain long term primary storage of personally identifiable information / patient information (e.g. PACS)? Does the device have a "factory reset" function to restore the original device settings as provided by the manufacturer? Does the device have an integral data backup capability to removable media? Does the device have an integral data backup capability to removable media? Does the device have an integral data backup capability to remote storage? Does the device have a backup capability for system configuration information, patch restoration, and software restoration? Does the device provide the capability to check the integrity and authenticity of a backup? EMERGENCY ACCESS (EMRG) 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.	Yes Yes No	Note 32
DTBK-1 DTBK-2 DTBK-3 DTBK-4 DTBK-5	Does the device maintain long term primary storage of personally identifiable information / patient information (e.g. PACS)? Does the device have a "factory reset" function to restore the original device settings as provided by the manufacturer? Does the device have an integral data backup capability to removable media? Does the device have an integral data backup capability to removable media? Does the device have an integral data backup capability to remote storage? Does the device have a backup capability for system configuration information, patch restoration, and software restoration? Does the device provide the capability to check the integrity and authenticity of a backup? EMERGENCY ACCESS [EMRG] The ability of the device user to access personally identifiable information in case of a medical emergency situation that requires	Yes Yes No	Note 32
DTBK-1 DTBK-2 DTBK-3 DTBK-4 DTBK-5 DTBK-6	Does the device maintain long term primary storage of personally identifiable information / patient information (e.g. PACS)? Does the device have a "factory reset" function to restore the original device settings as provided by the manufacturer? Does the device have an integral data backup capability to removable media? Does the device have an integral data backup capability to removable media? Does the device have a backup capability for system configuration information, patch restoration, and software restoration? Does the device provide the capability to check the integrity and authenticity of a backup? EMERGENCY ACCESS (EMRG) 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. Does the device incorporate an emergency access (i.e. "break-	Yes Yes No Yes	Note 32
DTBK-1 DTBK-2 DTBK-3 DTBK-4 DTBK-5 DTBK-6	Does the device maintain long term primary storage of personally identifiable information / patient information (e.g. PACS)? Does the device have a "factory reset" function to restore the original device settings as provided by the manufacturer? Does the device have an integral data backup capability to removable media? Does the device have an integral data backup capability to removable media? Does the device have an integral data backup capability to remote storage? Does the device have a backup capability for system configuration information, patch restoration, and software restoration? Does the device provide the capability to check the integrity and authenticity of a backup? EMERGENCY ACCESS (EMRG) 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. Does the device incorporate an emergency access (i.e. "break-glass") feature?	Yes Yes No Yes	Note 32
DTBK-1 DTBK-2 DTBK-3 DTBK-4 DTBK-5 DTBK-6	Does the device maintain long term primary storage of personally identifiable information / patient information (e.g. PACS)? Does the device have a "factory reset" function to restore the original device settings as provided by the manufacturer? Does the device have an integral data backup capability to removable media? Does the device have an integral data backup capability to removable media? Does the device have an integral data backup capability to remote storage? Does the device have a backup capability for system configuration information, patch restoration, and software restoration? Does the device provide the capability to check the integrity and authenticity of a backup? EMERGENCY ACCESS (EMRG) 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. Does the device incorporate an emergency access (i.e. "break-glass") feature?	Yes Yes No Yes	Note 32
DTBK-1 DTBK-2 DTBK-3 DTBK-4 DTBK-5 DTBK-6	Does the device maintain long term primary storage of personally identifiable information / patient information (e.g. PACS)? Does the device have a "factory reset" function to restore the original device settings as provided by the manufacturer? Does the device have an integral data backup capability to removable media? Does the device have an integral data backup capability to removable media? Does the device have an integral data backup capability to remote storage? Does the device have a backup capability for system configuration information, patch restoration, and software restoration? Does the device provide the capability to check the integrity and authenticity of a backup? EMERGENCY ACCESS (EMRG) 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. Does the device incorporate an emergency access (i.e. "breakglass") feature? HEALTH DATA INTEGRITY AND AUTHENTICITY (IGAU) 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	Yes Yes No Yes	Note 32
DTBK-1 DTBK-2 DTBK-3 DTBK-4 DTBK-5 DTBK-6	Does the device maintain long term primary storage of personally identifiable information / patient information (e.g. PACS)? Does the device have a "factory reset" function to restore the original device settings as provided by the manufacturer? Does the device have an integral data backup capability to removable media? Does the device have an integral data backup capability to removable media? Does the device have a backup capability for system configuration information, patch restoration, and software restoration? Does the device provide the capability to check the integrity and authenticity of a backup? EMERGENCY ACCESS (EMRG) 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. Does the device incorporate an emergency access (i.e. "break-glass") feature? HEALTH DATA INTEGRITY AND AUTHENTICITY (IGAU) How the device ensures that the stored data on the device has not	Yes Yes No Yes	Note 32
DTBK-1 DTBK-2 DTBK-3 DTBK-4 DTBK-5 DTBK-6	Does the device maintain long term primary storage of personally identifiable information / patient information (e.g. PACS)? Does the device have a "factory reset" function to restore the original device settings as provided by the manufacturer? Does the device have an integral data backup capability to removable media? Does the device have an integral data backup capability to removable media? Does the device have an integral data backup capability to remote storage? Does the device have a backup capability for system configuration information, patch restoration, and software restoration? Does the device provide the capability to check the integrity and authenticity of a backup? EMERGENCY ACCESS (EMRG) 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. Does the device incorporate an emergency access (i.e. "breakglass") feature? HEALTH DATA INTEGRITY AND AUTHENTICITY (IGAU) 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. Does the device provide data integrity checking mechanisms of	Yes Yes Yes No No No	Note 32
DTBK-1 DTBK-2 DTBK-3 DTBK-4 DTBK-5 DTBK-6	Does the device maintain long term primary storage of personally identifiable information / patient information (e.g. PACS)? Does the device have a "factory reset" function to restore the original device settings as provided by the manufacturer? Does the device have an integral data backup capability to removable media? Does the device have an integral data backup capability to removable media? Does the device have a backup capability for system configuration information, patch restoration, and software restoration? Does the device provide the capability to check the integrity and authenticity of a backup? EMERGENCY ACCESS (EMRG) 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. Does the device incorporate an emergency access (i.e. "break-glass") feature? HEALTH DATA INTEGRITY AND AUTHENTICITY (IGAU) 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.	Yes Yes No Yes	Note 32
DTBK-1 DTBK-2 DTBK-3 DTBK-4 DTBK-5 DTBK-6 EMRG-1	Does the device maintain long term primary storage of personally identifiable information / patient information (e.g. PACS)? Does the device have a "factory reset" function to restore the original device settings as provided by the manufacturer? Does the device have an integral data backup capability to removable media? Does the device have an integral data backup capability to removable media? Does the device have an integral data backup capability to remote storage? Does the device have a backup capability for system configuration information, patch restoration, and software restoration? Does the device provide the capability to check the integrity and authenticity of a backup? EMERGENCY ACCESS (EMRG) 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. Does the device incorporate an emergency access (i.e. "breakglass") feature? HEALTH DATA INTEGRITY AND AUTHENTICITY (IGAU) 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. Does the device provide data integrity checking mechanisms of stored health data (e.g., hash or digital signature)? Does the device provide error/failure protection and recovery	Yes Yes Yes No No No No	Note 32
DTBK-1 DTBK-2 DTBK-3 DTBK-4 DTBK-5 DTBK-6	Does the device maintain long term primary storage of personally identifiable information / patient information (e.g. PACS)? Does the device have a "factory reset" function to restore the original device settings as provided by the manufacturer? Does the device have an integral data backup capability to removable media? Does the device have an integral data backup capability to removable media? Does the device have a backup capability for system configuration information, patch restoration, and software restoration? Does the device provide the capability to check the integrity and authenticity of a backup? EMERGENCY ACCESS (EMRG) 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. Does the device incorporate an emergency access (i.e. "break-glass") feature? HEALTH DATA INTEGRITY AND AUTHENTICITY (IGAU) 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. Does the device provide data integrity checking mechanisms of stored health data (e.g., hash or digital signature)?	Yes Yes Yes No No No	Note 32
DTBK-1 DTBK-2 DTBK-3 DTBK-4 DTBK-5 DTBK-6 EMRG-1	Does the device maintain long term primary storage of personally identifiable information / patient information (e.g. PACS)? Does the device have a "factory reset" function to restore the original device settings as provided by the manufacturer? Does the device have an integral data backup capability to removable media? Does the device have an integral data backup capability to removable media? Does the device have a backup capability for system configuration information, patch restoration, and software restoration? Does the device provide the capability to check the integrity and authenticity of a backup? EMERGENCY ACCESS (EMRG) 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. Does the device incorporate an emergency access (i.e. "breakglass") feature? HEALTH DATA INTEGRITY AND AUTHENTICITY (IGAU) 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. Does the device provide data integrity checking mechanisms of stored health data (e.g., hash or digital signature)? Does the device provide error/failure protection and recovery mechanisms for stored health data (e.g., RAID-5)?	Yes Yes Yes No No No No	Note 32
DTBK-1 DTBK-2 DTBK-3 DTBK-4 DTBK-5 DTBK-6 EMRG-1	Does the device maintain long term primary storage of personally identifiable information / patient information (e.g. PACS)? Does the device have a "factory reset" function to restore the original device settings as provided by the manufacturer? Does the device have an integral data backup capability to removable media? Does the device have an integral data backup capability to removable media? Does the device have an integral data backup capability to remote storage? Does the device have a backup capability for system configuration information, patch restoration, and software restoration? Does the device provide the capability to check the integrity and authenticity of a backup? EMERGENCY ACCESS (EMRG) 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. Does the device incorporate an emergency access (i.e. "break-glass") feature? HEALTH DATA INTEGRITY AND AUTHENTICITY (IGAU) 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. Does the device provide data integrity checking mechanisms of stored health data (e.g., hash or digital signature)? Does the device provide error/failure protection and recovery mechanisms for stored health data (e.g., RAID-5)?	Yes Yes Yes No No No No	Note 32
DTBK-1 DTBK-2 DTBK-3 DTBK-4 DTBK-5 DTBK-6 EMRG-1 IGAU-1 IGAU-2	Does the device maintain long term primary storage of personally identifiable information / patient information (e.g. PACS)? Does the device have a "factory reset" function to restore the original device settings as provided by the manufacturer? Does the device have an integral data backup capability to removable media? Does the device have an integral data backup capability to removable media? Does the device have a backup capability for system configuration information, patch restoration, and software restoration? Does the device provide the capability to check the integrity and authenticity of a backup? EMERGENCY ACCESS (EMRG) 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. Does the device incorporate an emergency access (i.e. "breakglass") feature? HEALTH DATA INTEGRITY AND AUTHENTICITY (IGAU) 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. Does the device provide data integrity checking mechanisms of stored health data (e.g., hash or digital signature)? Does the device provide error/failure protection and recovery mechanisms for stored health data (e.g., RAID-5)? MALWARE DETECTION/PROTECTION (MLDP) The ability of the device to effectively prevent, detect and remove malicious software (malware).	Yes Yes Yes No No No No	Note 32
DTBK-1 DTBK-2 DTBK-3 DTBK-4 DTBK-5 DTBK-6 EMRG-1	Does the device maintain long term primary storage of personally identifiable information / patient information (e.g. PACS)? Does the device have a "factory reset" function to restore the original device settings as provided by the manufacturer? Does the device have an integral data backup capability to removable media? Does the device have an integral data backup capability to removable media? Does the device have an integral data backup capability to removable media? Does the device have a backup capability for system configuration information, patch restoration, and software restoration? Does the device provide the capability to check the integrity and authenticity of a backup? EMERGENCY ACCESS (EMRG) 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. Does the device incorporate an emergency access (i.e. "break-glass") feature? HEALTH DATA INTEGRITY AND AUTHENTICITY (IGAU) 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. Does the device provide data integrity checking mechanisms of stored health data (e.g., hash or digital signature)? Does the device provide error/failure protection and recovery mechanisms for stored health data (e.g., RAID-5)? MALWARE DETECTION/PROTECTION (MLDP) The ability of the device to effectively prevent, detect and remove	Yes Yes Yes No No No No	Note 32
DTBK-1 DTBK-2 DTBK-3 DTBK-4 DTBK-5 DTBK-6 EMRG-1 IGAU-1 IGAU-2	Does the device maintain long term primary storage of personally identifiable information / patient information (e.g. PACS)? Does the device have a "factory reset" function to restore the original device settings as provided by the manufacturer? Does the device have an integral data backup capability to removable media? Does the device have an integral data backup capability to removable media? Does the device have a backup capability for system configuration information, patch restoration, and software restoration? Does the device provide the capability to check the integrity and authenticity of a backup? EMERGENCY ACCESS (EMRG) 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. Does the device incorporate an emergency access (i.e. "breakglass") feature? HEALTH DATA INTEGRITY AND AUTHENTICITY (IGAU) 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. Does the device provide data integrity checking mechanisms of stored health data (e.g., hash or digital signature)? Does the device provide error/failure protection and recovery mechanisms for stored health data (e.g., RAID-5)? MALWARE DETECTION/PROTECTION (MLDP) The ability of the device to effectively prevent, detect and remove malicious software (malware).	Yes Yes No No No No No No	Note 32
DTBK-1 DTBK-2 DTBK-3 DTBK-4 DTBK-5 DTBK-6 EMRG-1 IGAU-1 IGAU-2	Does the device maintain long term primary storage of personally identifiable information / patient information (e.g. PACS)? Does the device have a "factory reset" function to restore the original device settings as provided by the manufacturer? Does the device have an integral data backup capability to removable media? Does the device have an integral data backup capability to removable media? Does the device have a backup capability for system configuration information, patch restoration, and software restoration? Does the device provide the capability to check the integrity and authenticity of a backup? EMERGENCY ACCESS (EMRG) 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. Does the device incorporate an emergency access (i.e. "break-glass") feature? HEALTH DATA INTEGRITY AND AUTHENTICITY (IGAU) 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. Does the device provide data integrity checking mechanisms of stored health data (e.g., hash or digital signature)? Does the device provide error/failure protection and recovery mechanisms for stored health data (e.g., RAID-5)? MALWARE DETECTION/PROTECTION (MLDP) The ability of the device to effectively prevent, detect and remove malicious software (malware). Is the device capable of hosting executable software?	Yes Yes No No No No No No	Note 32
DTBK-1 DTBK-2 DTBK-3 DTBK-4 DTBK-5 DTBK-6 EMRG-1 IGAU-1 IGAU-2 MLDP-1	Does the device maintain long term primary storage of personally identifiable information / patient information (e.g. PACS)? Does the device have a "factory reset" function to restore the original device settings as provided by the manufacturer? Does the device have an integral data backup capability to removable media? Does the device have an integral data backup capability to removable media? Does the device have an integral data backup capability to removable media? Does the device have a backup capability for system configuration information, patch restoration, and software restoration? Does the device provide the capability to check the integrity and authenticity of a backup? EMERGENCY ACCESS (EMRG) 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. Does the device incorporate an emergency access (i.e. "break-glass") feature? HEALTH DATA INTEGRITY AND AUTHENTICITY (IGAU) 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. Does the device provide data integrity checking mechanisms of stored health data (e.g., hash or digital signature)? Does the device provide error/failure protection and recovery mechanisms for stored health data (e.g., RAID-5)? MALWARE DETECTION/PROTECTION (MLDP) The ability of the device to effectively prevent, detect and remove malicious software (malware). Is the device capable of hosting executable software?	Yes Yes No Yes No	Note 32
DTBK-1 DTBK-2 DTBK-3 DTBK-4 DTBK-5 DTBK-6 EMRG-1 IGAU-1 IGAU-2 MLDP-1 MLDP-2	Does the device maintain long term primary storage of personally identifiable information / patient information (e.g. PACS)? Does the device have a "factory reset" function to restore the original device settings as provided by the manufacturer? Does the device have an integral data backup capability to removable media? Does the device have an integral data backup capability to removable media? Does the device have a backup capability for system configuration information, patch restoration, and software restoration? Does the device provide the capability to check the integrity and authenticity of a backup? EMERGENCY ACCESS (EMRG) 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. Does the device incorporate an emergency access (i.e. "break-glass") feature? HEALTH DATA INTEGRITY AND AUTHENTICITY (IGAU) 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. Does the device provide data integrity checking mechanisms of stored health data (e.g., hash or digital signature)? Does the device provide error/failure protection and recovery mechanisms for stored health data (e.g., RAID-5)? MALWARE DETECTION/PROTECTION (MLDP) The ability of the device to effectively prevent, detect and remove malicious software (malware). Is the device capable of hosting executable software? Does the device support the use of anti-malware software (or other anti-malware mechanism)? Provide details or reference in notes.	Yes Yes No No No No Yes Yes Yes	Note 32

No. 1		T		1
March 1	BIOFIRE Diagnostics, LLC	BIOFIRE® SPOTFIRE® SYSTEM	BFR0001-8102-03	June 17th 2024
March 1				
March 1		Does the device documentation allow the owner/operator to install		
Comment Comm	MLDP-2.3		No	
See continuon of misses described on the described on the see of the seed of t				_
March 1964	MLDP-2.4		No	
AND 25 A CONTRACT CANADITIS CONTRACT AND CONTRACT CANADIT CONTRACT AND CONTRACT CANADIT CONTRACT AND CONTRACT CANADIT CONTRACT AND CONTRACT CANADIT CONTRACT AND CONTRACT CONTRACT CONTRACT CONTRACT	MIDD 2.5		No	
March Marc	MLDP-2.5		NO .	
MIRCH 1997	MLDP-2.6		See Notes	Note 33
March	MLDP-2.7			
If the amount of MITO-2 in				
March Section Sectio	MLDP-2.8		Yes	
MILEY 2. Outside the done is employ equication with bridge file in certain the MILEY 2. Outside and employ equication with the following the certain the properties of the certain properties of the cer				
Minch Online of an engine of the sea of the desire of the sea of the desire of the sea of the s	MLDP-3		N/A	_
Minch Online of an engine of the sea of the desire of the sea of the desire of the sea of the s				
MILES A Consideration requires that handed immanage and the control of the contro	MIDD 4		No.	
MID-52	IVILUP-4		INO	_
Main 1. de undique de la place colonier? All 199-2 de un format de la colonier d	MLDP-5		No	_
Con 2 hours because devotrous prevention agrient to 2 hours of the control of the		Can the host-based intrusion detection/prevention system be		
Marche Mode Authoritication Mode Mod	MLDP-5.1		N/A	_
NOTE AUTHORITICATION (NUM) See thing of the Court on commenced communication Court of the Court on commenced commenced communication Court of the Court on commenced c	MIDD E 2		See Notes	Note 35
Date ability of the device to confinence communication protects (mining a protect of more)	IVILDE-3.2	instance by the customer:	SEC NOCES	Note 33
Date ability of the device to confinence communication protects (mining a protect of more)				
COMECTUTY CAPABILITIES (COM) All referent processor and a few formation and a few formation of the section and the reference of the section and the section a		NODE AUTHENTICATION (NAUT)		
Does the device provide/support any means of mode subhentication that allow both the sunder and the response of data and known to the sunder and the response of data and known to the sunder and the response of data and known to the sunder and the response of data and known to the sunder and the response of data and known to the sunder and sundatable for review? Note: The forest content or content and sundatable for review? Occess the device use certificate based network connection and the sundatable for sevelum and the sunda				
AND 1		partners/nodes.		
AND 1		Does the device provide/support any means of node authentication		
INAUT 1 (ag. No. Afte, SAMTE, SAMTE, SAMTE) Are Restoria Access control mechanisms supported (E.g., does the election second mechanisms support election) All Arteriods and arrestorial support with the may be present on the election support election second the elec				
And the section access control mechanisms supported (E.g., does the device have an internal friend), or use a network connection where the section of the se				
AMAPT.2. In the financial ricevals, or use a network connection white here. INSERT STATE AND ST	NAUT-1		See Notes	Note 36
NAUT 2.1 Is the firewall rulesed documented and available for review? No NAUT 3.1 Stee firewall rulesed documented and available for review? No One the device up the critical based included and available for review? No Note that 3.2 Stee firewall rulesed documented and available for review? No NAUT 3.1 Stee firewall rulesed documented and available for review? No NAUT 3.2 Stee firewall rulesed documented and available for review? No NAUT 3.3 Stee firewall rulesed documented and available for review? No NAUT 3.4 And returned to and review connections must be considered in determining appealines but may be present on the efforts. CORNA 1.1 Docs the device support without you papelline? No CORNA 1.1 Docs the device support without you papelline? No CORNA 1.1 Docs the device support WIFF? No				
IAUT 2.1 Is the firewall inclused documented and available for review? Does the device use certificates based retreation connection Author 3 All network and removable media connections must be consistered in demanding appropries and produced in the connection of the connection o	NAUT-2		Yes	
Does the device successful and appropriate several processors of the foliage of t				
NAUT-3	NAUT-2.1		No	_
CONNECTIVITY CAPABILITIES (CONN) All network and removable media connections must be considered in adetermining appropriate security contrain. This section lists connectivity capabilities of may be present on the device. CONN-1 Does the device have hardware connections? CONN-1 11 Oces the device support diversely capabilities? CONN-1 12 Oces the device support diversely capabilities? CONN-1 13 Oces the device support diversely capabilities? CONN-1 14 Oces the device support diversely capabilities? CONN-1 15 Oces the device support diversely connections? To CONN-1 16 Constructions of the device support diversely connections? To CONN-1 17 Constructions of the device support diversely connections? To CONN-1 18 Oces the device support diversely connections? To CONN-1 19 Oces the device support diversely connections? To CONN-1 20 Oces the device support diversely connections? To CONN-1 21 Oces the device support diversely connections? To CONN-1 22 Oces the device support diversely connections? To CONN-1 23 Oces the device support diversely connections? To CONN-1 24 Oces the device support diversely connections? To CONN-1 25 Oces the device support diversely connections? To CONN-1 26 Oces the device support diversely connections? To CONN-1 27 Oces the device support other physical connections? To CONN-1 28 Oces the device support other physical connections? CONN-1 29 Oces the device support other physical connections? CONN-1 20 Oces the device communicate with other systems within the customer environment? CONN-1 20 Oces the device communicate with other systems within the customer environment (e.g., a service host)? To CONN-1 20 Oces the device require an internet connection for its intended use? CONN-2 Oces the device communicate with other systems within the customer environment (e.g., a service host)? To CONN-1 20 Oces the device support Tonsport Layer Security? To CONN-2 Oces the device communicate with other systems within the customer environment (e.g., a service host)? To CONN-2 Oc	NAUT 2		Con Notes	Note 27
All network and removable media connections must be considered in determining appropriate security controls. This section lists connectivity capabilities? CORN-1.1 CORN-1.1.1 CORN-1.1.2 CORN-1.1.1 CORN-1.1.3 CORN-1.1.3 CORN-1.1.3 CORN-1.1.4 CORN-1.1.4 CORN-1.1.4 CORN-1.1.5 CORN-1.1.5 CORN-1.1.5 CORN-1.1.5 CORN-1.1.6 CORN-1.1.6 CORN-1.1.7 CORN-1.1.7 CORN-1.1.7 CORN-1.1.8 CORN-1.1.9 CORN-1.1.9 CORN-1.1.9 CORN-1.1.9 CORN-1.1.0 CORN-1.1.0 CORN-1.1.0 CORN-1.1.1 CORN-1.1.1 CORN-1.1.1 CORN-1.1.2 CORN-1.1.2 CORN-1.1.3 CORN-1.1.3 CORN-1.1.3 CORN-1.1.3 CORN-1.1.4 CORN-1.1.4 CORN-1.1.5 CORN-1.1.5 CORN-1.1.5 CORN-1.1.5 CORN-1.1.6 CORN-1.1.7 CORN-1.1.7 CORN-1.1.7 CORN-1.1.8 CORN-1.1.9 CORN-1.9 CORN-1.1.9 CORN-1.1.9 CORN-1.1.9 CORN-1.1.9 CORN-1.1.9	NAU1-3	authentication?	see Notes	Note 37
All network and removable media connections must be considered in determining appropriate security controls. This section lists connectivity capabilities? CORN-1.1 CORN-1.1.1 CORN-1.1.2 CORN-1.1.1 CORN-1.1.3 CORN-1.1.3 CORN-1.1.3 CORN-1.1.4 CORN-1.1.4 CORN-1.1.4 CORN-1.1.5 CORN-1.1.5 CORN-1.1.5 CORN-1.1.5 CORN-1.1.6 CORN-1.1.6 CORN-1.1.7 CORN-1.1.7 CORN-1.1.7 CORN-1.1.8 CORN-1.1.9 CORN-1.1.9 CORN-1.1.9 CORN-1.1.9 CORN-1.1.0 CORN-1.1.0 CORN-1.1.0 CORN-1.1.1 CORN-1.1.1 CORN-1.1.1 CORN-1.1.2 CORN-1.1.2 CORN-1.1.3 CORN-1.1.3 CORN-1.1.3 CORN-1.1.3 CORN-1.1.4 CORN-1.1.4 CORN-1.1.5 CORN-1.1.5 CORN-1.1.5 CORN-1.1.5 CORN-1.1.6 CORN-1.1.7 CORN-1.1.7 CORN-1.1.7 CORN-1.1.8 CORN-1.1.9 CORN-1.9 CORN-1.1.9 CORN-1.1.9 CORN-1.1.9 CORN-1.1.9 CORN-1.1.9				
an determining appropriate security controls. This section lists connectivity operation the device. CONN-1.1 Does the device have hardware connectivity capabilities? See Notes Note 38 CONN-1.1 Does the device support where security (applications)? See Notes Note 100-1.1 Does the device support where security (applications)? Note 100-1.1 Does the device support where security (applications)? Note 100-1.1 Does the device support where security (applications)? Note 11.1 Does the device support the writes retirevis connectivity (applications). Obes the device support other writes connections (ap., custom RF) CONN-1.2 Does the device support other writes connections (ap., custom RF) CONN-1.2 Does the device support other writes connections? Note 100-1.1 Does the device support other writes connections? Note 100-1.1 Does the device support other physical connections? Yes CONN-1.2 Does the device support other physical connections? Note 100-1.1 Does the device support other physical connections? Note Notes CONN-1.2 Does the device support other physical connections? See Notes Note 40 CONN-1.2 Does the device support other physical connections? See Notes CONN-1.2 Does the device support other physical connections? See Notes Note 40 CONN-1.2 Does the device support other physical connections? See Notes Note 41 CONN-1.2 Does the device support other physical connections? See Notes Note 41 CONN-2 Does the device communicate with other systems within the customer environment? CONN-3 Connections and the device communicate with other systems within the customer environment? See Notes Note 41 CONN-1 Does the device make or receive AFI calls? See Notes Note 42 CONN-2 Does the device support and enforce unique (bits and passwords for all users and rother device controlling and a security? No Obes the device communicate unique (bits and passwords for all users and rother device controlling and security? No Obes the device configurable to gits out an administration of unique (bits and p		CONNECTIVITY CAPABILITIES (CONN)		
an determining appropriate security controls. This section lists connectivity operation the device. CONN-1.1 Does the device have hardware connectivity capabilities? See Notes Note 38 CONN-1.1 Does the device support where security (applications)? See Notes Note 100-1.1 Does the device support where security (applications)? Note 100-1.1 Does the device support where security (applications)? Note 100-1.1 Does the device support where security (applications)? Note 11.1 Does the device support the writes retirevis connectivity (applications). Obes the device support other writes connections (ap., custom RF) CONN-1.2 Does the device support other writes connections (ap., custom RF) CONN-1.2 Does the device support other writes connections? Note 100-1.1 Does the device support other writes connections? Note 100-1.1 Does the device support other physical connections? Yes CONN-1.2 Does the device support other physical connections? Note 100-1.1 Does the device support other physical connections? Note Notes CONN-1.2 Does the device support other physical connections? See Notes Note 40 CONN-1.2 Does the device support other physical connections? See Notes CONN-1.2 Does the device support other physical connections? See Notes Note 40 CONN-1.2 Does the device support other physical connections? See Notes Note 41 CONN-1.2 Does the device support other physical connections? See Notes Note 41 CONN-2 Does the device communicate with other systems within the customer environment? CONN-3 Connections and the device communicate with other systems within the customer environment? See Notes Note 41 CONN-1 Does the device make or receive AFI calls? See Notes Note 42 CONN-2 Does the device support and enforce unique (bits and passwords for all users and rother device controlling and a security? No Obes the device communicate unique (bits and passwords for all users and rother device controlling and security? No Obes the device configurable to gits out an administration of unique (bits and p				
CORN-1 1 Oces the device have hardware connectivity capabilities? See Notes No	1			
CONN-1 1 Obes the device have hardware connectivity capabilities? See Notes Notes 9. CONN-1.1 1 Obes the device support wireless connections? Yes 9. CONN-1.1 2 Obes the device support biller 197 Yes 9. CONN-1.1 3 Obes the device support biller biller 197 Yes 9. CONN-1.1 3 Obes the device support biller wireless retwork connectivity (e.g. 117, Zighee, proprietury)? CONN-1.1 3 Obes the device support other wireless connections (e.g., custom RF obs.) No 0				
CONN-1.1 Does the device support wireless connections? Yes		in determining appropriate security controls. This section lists		
CONN-1.11 Does the device support Other wireless network connectivity (e.g., Does the device support other wireless network connectivity (e.g., Does the device support other wireless network connectivity (e.g., CONN-1.1 Does the device support other wireless connections (e.g., custom F No Does the device support other wireless connections (e.g., custom F No Does the device support other wireless connections? Yes Does the device support physical connection? Yes Does the device support physical connection? Yes Does the device have available USB prots? Yes Does the device provide a last of network ports and protocols that are used or may be used on the device? Does the device communicate with other systems within the customer environment? See Notes Note 41 CONN-2 Can the device communicate with other systems within the customer environment? See Notes Note 42 CONN-3 Does the device communicate with other systems external to the customer environment? See Notes Note 43 CONN-1 Does the device make or rescribe APR Calls? See Notes Note 43 CONN-1 Does the device make or rescribe APR Calls? Yes Does the device have provide sperator control functionality from a sparnet device (e.g., telemedicine)? Yes Does the device support and reformation of unique 10s and Does the device support and reformation of unique 10s and Does the device support and reformation of unique 10s and Does the device support and reformation of unique 10s and Do		in determining appropriate security controls. This section lists		
Does the device support Bluetooth? Does the device support Support Support Device Support Device Support Device Support Supp	CONN-1	In determining appropriate security controls. This section lists connectivity capabilities that may be present on the device. Does the device have hardware connectivity capabilities?		Note 38
Does the device support other wireless network connectivity (e.g., 10.0NN-1.1.4 Does the device support other wireless connections (e.g., custom RF conN-1.2.1 Does the device have available to 18.5 them the prots? Ves ———————————————————————————————————	CONN-1.1	in determining appropriate security controls. This section lists connectivity capabilities that may be present on the device. Does the device have hardware connectivity capabilities? Does the device support wireless connections?	Yes	Note 38
CONN-1.1.3 LT. Zigbee, proprietary? Ones the device support of the wireless connections [e.g., custom RF CONN-1.1.4 controls, wireless detectors)? Ones the device support spring the wireless connections? CONN-1.2.1 Does the device have available IMS Ethernet ports? Ones the device require, use, or support removable memory devices? CONN-1.2.1 Does the device support other physical connectivity? Ones the device support other physical connectivity? Ones the device support other physical connectivity? Ones the device support other physical connectivity? CONN-2 Con the device communicate with other systems within the customer environment? CONN-4 customer environment [e.g., a service hoxt]? CONN-5 Opes the device make or receive API callis? CONN-6 Opes the device make or receive API callis? CONN-7 Opes the device make or receive API callis? Ones the device compunitate with other systems external to the customer environment [e.g., a service hoxt]? Yes CONN-7 Opes the device make or receive API callis? Ones the device support Transport Layer Security (TLS)? For Opiny to configurable? Ones the device support and enforce unique IDs and passwords for all users and roles (including service accounts)? Ones the device support and enforce unique IDs and passwords for all users and roles (including service accounts)? See Notes Ones the device support and enforce unique IDs and passwords for all users and roles (including service accounts)? See Notes Ones the device configurable to authenticate users. Ones the device configurable to outhenticate users through an external authentication service (e.g., MS Active Directory, NOS, LDAP, OAuth, Nos. LDAP, OAUth, N	CONN-1.1 CONN-1.1.1	in determining appropriate security controls. This section lists connectivity capabilities that may be present on the device. Does the device have hardware connectivity capabilities? Does the device support wireless connections? Does the device support Wi-Fi?	Yes Yes	Note 38
CONN-1.1.4 controls, writeless detectors]?	CONN-1.1 CONN-1.1.1	In determining appropriate security controls. This section lists connectivity capabilities that may be present on the device. Does the device have hardware connectivity capabilities? Does the device support Wireless connections? Does the device support Wi-Fi? Does the device support Bluetooth?	Yes Yes	Note 38
CONN-1.2 Does the device support physical connections? CONN-1.2.1 Does the device have available MS Ethernet ports? CONN-1.2.2 Does the device have available MS Ethernet ports? CONN-1.2.3 devices? CONN-1.2.4 Does the device require, use, or support removable memory CONN-1.2.4 Does the device support other physical connectivity? Does the device communicate with other systems within the customer environment? CONN-1.2.4 Does the device communicate with other systems within the customer environment? CONN-2 Can the device communicate with other systems within the customer environment? CONN-3 Can the device communicate with other systems within the customer environment? CONN-4 customer environment? CONN-5 Does the device make or receive API calls? CONN-6 Does the device support Transport Layer Security (TLS)? CONN-7 Does the device support Transport Layer Security (TLS)? CONN-7 Does the device support Transport Layer Security (TLS)? CONN-8 separate device (e.g., telemedicine)? PERSON AUTHENTICATION (PAUT) The ability to configurable to authenticate users. Does the device engiprable to authenticate users. Does the device configurable to authenticate users. Does the device configurable to authenticate users. See Notes See Notes Note 42 See Notes Note 43 See Notes Note 43 See Notes Note 43 See Notes Note 44 PAUT-1 Does the device support and enforce unique IDs and passwords for all users and roles (including service accounts)? See Notes Note 45 See Not	CONN-1.1 CONN-1.1.1 CONN-1.1.2	in determining appropriate security controls. This section lists connectivity capabilities that may be present on the device. Does the device have hardware connectivity capabilities? Does the device support Wi-Fi? Does the device support Bluetooth? Does the device support other wireless network connectivity (e.g.	Yes Yes No	Note 38
CONN-1.2.1 Does the device have available MAS Ethernet ports? Obest the device require, use, or support removable memory devices? CONN-1.2.3 Does the device support other physical connectivity? No Does the device support other physical connectivity? No Does the manufacturer provide a list of network ports and protocols that are used or may be used on the device? CONN-2.2 that are used or may be used on the device? CONN-3 customer environment? Can the device communicate with other systems within the customer environment? Can the device communicate with other systems external to the customer environment? CONN-5 Does the device make or receive API calls? CONN-6 Does the device require an internet connection for its intended use? CONN-7. Does the device support Transport Layer Security (TLS)? CONN-7. Does the device support Transport Layer Security (TLS)? CONN-7.1 STIS configurable? Obest the device provide operator control functionality from a sparate device (e.g., elemedicine)? PRESON AUTHENTICATION (PAUT) The ability to configure the device to authenticate users. Does the device enforce authentication of unique IDs and passwords for all users and roles (including service accounts)? Is the device configurable to authenticate users. Does the device enforce authentication of unique IDs and passwords for all users and roles (including service accounts)? See Notes See Notes Note 45 See Notes See Notes Note 45 See Notes See Notes Note 45	CONN-1.1 CONN-1.1.1 CONN-1.1.2 CONN-1.1.3	In determining appropriate security controls. This section lists connectivity capabilities that may be present on the device. Does the device have hardware connectivity capabilities? Does the device support Wireless connections? Does the device support Bluetooth? Does the device support other wireless network connectivity (e.g. LTE, Zigbee, proprietary)? Does the device support other wireless connections (e.g., custom RF	Yes Yes No	Note 38
CONN-1.2.1 Does the device have available USB ports? Does the device require, use, or support removable memory devices? CONN-1.2.3 devices? CONN-1.2.4 Does the device support other physical connectivity? Does the manufacturer provide a list of network ports and protocols that are used or may be used on the device? CONN-2 Can the device communicate with other systems within the customer environment? CONN-3 Can the device communicate with other systems external to the customer environment (e.g., a service host)? CONN-4 customer environment (e.g., a service host)? CONN-5 Does the device require an internet connection for its intended use? CONN-6 Does the device provide operator control functionality from a sparate device (e.g., telemedicine)? CONN-7 Does the device provide operator control functionality from a sparate device (e.g., telemedicine)? PERSON AUTHENTICATION (PAUT) The ability to configure the device to authenticate users. Does the device compliance to authenticate users through an external authentication service (e.g., MS Active Directory, NS), LOAP, OAUT, and authenticate on service (e.g., MS Active Directory, NS), LOAP, OAUT, No Is the device configurable to authenticate users through an external authentication service (e.g., MS Active Directory, NS), LOAP, OAUT, No Is the device configurable to authenticate users through an external authentication service (e.g., MS Active Directory, NS), LOAP, OAUT, No Is the device configurable to authenticate users through an external authentication service (e.g., MS Active Directory, NS), LOAP, OAUT, No Is the device configurable to authenticate users through an external authentication service (e.g., MS Active Directory, NS), LOAP, OAUT, No Is the device configurable to lock out a user after a certain number of the configurable to lock out a user after a certain number of the configurable to lock out a user after a certain number of the configurable to lock out a user after a certain number of the configurable to lock out a user after a certain n	CONN-1.1 CONN-1.1.1 CONN-1.1.2 CONN-1.1.3	In determining appropriate security controls. This section lists connectivity capabilities that may be present on the device. Does the device have hardware connectivity capabilities? Does the device support wireless connections? Does the device support Bluetooth? Does the device support other wireless network connectivity (e.g. LTE, Zigbee, proprietary)? Does the device support other wireless connections (e.g., custom RF controls, wireless detectors)?	Yes Yes No No	Note 38
CONN-1.2.3 devices? See Notes Note 40	CONN-1.1 CONN-1.1.1 CONN-1.1.2 CONN-1.1.3 CONN-1.1.4 CONN-1.2	In determining appropriate security controls. This section lists connectivity capabilities that may be present on the device. Does the device have hardware connectivity capabilities? Does the device support wireless connections? Does the device support Bluetooth? Does the device support other wireless network connectivity (e.g. LTE, Zigbee, proprietary)? Does the device support other wireless connections (e.g., custom RF controls, wireless detectors)? Does the device support other wireless connections (e.g., custom RF controls, wireless detectors)?	Yes Yes No No No Ves	Note 38
Does the device support other physical connectivity? Does the manufacturer provide a list of network ports and protocols that are used or may be used on the device? Can the device communicate with other systems within the customer environment? Can the device communicate with other systems external to the customer environment (e.g., a service host)? Connection of the device communicate with other systems external to the customer environment (e.g., a service host)? Connection of the device confluence of the device of the control of the device of the control of the device of the de	CONN-1.1 CONN-1.1.1 CONN-1.1.2 CONN-1.1.3 CONN-1.1.4 CONN-1.2 CONN-1.2	In determining appropriate security controls. This section lists connectivity capabilities that may be present on the device. Does the device have hardware connectivity capabilities? Does the device support wireless connections? Does the device support Bluetooth? Does the device support other wireless network connectivity (e.g. LTE, Zigbee, proprietary)? Does the device support other wireless connections (e.g., custom RF controls, wireless detectors)? Does the device support physical connections? Does the device have available RJ45 Ethernet ports?	Yes Yes No No Vo Yes Yes Yes	
Does the manufacturer provide a list of network ports and protocols that are used or may be used on the device? Can the device communicate with other systems within the customer environment? See Notes Note 41 Conn-2 Conn-3 Con the device communicate with other systems external to the customer environment (e.g., a service host)? See Notes Note 42 Conn-4 coustomer environment (e.g., a service host)? See Notes Note 43 Conn-5 Does the device require an internet connection for its intended use? No Oes the device support Transport Layer Security (TLS)? Yes CONN-7 Does the device support Transport Layer Security (TLS)? No Oes the device provide operator control functionality from a separate device (e.g., telemedicine)? Yes CONN-8 PERSON AUTHENTICATION (PAUT) The ability to configure the device to authenticate users. Does the device support and enforce unique IDs and passwords for all users and roles (including service accounts)? See Notes Note 45 By the device enforce authentication of unique IDs and passwords for all users and roles (including service accounts)? Is the device enforce authenticate users through an external authentication service (e.g., MS Active Directory, NDS, LDAP, ONuth, authenticate users through an external authentication service (e.g., MS Active Directory, NDS, LDAP, ONuth, No	CONN-1.1 CONN-1.1.1 CONN-1.1.2 CONN-1.1.3 CONN-1.1.4 CONN-1.2 CONN-1.2	In determining appropriate security controls. This section lists connectivity capabilities that may be present on the device. Does the device have hardware connectivity capabilities? Does the device support wireless connections? Does the device support Bluetooth? Does the device support Bluetooth? Does the device support other wireless network connectivity (e.g. LTE, Zigbee, proprietary)? Does the device support other wireless connections (e.g., custom RF controls, wireless detectors)? Does the device support physical connections? Does the device have available R445 Ethernet ports? Does the device have available USB ports?	Yes Yes No No Vo Yes Yes Yes	
CONN-2 that are used or may be used on the device? Can the device communicate with other systems within the customer environment? Can the device communicate with other systems external to the customer environment (e.g., a service host)? Conny-3 Does the device make or receive API calls? CONN-4 customer environment (e.g., a service host)? CONN-5 Does the device make or receive API calls? CONN-6 Does the device support Transport Layer Security (TLS)? Ves CONN-7.1 Is TLS configurable? Does the device support Transport Layer Security (TLS)? Ves CONN-8 separate device (e.g., telemedicine)? PERSON AUTHENTICATION (PAUT) The oblity to configure the device to authenticate users. Does the device enforce authentication of unique IDs and passwords for all users and roles (including service accounts)? See Notes Note 43 No PAUT-1 all sers and roles (including service accounts)? See Notes Note 44 Note 44 Note 44 Note 44 Note 45 See Notes Note 45 See Notes Note 45 See Notes	CONN-1.1 CONN-1.1.1 CONN-1.1.2 CONN-1.1.3 CONN-1.1.4 CONN-1.2 CONN-1.2 CONN-1.2.1 CONN-1.2.1 CONN-1.2.2 CONN-1.2.3	In determining appropriate security controls. This section lists connectivity capabilities that may be present on the device. Does the device have hardware connectivity capabilities? Does the device support wireless connections? Does the device support Bluetooth? Does the device support other wireless network connectivity (e.g. LTE, Zigbee, proprietary)? Does the device support other wireless connections (e.g., custom RF controls, wireless detectors)? Does the device support physical connections? Does the device have available RJ45 Ethernet ports? Does the device have available USB ports? Does the device have available USB ports? Does the device require, use, or support removable memory devices?	Yes Yes No No No See Notes See Notes	
CONN-2 that are used or may be used on the device? Can the device communicate with other systems within the customer environment? Can the device communicate with other systems external to the customer environment (e.g., a service host)? Conny-3 Does the device make or receive API calls? CONN-4 customer environment (e.g., a service host)? CONN-5 Does the device make or receive API calls? CONN-6 Does the device support Transport Layer Security (TLS)? Ves CONN-7.1 Is TLS configurable? Does the device support Transport Layer Security (TLS)? Ves CONN-8 separate device (e.g., telemedicine)? PERSON AUTHENTICATION (PAUT) The oblity to configure the device to authenticate users. Does the device enforce authentication of unique IDs and passwords for all users and roles (including service accounts)? See Notes Note 43 No PAUT-1 all sers and roles (including service accounts)? See Notes Note 44 Note 44 Note 44 Note 44 Note 45 See Notes Note 45 See Notes Note 45 See Notes	CONN-1.1 CONN-1.1.1 CONN-1.1.2 CONN-1.1.3 CONN-1.1.4 CONN-1.2 CONN-1.2 CONN-1.2.1 CONN-1.2.1 CONN-1.2.2 CONN-1.2.3	In determining appropriate security controls. This section lists connectivity capabilities that may be present on the device. Does the device have hardware connectivity capabilities? Does the device support wireless connections? Does the device support Bluetooth? Does the device support other wireless network connectivity (e.g. LTE, Zigbee, proprietary)? Does the device support other wireless connections (e.g., custom RF controls, wireless detectors)? Does the device support physical connections? Does the device have available RJ45 Ethernet ports? Does the device have available USB ports? Does the device have available USB ports? Does the device require, use, or support removable memory devices?	Yes Yes No No No See Notes See Notes	
CONN-3 customer environment? Can the device communicate with other systems external to the customer environment (e.g., a service host)? Does the device make or receive API calls? CONN-4 Does the device require an internet connection for its intended use? CONN-6 Does the device require an internet connection for its intended use? CONN-7 Does the device support Transport Layer Security (TLS)? Does the device support Transport Layer Security (TLS)? No CONN-7.1 Is TLS configurable? Does the device provide operator control functionality from a separate device (e.g., telemedicine)? PERSON AUTHENTICATION (PAUT) The ability to configure the device to authenticate users. Does the device support and enforce unique IDs and passwords for all users and roles (including service accounts)? See Notes Note 43 POUR SERVICE OF TRANSPORT OF TR	CONN-1.1 CONN-1.1.1 CONN-1.1.2 CONN-1.1.3 CONN-1.1.4 CONN-1.2 CONN-1.2 CONN-1.2.1 CONN-1.2.1 CONN-1.2.2 CONN-1.2.3	in determining appropriate security controls. This section lists connectivity capabilities that may be present on the device. Does the device have hardware connectivity capabilities? Does the device support wireless connections? Does the device support Bluetooth? Does the device support Bluetooth? Does the device support other wireless network connectivity (e.g. LTE, Zigbee, proprietary)? Does the device support other wireless connections (e.g., custom RF controls, wireless detectors)? Does the device support physical connections? Does the device have available RJ45 Ethernet ports? Does the device have available USB ports? Does the device require, use, or support removable memory devices? Does the device support other physical connectivity?	Yes Yes No No No See Notes See Notes	
Con the device communicate with other systems external to the customer environment (e.g., a service host)? CONN-5 Does the device make or receive API calls? See Notes Note 42 CONN-6 Does the device require an internet connection for its intended use? CONN-7 Does the device support Transport Layer Security (TLS)? Ves CONN-7.1 Is TLS configurable? No Does the device provide operator control functionality from a separate device (e.g., telemedicine)? PERSON AUTHENTICATION (PAUT) The ability to configure the device to authenticate users. Does the device support and enforce unique IDs and passwords for all users and roles (including service accounts)? Does the device enforce authentication of unique IDs and passwords for all users and roles (including service accounts)? See Notes Note 45 See Notes Note 45 See Notes Note 45 See Notes	CONN-1.1 CONN-1.1.1 CONN-1.1.2 CONN-1.1.3 CONN-1.1.4 CONN-1.2 CONN-1.2 CONN-1.2.1 CONN-1.2.1 CONN-1.2.2 CONN-1.2.3	In determining appropriate security controls. This section lists connectivity capabilities that may be present on the device. Does the device have hardware connectivity capabilities? Does the device support wireless connections? Does the device support Bluetooth? Does the device support Bluetooth? Does the device support other wireless network connectivity (e.g. LITE, Zigbee, proprietary)? Does the device support other wireless connections (e.g., custom RF controls, wireless detectors)? Does the device support physical connections? Does the device have available RJ45 Ethernet ports? Does the device have available RJ45 Ethernet ports? Does the device have available USB ports? Does the device require, use, or support removable memory devices? Does the device support other physical connectivity?	Yes Yes No No No See Notes No	
CONN-4 customer environment (e.g., a service host)? See Notes Note 42 CONN-5 Does the device make or receive API calls? See Notes No CONN-6 Does the device require an internet connection for its intended use? No CONN-7 Does the device support Transport Layer Security (TLS)? Yes CONN-7.1 Is TLS configurable? No CONN-8 separate device (e.g., telemedicine)? Yes CONN-8 separate device (e.g., telemedicine)? Yes PERSON AUTHENTICATION (PAUT) The ability to configure the device to authenticate users. Does the device support and enforce unique IDs and passwords for all users and roles (including service accounts)? See Notes PAUT-1 Does the device enforce authenticate user strough an external authentication service (e.g., MS Active Directory, NDS, LDAP, OAuth, PAUT-2 etc.)? Is the device configurable to block out a user after a certain number of the strough and external authentication service (e.g., MS Active Directory, NDS, LDAP, OAuth, No Is the device configurable to authenticate user after a certain number of the strough and external authentication service (e.g., MS Active Directory, NDS, LDAP, OAuth, No Is the device configurable to authenticate user after a certain number of the strough and external authentication service (e.g., MS Active Directory, NDS, LDAP, OAuth, No Is the device configurable to lock out a user after a certain number of the strough and external authenticate user after a certain number of the strough and external authenticate user after a certain number of the strough and external authenticate user after a certain number of the strough and external authenticate user after a certain number of the strough and external authenticate user after a certain number of the strough and external authenticate user after a certain number of the strough and external authenticate user after a certain number of the strough and the strough and external authenticate user after a certain number of the strough and the strough and the strough and external authenticate user after a certain number of the	CONN-1.1 CONN-1.1.1 CONN-1.1.2 CONN-1.1.3 CONN-1.1.4 CONN-1.2 CONN-1.2.1 CONN-1.2.1 CONN-1.2.2 CONN-1.2.3 CONN-1.2.4 CONN-2	in determining appropriate security controls. This section lists connectivity capabilities that may be present on the device. Does the device have hardware connectivity capabilities? Does the device support wireless connections? Does the device support Bluetooth? Does the device support other wireless network connectivity (e.g. LTE, Zigbee, proprietary)? Does the device support other wireless connections (e.g., custom RF controls, wireless detectors)? Does the device support other wireless connections (e.g., custom RF controls, wireless detectors)? Does the device have available RJ45 Ethernet ports? Does the device have available USB ports? Does the device require, use, or support removable memory devices? Does the device support other physical connectivity? Does the manufacturer provide a list of network ports and protocols that are used or may be used on the device? Can the device communicate with other systems within the	Yes Yes No No No No See Notes No	
CONN-4 customer environment (e.g., a service host)? See Notes Note 42 CONN-5 Does the device make or receive API calls? See Notes No CONN-6 Does the device require an internet connection for its intended use? No CONN-7 Does the device support Transport Layer Security (TLS)? Yes CONN-7.1 Is TLS configurable? No CONN-8 separate device (e.g., telemedicine)? Yes CONN-8 separate device (e.g., telemedicine)? Yes PERSON AUTHENTICATION (PAUT) The ability to configure the device to authenticate users. Does the device support and enforce unique IDs and passwords for all users and roles (including service accounts)? See Notes PAUT-1 Does the device enforce authenticate user strough an external authentication service (e.g., MS Active Directory, NDS, LDAP, OAuth, PAUT-2 etc.)? Is the device configurable to block out a user after a certain number of the strough and external authentication service (e.g., MS Active Directory, NDS, LDAP, OAuth, No Is the device configurable to authenticate user after a certain number of the strough and external authentication service (e.g., MS Active Directory, NDS, LDAP, OAuth, No Is the device configurable to authenticate user after a certain number of the strough and external authentication service (e.g., MS Active Directory, NDS, LDAP, OAuth, No Is the device configurable to lock out a user after a certain number of the strough and external authenticate user after a certain number of the strough and external authenticate user after a certain number of the strough and external authenticate user after a certain number of the strough and external authenticate user after a certain number of the strough and external authenticate user after a certain number of the strough and external authenticate user after a certain number of the strough and external authenticate user after a certain number of the strough and the strough and external authenticate user after a certain number of the strough and the strough and the strough and external authenticate user after a certain number of the	CONN-1.1 CONN-1.1.1 CONN-1.1.2 CONN-1.1.3 CONN-1.1.4 CONN-1.2 CONN-1.2 CONN-1.2.1 CONN-1.2.1 CONN-1.2.2 CONN-1.2.3 CONN-1.2.4	in determining appropriate security controls. This section lists connectivity capabilities that may be present on the device. Does the device have hardware connectivity capabilities? Does the device support wireless connections? Does the device support Bluetooth? Does the device support other wireless network connectivity (e.g. LTE, Zigbee, proprietary)? Does the device support other wireless connections (e.g., custom RF controls, wireless detectors)? Does the device support other wireless connections (e.g., custom RF controls, wireless detectors)? Does the device have available RJ45 Ethernet ports? Does the device have available USB ports? Does the device require, use, or support removable memory devices? Does the device support other physical connectivity? Does the manufacturer provide a list of network ports and protocols that are used or may be used on the device? Can the device communicate with other systems within the	Yes Yes No No No No See Notes No	
CONN-5 Does the device make or receive API calls? Does the device require an internet connection for its intended use? CONN-7 Does the device support Transport Layer Security (TLS)? Is TLS configurable? Does the device provide operator control functionality from a separate device (e.g., telemedicine)? PERSON AUTHENTICATION (PAUT) The ability to configure the device to authenticate users. Does the device support and enforce unique IDs and passwords for all users and roles (including service accounts)? Is the device configurable to authenticate users through an external authentication service (e.g., MS Active Directory, NDS, LDAP, OAUth, PAUT-2 Is the device configurable to lock out a user after a certain number See Notes Note 43 No Ves Ves Ves Ves Ves Ves See Notes Note 44 See Notes Note 44 No Ves See Notes Note 45 Is the device configurable to outhenticate users through an external authentication service (e.g., MS Active Directory, NDS, LDAP, OAUth, No Is the device configurable to lock out a user after a certain number	CONN-1.1 CONN-1.1.1 CONN-1.1.2 CONN-1.1.3 CONN-1.1.4 CONN-1.2 CONN-1.2.1 CONN-1.2.1 CONN-1.2.2 CONN-1.2.3 CONN-1.2.4 CONN-2	in determining appropriate security controls. This section lists connectivity capabilities that may be present on the device. Does the device have hardware connectivity capabilities? Does the device support wireless connections? Does the device support Bluetooth? Does the device support Bluetooth? Does the device support other wireless network connectivity (e.g. LTE, Zigbee, proprietary)? Does the device support other wireless connections (e.g., custom RF controls, wireless detectors)? Does the device support physical connections? Does the device have available RJ45 Ethernet ports? Does the device have available RJ45 Ethernet ports? Does the device require, use, or support removable memory devices? Does the device support other physical connectivity? Does the manufacturer provide a list of network ports and protocols that are used or may be used on the device? Can the device communicate with other systems within the customer environment?	Yes Yes No No No No See Notes No	
CONN-7 Does the device support Transport Layer Security (TLS)? CONN-7.1 Is TLS configurable? Does the device provide operator control functionality from a separate device (e.g., telemedicine)? PERSON AUTHENTICATION (PAUT) The ability to configure the device to authenticate users. Does the device support and enforce unique IDs and passwords for all users and roles (including service accounts)? See Notes Note 44 PAUT-1.1 passwords for all users and roles (including service accounts)? Is the device configurable to authenticate users through an external authentication service (e.g., MS Active Directory, NDS, LDAP, OAuth, etc.)? Is the device configurable to lock out a user after a certain number Ves	CONN-1.1 CONN-1.1.1 CONN-1.1.2 CONN-1.1.3 CONN-1.1.4 CONN-1.2 CONN-1.2.1 CONN-1.2.1 CONN-1.2.2 CONN-1.2.3 CONN-1.2.4 CONN-2	in determining appropriate security controls. This section lists connectivity capabilities that may be present on the device. Does the device have hardware connectivity capabilities? Does the device support wireless connections? Does the device support Bluetooth? Does the device support other wireless network connectivity (e.g. LTE, Zigbee, proprietary)? Does the device support other wireless connections (e.g., custom RF controls, wireless detectors)? Does the device support physical connections? Does the device have available RJ45 Ethernet ports? Does the device have available RJ45 Ethernet ports? Does the device require, use, or support removable memory devices? Does the device or may be used on the device? Can the device communicate with other systems within the customer environment? Can the device communicate with other systems external to the customer environment (e.g., a service host)?	Yes Yes No No No No See Notes No See Notes	Note 40 Note 41 Note 42
CONN-7 Does the device support Transport Layer Security (TLS)? CONN-7.1 Is TLS configurable? Does the device provide operator control functionality from a separate device (e.g., telemedicine)? PERSON AUTHENTICATION (PAUT) The ability to configure the device to authenticate users. Does the device support and enforce unique IDs and passwords for all users and roles (including service accounts)? See Notes Note 44 PAUT-1.1 passwords for all users and roles (including service accounts)? Is the device configurable to authenticate users through an external authentication service (e.g., MS Active Directory, NDS, LDAP, OAuth, etc.)? Is the device configurable to lock out a user after a certain number Ves	CONN-1.1 CONN-1.1.1 CONN-1.1.2 CONN-1.1.3 CONN-1.1.4 CONN-1.2 CONN-1.2.1 CONN-1.2.1 CONN-1.2.2 CONN-1.2.3 CONN-1.2.4 CONN-1.2.4 CONN-2	in determining appropriate security controls. This section lists connectivity capabilities that may be present on the device. Does the device have hardware connectivity capabilities? Does the device support wireless connections? Does the device support Bluetooth? Does the device support other wireless network connectivity (e.g. LTE, Zigbee, proprietary)? Does the device support other wireless connections (e.g., custom RF controls, wireless detectors)? Does the device support physical connections? Does the device have available RJ45 Ethernet ports? Does the device have available RJ45 Ethernet ports? Does the device require, use, or support removable memory devices? Does the device or may be used on the device? Can the device communicate with other systems within the customer environment? Can the device communicate with other systems external to the customer environment (e.g., a service host)?	Yes Yes No No No No No See Notes See Notes See Notes	Note 40 Note 41 Note 42
CONN-7.1 Is TLS configurable? Does the device provide operator control functionality from a separate device (e.g., telemedicine)? PERSON AUTHENTICATION (PAUT) The ability to configure the device to authenticate users. Does the device support and enforce unique IDs and passwords for all users and roles (including service accounts)? See Notes Note 44 Does the device enforce authentication of unique IDs and passwords for all users and roles (including service accounts)? Is the device configurable to authenticate users through an external authentication service (e.g., MS Active Directory, NDS, LDAP, OAuth, etc.)? Is the device configurable to lock out a user after a certain number See Notes Note 45 See Notes Note 45 See Notes	CONN-1.1 CONN-1.1.1 CONN-1.1.2 CONN-1.1.3 CONN-1.1.4 CONN-1.2 CONN-1.2.1 CONN-1.2.1 CONN-1.2.2 CONN-1.2.3 CONN-1.2.4 CONN-3 CONN-3 CONN-3	in determining appropriate security controls. This section lists connectivity capabilities that may be present on the device. Does the device have hardware connectivity capabilities? Does the device support wireless connections? Does the device support bluetooth? Does the device support Bluetooth? Does the device support other wireless network connectivity (e.g. LTE, Zigbee, proprietary)? Does the device support other wireless connections (e.g., custom RF controls, wireless detectors)? Does the device support other wireless connections (e.g., custom RF controls, wireless detectors)? Does the device support physical connections? Does the device have available USB ports? Does the device have available USB ports? Does the device require, use, or support removable memory devices? Does the device support other physical connectivity? Does the device support other physical connectivity? Can the device communicate with other systems within the customer environment? Can the device communicate with other systems external to the customer environment (e.g., a service host)? Does the device make or receive API calls?	Yes Yes No No No No No See Notes See Notes See Notes See Notes See Notes	Note 40 Note 41 Note 42
CONN-7.1 Is TLS configurable? Does the device provide operator control functionality from a separate device (e.g., telemedicine)? PERSON AUTHENTICATION (PAUT) The ability to configure the device to authenticate users. Does the device support and enforce unique IDs and passwords for all users and roles (including service accounts)? See Notes Note 44 Does the device enforce authentication of unique IDs and passwords for all users and roles (including service accounts)? Is the device configurable to authenticate users through an external authentication service (e.g., MS Active Directory, NDS, LDAP, OAuth, etc.)? Is the device configurable to lock out a user after a certain number See Notes Note 45 See Notes Note 45 See Notes	CONN-1.1 CONN-1.1.1 CONN-1.1.2 CONN-1.1.3 CONN-1.1.4 CONN-1.2 CONN-1.2 CONN-1.2 CONN-1.2.1 CONN-1.2.2 CONN-1.2.3 CONN-1.2.4 CONN-2 CONN-2 CONN-3	in determining appropriate security controls. This section lists connectivity capabilities that may be present on the device. Does the device have hardware connectivity capabilities? Does the device support wireless connections? Does the device support bluetooth? Does the device support Bluetooth? Does the device support other wireless network connectivity (e.g. LTE, Zigbee, proprietary)? Does the device support other wireless connections (e.g., custom RF controls, wireless detectors)? Does the device support other wireless connections (e.g., custom RF controls, wireless detectors)? Does the device support physical connections? Does the device have available USB ports? Does the device have available USB ports? Does the device require, use, or support removable memory devices? Does the device support other physical connectivity? Does the device support other physical connectivity? Can the device communicate with other systems within the customer environment? Can the device communicate with other systems external to the customer environment (e.g., a service host)? Does the device make or receive API calls?	Yes Yes No No No No No See Notes See Notes See Notes See Notes See Notes	Note 40 Note 41 Note 42
CONN-8 separate device (e.g., telemedicine)? PERSON AUTHENTICATION (PAUT) The ability to configure the device to authenticate users. Does the device support and enforce unique IDs and passwords for all users and roles (including service accounts)? PAUT-1 all users and roles (including service accounts)? Does the device enforce authentication of unique IDs and passwords for all users and roles (including service accounts)? See Notes Note 44 PAUT-1.1 passwords for all users and roles (including service accounts)? Is the device configurable to authenticate users through an external authentication service (e.g., MS Active Directory, NDS, LDAP, OAuth, PAUT-2 etc.)? Is the device configurable to lock out a user after a certain number Is the device configurable to lock out a user after a certain number	CONN-1.1 CONN-1.1.1 CONN-1.1.2 CONN-1.1.3 CONN-1.1.4 CONN-1.2 CONN-1.2.1 CONN-1.2.1 CONN-1.2.2 CONN-1.2.3 CONN-1.2.4 CONN-2 CONN-2 CONN-5 CONN-5 CONN-5	in determining appropriate security controls. This section lists connectivity capabilities that may be present on the device. Does the device have hardware connectivity capabilities? Does the device support wireless connections? Does the device support Bluetooth? Does the device support other wireless network connectivity (e.g. LTE, Zigbee, proprietary)? Does the device support other wireless connections (e.g., custom RF controls, wireless detectors)? Does the device support other wireless connections? Does the device support physical connections? Does the device have available RJ45 Ethernet ports? Does the device have available RJ45 Ethernet ports? Does the device require, use, or support removable memory devices? Does the device support other physical connectivity? Does the device support other physical connectivity? Does the device support other physical connectivity? Can the device communicate with other systems within the customer environment? Can the device communicate with other systems external to the customer environment (e.g., a service host)? Does the device make or receive API calls?	Yes Yes No No No No No No See Notes See Notes See Notes See Notes See Notes	Note 40 Note 41 Note 42
PERSON AUTHENTICATION (PAUT) The ability to configure the device to authenticate users. Does the device support and enforce unique IDs and passwords for all users and roles (including service accounts)? See Notes Note 44 PAUT-1.1 passwords for all users and roles (including service accounts)? Is the device configurable to authenticate users through an external authentication service (e.g., MS Active Directory, NDS, LDAP, OAuth, etc.)? Is the device configurable to lock out a user after a certain number Is the device configurable to lock out a user after a certain number	CONN-1.1 CONN-1.1.1 CONN-1.1.2 CONN-1.1.3 CONN-1.1.4 CONN-1.2 CONN-1.2 CONN-1.2.1 CONN-1.2.1 CONN-1.2.2 CONN-1.2.3 CONN-1.2.4 CONN-1.2.4 CONN-2 CONN-3 CONN-3 CONN-6 CONN-6 CONN-6	in determining appropriate security controls. This section lists connectivity capabilities that may be present on the device. Does the device have hardware connectivity capabilities? Does the device support wireless connections? Does the device support bluetooth? Does the device support other wireless network connectivity (e.g. LTE, Zigbee, proprietary)? Does the device support other wireless network connectivity (e.g. LTE, Zigbee, proprietary)? Does the device support other wireless connections (e.g., custom RF controls, wireless detectors)? Does the device support physical connections? Does the device have available USB ports? Does the device have available USB ports? Does the device require, use, or support removable memory devices? Does the device support other physical connectivity? Does the device support other physical connectivity? Can the device communicate with other systems within the customer environment? Can the device communicate with other systems external to the customer environment (e.g., a service host)? Does the device make or receive API calls? Does the device require an internet connection for its intended use? Does the device support Transport Layer Security (TLS)?	Yes Yes No No No No No No No See Notes See Notes No See Notes No No See Notes	Note 40 Note 41 Note 42
The ability to configure the device to authenticate users. Does the device support and enforce unique IDs and passwords for all users and roles (including service accounts)? See Notes Note 44 Does the device enforce authentication of unique IDs and passwords for all users and roles (including service accounts)? Is the device configurable to authenticate users through an external authentication service (e.g., MS Active Directory, NDS, LDAP, OAuth, etc.)? Is the device configurable to lock out a user after a certain number Is the device configurable to lock out a user after a certain number	CONN-1.1 CONN-1.1.1 CONN-1.1.2 CONN-1.1.3 CONN-1.1.4 CONN-1.2 CONN-1.2.1 CONN-1.2.1 CONN-1.2.2 CONN-1.2.3 CONN-1.2.4 CONN-2 CONN-2 CONN-5 CONN-5 CONN-6 CONN-5	in determining appropriate security controls. This section lists connectivity capabilities that may be present on the device. Does the device have hardware connectivity capabilities? Does the device support wireless connections? Does the device support Bluetooth? Does the device support bluetooth? Does the device support other wireless network connectivity (e.g. LTE, Zigbee, proprietary)? Does the device support other wireless connections (e.g., custom RF controls, wireless detectors)? Does the device support other wireless connections? Does the device have available RJ45 Ethernet ports? Does the device have available RJ45 Ethernet ports? Does the device have available RJ45 Ethernet ports? Does the device require, use, or support removable memory devices? Does the device support other physical connectivity? Does the manufacturer provide a list of network ports and protocols that are used or may be used on the device? Can the device communicate with other systems within the customer environment? Can the device communicate with other systems external to the customer environment (e.g., a service host)? Does the device make or receive API calls? Does the device make or receive API calls? Does the device support Transport Layer Security (TLS)? Is s TLS configurable? Does the device provide operator control functionality from a	Yes Yes No No No No No No See Notes See Notes See Notes See Notes No No See Notes See Notes	Note 40 Note 41 Note 42
The ability to configure the device to authenticate users. Does the device support and enforce unique IDs and passwords for all users and roles (including service accounts)? See Notes Note 44 Does the device enforce authentication of unique IDs and passwords for all users and roles (including service accounts)? Is the device configurable to authenticate users through an external authentication service (e.g., MS Active Directory, NDS, LDAP, OAuth, etc.)? Is the device configurable to lock out a user after a certain number Is the device configurable to lock out a user after a certain number	CONN-1.1 CONN-1.1.1 CONN-1.1.2 CONN-1.1.3 CONN-1.1.4 CONN-1.2 CONN-1.2.1 CONN-1.2.1 CONN-1.2.2 CONN-1.2.3 CONN-1.2.4 CONN-2 CONN-2 CONN-5 CONN-5 CONN-6 CONN-5	in determining appropriate security controls. This section lists connectivity capabilities that may be present on the device. Does the device have hardware connectivity capabilities? Does the device support wireless connections? Does the device support Bluetooth? Does the device support bluetooth? Does the device support other wireless network connectivity (e.g. LTE, Zigbee, proprietary)? Does the device support other wireless connections (e.g., custom RF controls, wireless detectors)? Does the device support other wireless connections? Does the device have available RJ45 Ethernet ports? Does the device have available RJ45 Ethernet ports? Does the device have available RJ45 Ethernet ports? Does the device require, use, or support removable memory devices? Does the device support other physical connectivity? Does the manufacturer provide a list of network ports and protocols that are used or may be used on the device? Can the device communicate with other systems within the customer environment? Can the device communicate with other systems external to the customer environment (e.g., a service host)? Does the device make or receive API calls? Does the device make or receive API calls? Does the device support Transport Layer Security (TLS)? Is s TLS configurable? Does the device provide operator control functionality from a	Yes Yes No No No No No No See Notes See Notes See Notes See Notes No No See Notes See Notes	Note 40 Note 41 Note 42
The ability to configure the device to authenticate users. Does the device support and enforce unique IDs and passwords for all users and roles (including service accounts)? See Notes Note 44 Does the device enforce authentication of unique IDs and passwords for all users and roles (including service accounts)? Is the device configurable to authenticate users through an external authentication service (e.g., MS Active Directory, NDS, LDAP, OAuth, etc.)? Is the device configurable to lock out a user after a certain number Is the device configurable to lock out a user after a certain number	CONN-1.1 CONN-1.1.1 CONN-1.1.2 CONN-1.1.3 CONN-1.1.4 CONN-1.2 CONN-1.2.1 CONN-1.2.1 CONN-1.2.2 CONN-1.2.3 CONN-1.2.4 CONN-2 CONN-2 CONN-5 CONN-5 CONN-6 CONN-5	in determining appropriate security controls. This section lists connectivity capabilities that may be present on the device. Does the device have hardware connectivity capabilities? Does the device support wireless connections? Does the device support Bluetooth? Does the device support bluetooth? Does the device support other wireless network connectivity (e.g. LTE, Zigbee, proprietary)? Does the device support other wireless connections (e.g., custom RF controls, wireless detectors)? Does the device support other wireless connections? Does the device have available RJ45 Ethernet ports? Does the device have available RJ45 Ethernet ports? Does the device have available RJ45 Ethernet ports? Does the device require, use, or support removable memory devices? Does the device support other physical connectivity? Does the manufacturer provide a list of network ports and protocols that are used or may be used on the device? Can the device communicate with other systems within the customer environment? Can the device communicate with other systems external to the customer environment (e.g., a service host)? Does the device make or receive API calls? Does the device make or receive API calls? Does the device support Transport Layer Security (TLS)? Is s TLS configurable? Does the device provide operator control functionality from a	Yes Yes No No No No No No See Notes See Notes See Notes See Notes No No See Notes See Notes	Note 40 Note 41 Note 42
Does the device support and enforce unique IDs and passwords for all users and roles (including service accounts)? Does the device enforce authentication of unique IDs and passwords for all users and roles (including service accounts)? Is the device configurable to authenticate users through an external authentication service (e.g., MS Active Directory, NDS, LDAP, OAuth, etc.)? Is the device configurable to lock out a user after a certain number Is the device configurable to lock out a user after a certain number	CONN-1.1 CONN-1.1.1 CONN-1.1.2 CONN-1.1.3 CONN-1.1.4 CONN-1.2 CONN-1.2.1 CONN-1.2.1 CONN-1.2.2 CONN-1.2.3 CONN-1.2.4 CONN-2 CONN-2 CONN-5 CONN-5 CONN-6 CONN-5	in determining appropriate security controls. This section lists connectivity capabilities that may be present on the device. Does the device have hardware connectivity capabilities? Does the device support wireless connections? Does the device support Bluetooth? Does the device support other wireless network connectivity (e.g. LTE, Zigbee, proprietary)? Does the device support other wireless connections (e.g., custom RF controls, wireless detectors)? Does the device support other wireless connections (e.g., custom RF controls, wireless detectors)? Does the device support physical connections? Does the device have available RJ45 Ethernet ports? Does the device have available RJ45 Ethernet ports? Does the device require, use, or support removable memory devices? Does the device support other physical connectivity? Does the manufacturer provide a list of network ports and protocols that are used or may be used on the device? Can the device communicate with other systems within the customer environment? Can the device communicate with other systems external to the customer environment (e.g., a service host)? Does the device make or receive API calls? Does the device support Transport Layer Security (TLS)? Is TLS configurable? Does the device envired operator control functionality from a separate device (e.g., telemedicine)?	Yes Yes No No No No No No See Notes See Notes See Notes See Notes No No See Notes See Notes	Note 40 Note 41 Note 42
PAUT-1 all users and roles (including service accounts)? Does the device enforce authentication of unique IDs and passwords for all users and roles (including service accounts)? Is the device configurable to authenticate users through an external authentication service (e.g., MS Active Directory, NDS, LDAP, OAUT). PAUT-2 etc.)? Is the device configurable to lock out a user after a certain number Is the device configurable to lock out a user after a certain number No	CONN-1.1 CONN-1.1.1 CONN-1.1.2 CONN-1.1.3 CONN-1.1.4 CONN-1.2 CONN-1.2.1 CONN-1.2.1 CONN-1.2.2 CONN-1.2.3 CONN-1.2.4 CONN-2 CONN-2 CONN-5 CONN-5 CONN-6 CONN-5	in determining appropriate security controls. This section lists connectivity capabilities that may be present on the device. Does the device have hardware connectivity capabilities? Does the device support wireless connections? Does the device support Bluetooth? Does the device support other wireless network connectivity (e.g. LTE, Zigbee, proprietary)? Does the device support other wireless connections (e.g., custom RF controls, wireless detectors)? Does the device support other wireless connections (e.g., custom RF controls, wireless detectors)? Does the device have available RJ45 Ethernet ports? Does the device have available USB ports? Does the device require, use, or support removable memory devices? Does the device support other physical connectivity? Does the device support other physical connectivity? Does the manufacturer provide a list of network ports and protocols that are used or may be used on the device? Can the device communicate with other systems within the customer environment? Can the device communicate with other systems external to the customer environment (e.g., a service host)? Does the device make or receive API calls? Does the device require an internet connection for its intended use? Does the device support Transport Layer Security (TLS)? Is TLS configurable? Does the device provide operator control functionality from a separate device (e.g., telemedicine)?	Yes Yes No No No No No No See Notes See Notes See Notes See Notes No No See Notes See Notes	Note 40 Note 41 Note 42
Does the device enforce authentication of unique IDs and passwords for all users and roles (including service accounts)? Is the device configurable to authenticate users through an external authentication service (e.g., MS Active Directory, NDS, LDAP, OAuth, etc.)? Is the device configurable to lock out a user after a certain number See Notes Note 45 No Is the device configurable to lock out a user after a certain number	CONN-1.1 CONN-1.1.1 CONN-1.1.2 CONN-1.1.3 CONN-1.1.4 CONN-1.2 CONN-1.2.1 CONN-1.2.1 CONN-1.2.2 CONN-1.2.3 CONN-1.2.4 CONN-2 CONN-2 CONN-5 CONN-5 CONN-6 CONN-5	In determining appropriate security controls. This section lists connectivity capabilities that may be present on the device. Does the device have hardware connectivity capabilities? Does the device support wireless connections? Does the device support Bluetooth? Does the device support other wireless network connectivity (e.g. LTE, Zigbee, proprietary)? Does the device support other wireless connections (e.g., custom RF controls, wireless detectors)? Does the device support physical connections? Does the device support physical connections? Does the device support physical connections? Does the device available RJ45 Ethernet ports? Does the device available RJ45 Ethernet ports? Does the device require, use, or support removable memory devices? Does the device support other physical connectivity? Does the device support other physical connectivity? Does the device communicate with other systems within the customer environment? Can the device communicate with other systems external to the customer environment (e.g., a service host)? Does the device require an internet connection for its intended use? Does the device support Transport Layer Security (TLS)? Is TLS configurable? Does the device provide operator control functionality from a separate device (e.g., telemedicine)? PERSON AUTHENTICATION (PAUT) The ability to configure the device to authenticate users.	Yes Yes No No No No No No See Notes See Notes See Notes See Notes No No See Notes See Notes	Note 40 Note 41 Note 42
PAUT-1.1 passwords for all users and roles (including service accounts)? See Notes Note 45 Is the device configurable to authenticate users through an external authentication service (e.g., MS Active Directory, NDS, LDAP, OAuth, etc.)? No See Notes Note 45 See Notes Note 45 See Notes Note 45 No See Notes Note 45 See Notes Note 45	CONN-1.1 CONN-1.1.1 CONN-1.1.2 CONN-1.1.3 CONN-1.1.4 CONN-1.2 CONN-1.2 CONN-1.2 CONN-1.2.1 CONN-1.2.2 CONN-1.2.3 CONN-1.2.4 CONN-1.2.4 CONN-2 CONN-5 CONN-6 CONN-7 CONN-7 CONN-7 CONN-7.1 CONN-8	in determining appropriate security controls. This section lists connectivity capabilities that may be present on the device. Does the device have hardware connectivity capabilities? Does the device support wireless connections? Does the device support Bluetooth? Does the device support Bluetooth? Does the device support other wireless network connectivity (e.g. LTE, Zigbee, proprietary)? Does the device support other wireless connections (e.g., custom RF controls, wireless detectors)? Does the device support physical connections? Does the device have available USB ports? Does the device have available USB ports? Does the device require, use, or support removable memory devices? Does the device support other physical connectivity? Does the device support other physical connectivity? Does the device communicate with other systems within the customer environment? Can the device communicate with other systems within the customer environment (e.g., a service host)? Does the device make or receive API calls? Does the device make or receive API calls? Does the device require an internet connection for its intended use? Does the device require an internet connection for its intended use? Does the device require an internet connection for its intended use? Does the device operator control functionality from a separate device (e.g., telemedicine)? PERSON AUTHENTICATION (PAUT) The ability to configure the device to authenticate users. Does the device support and enforce unique IDs and passwords for	Yes Yes No No No Yes See Notes See Notes No No See Notes See Notes See Notes No Yes No Yes No Yes	Note 39 Note 40 Note 41 Note 42 Note 43
PAUT-1.1 passwords for all users and roles (including service accounts)? See Notes Note 45 Is the device configurable to authenticate users through an external authentication service (e.g., MS Active Directory, NDS, LDAP, OAuth, etc.)? No See Notes Note 45 See Notes Note 45 See Notes Note 45 No See Notes Note 45 See Notes Note 45	CONN-1.1 CONN-1.1.1 CONN-1.1.2 CONN-1.1.3 CONN-1.1.4 CONN-1.2 CONN-1.2.1 CONN-1.2.1 CONN-1.2.2 CONN-1.2.3 CONN-1.2.4 CONN-2 CONN-2 CONN-5 CONN-5 CONN-6 CONN-5	in determining appropriate security controls. This section lists connectivity capabilities that may be present on the device. Does the device have hardware connectivity capabilities? Does the device support wireless connections? Does the device support Bluetooth? Does the device support Bluetooth? Does the device support other wireless network connectivity (e.g. LTE, Zigbee, proprietary)? Does the device support other wireless connections (e.g., custom RF controls, wireless detectors)? Does the device support physical connections? Does the device have available USB ports? Does the device have available USB ports? Does the device require, use, or support removable memory devices? Does the device support other physical connectivity? Does the device support other physical connectivity? Does the device communicate with other systems within the customer environment? Can the device communicate with other systems within the customer environment (e.g., a service host)? Does the device make or receive API calls? Does the device make or receive API calls? Does the device require an internet connection for its intended use? Does the device require an internet connection for its intended use? Does the device require an internet connection for its intended use? Does the device operator control functionality from a separate device (e.g., telemedicine)? PERSON AUTHENTICATION (PAUT) The ability to configure the device to authenticate users. Does the device support and enforce unique IDs and passwords for	Yes Yes No No No Yes See Notes See Notes No No See Notes See Notes See Notes No Yes No Yes No Yes	Note 39 Note 40 Note 41 Note 42 Note 43
authentication service (e.g., MS Active Directory, NDS, LDAP, OAuth, PAUT-2 etc.)? No	CONN-1.1 CONN-1.1.1 CONN-1.1.2 CONN-1.1.3 CONN-1.1.4 CONN-1.2 CONN-1.2 CONN-1.2 CONN-1.2.1 CONN-1.2.2 CONN-1.2.3 CONN-1.2.4 CONN-1.2.4 CONN-2 CONN-2 CONN-3 CONN-3 CONN-4 CONN-5 CONN-6 CONN-7 CONN-7 CONN-7.1 CONN-8	In determining appropriate security controls. This section lists connectivity capabilities that may be present on the device. Does the device have hardware connectivity capabilities? Does the device support wireless connections? Does the device support Bluetooth? Does the device support other wireless network connectivity (e.g. LTE, Zigbee, proprietary)? Does the device support other wireless connections (e.g., custom RF controls, wireless detectors)? Does the device support physical connections? Does the device support physical connections? Does the device have available RJ45 Ethernet ports? Does the device support physical connectivity? Does the device require, use, or support removable memory devices? Does the device support other physical connectivity? Does the device support other physical connectivity? Does the device communicate with other systems within the customer environment? Can the device communicate with other systems external to the customer environment? Can the device communicate with other systems external to the customer environment (e.g., a service host)? Does the device require an internet connection for its intended use? Does the device support Transport Layer Security (TLS)? Is TLS configurable? Does the device provide operator control functionality from a separate device (e.g., telemedicine)? PERSON AUTHENTICATION (PAUT) The ability to configure the device to authenticate users. Does the device support and enforce unique Ibs and passwords for all users and roles (including service accounts)?	Yes Yes No No No Yes See Notes See Notes No No See Notes See Notes See Notes No Yes No Yes No Yes	Note 39 Note 40 Note 41 Note 42 Note 43
PAUT-2 etc.)? No	CONN-1.1 CONN-1.1.1 CONN-1.1.2 CONN-1.1.3 CONN-1.1.4 CONN-1.2 CONN-1.2 CONN-1.2 CONN-1.2.1 CONN-1.2.2 CONN-1.2.3 CONN-1.2.4 CONN-1.2.4 CONN-2 CONN-5 CONN-6 CONN-7 CONN-7 CONN-7 CONN-7.1 CONN-8	in determining appropriate security controls. This section lists connectivity capabilities that may be present on the device. Does the device have hardware connectivity capabilities? Does the device support wireless connections? Does the device support bluetooth? Does the device support other wireless network connectivity (e.g. LTE, Zigbee, proprietary)? Does the device support other wireless connections (e.g., custom RF controls, wireless detectors)? Does the device support physical connections? Does the device support physical connections? Does the device support physical sports? Does the device available R45 Ethernet ports? Does the device require, use, or support removable memory devices? Does the device require, use, or support removable memory devices? Does the device support other physical connectivity? Does the manufacturer provide a list of network ports and protocols that are used or may be used on the device? Can the device communicate with other systems within the customer environment? Can the device communicate with other systems external to the customer environment (e.g., a service host)? Does the device require an internet connection for its intended use? Does the device support Transport Layer Security (TLS)? Is TLS configurable? Does the device provide operator control functionality from a separate device (e.g., telemedicine)? PERSON AUTHENTICATION (PAUT) The ability to configure the device to authenticate users. Does the device support and enforce unique IDs and passwords for all users and roles (including service accounts)?	Yes Yes No No No Yes See Notes See Notes No No See Notes See Notes See Notes See Notes See Notes See Notes	Note 39 Note 40 Note 41 Note 42 Note 43 Note 43
Is the device configurable to lock out a user after a certain number	CONN-1.1 CONN-1.1.1 CONN-1.1.2 CONN-1.1.3 CONN-1.1.4 CONN-1.2 CONN-1.2 CONN-1.2.1 CONN-1.2.1 CONN-1.2.2 CONN-1.2.3 CONN-1.2.4 CONN-1.2.4 CONN-2 CONN-2 CONN-3 CONN-3 CONN-5 CONN-6 CONN-7 CONN-7 CONN-7 CONN-7.1 CONN-8	In determining appropriate security controls. This section lists connectivity capabilities that may be present on the device. Does the device have hardware connectivity capabilities? Does the device support wireless connections? Does the device support Bluetooth? Does the device support Bluetooth? Does the device support other wireless network connectivity (e.g. LTE, Zigbee, proprietary)? Does the device support other wireless connections (e.g., custom RF controls, wireless detectors)? Does the device support physical connections? Does the device support physical connections? Does the device have available RJ45 Ethernet ports? Does the device have available RJ45 Ethernet ports? Does the device require, use, or support removable memory devices? Does the device support other physical connectivity? Does the device support other physical connectivity? Does the device compunicate with other systems within the customer environment? Can the device communicate with other systems within the customer environment? Can the device communicate with other systems external to the customer environment (e.g., a service host)? Does the device make or receive API calls? Does the device support Transport Layer Security (TLS)? Is TLS configurable? Does the device support Transport Layer Security (TLS)? Is TLS configurable? Does the device provide operator control functionality from a separate device (e.g., telemedicine)? PERSON AUTHENTICATION (PAUT) The ability to configure the device to authenticate users. Does the device support and enforce unique IDs and passwords for all users and roles (including service accounts)? Is the device configurable to authenticate users through an external	Yes Yes No No No Yes See Notes See Notes No No See Notes See Notes See Notes See Notes See Notes See Notes	Note 39 Note 40 Note 41 Note 42 Note 43 Note 43
	CONN-1.1 CONN-1.1.1 CONN-1.1.2 CONN-1.1.3 CONN-1.1.4 CONN-1.2 CONN-1.2 CONN-1.2.1 CONN-1.2.1 CONN-1.2.2 CONN-1.2.3 CONN-1.2.4 CONN-1.2.4 CONN-2 CONN-2 CONN-3 CONN-3 CONN-5 CONN-6 CONN-7 CONN-7 CONN-7 CONN-7.1 CONN-8	in determining appropriate security controls. This section lists connectivity capabilities that may be present on the device. Does the device have hardware connectivity capabilities? Does the device support wireless connections? Does the device support devices connections? Does the device support Bluetooth? Does the device support other wireless network connectivity (e.g. LTE, Zigbee, proprietary)? Does the device support other wireless connections (e.g., custom RF controls, wireless detectors)? Does the device support physical connections? Does the device have available USB ports? Does the device have available USB ports? Does the device require, use, or support removable memory devices? Does the device support other physical connectivity? Does the device support other physical connectivity? Does the device support other physical connectivity? Can the device communicate with other systems within the customer environment? Can the device communicate with other systems external to the customer environment (e.g., a service host)? Does the device make or receive API calls? Does the device make or receive API calls? Does the device require an internet connection for its intended use? Does the device provide operator control functionality from a separate device (e.g., telemedicine)? PERSON AUTHENTICATION (PAUT) The ability to configure the device to authenticate users. Does the device support and enforce unique IDs and passwords for all users and roles (including service accounts)? Does the device enforce authentication of unique IDs and passwords for all users and roles (including service accounts)?	Yes Yes No No No No No No No Yes See Notes	Note 39 Note 40 Note 41 Note 42 Note 43 Note 43
In an accession of the contract of the c	CONN-1.1 CONN-1.1.1 CONN-1.1.2 CONN-1.1.3 CONN-1.1.4 CONN-1.2 CONN-1.2 CONN-1.2.1 CONN-1.2.1 CONN-1.2.2 CONN-1.2.3 CONN-1.2.4 CONN-1.2.4 CONN-2 CONN-2 CONN-3 CONN-3 CONN-5 CONN-6 CONN-7 CONN-7 CONN-7 CONN-7.1 CONN-8	in determining appropriate security controls. This section lists connectivity capabilities that may be present on the device. Does the device have hardware connectivity capabilities? Does the device support wireless connections? Does the device support bluetooth? Does the device support bluetooth? Does the device support other wireless network connectivity (e.g. LTE, Zigbee, proprietary)? Does the device support other wireless connections (e.g., custom RF controls, wireless detectors)? Does the device support physical connections? Does the device support physical connections? Does the device have available R45 Ethernet ports? Does the device available R45 Ethernet ports? Does the device require, use, or support removable memory devices? Does the device require, use, or support removable memory devices? Does the device support other physical connectivity? Does the manufacturer provide a list of network ports and protocols that are used or may be used on the device? Can the device communicate with other systems within the customer environment? Can the device communicate with other systems external to the customer environment (e.g., a service host)? Does the device make or receive API calis? Does the device support Transport Layer Security (TLS)? Is TLS configurable? Does the device popurate an internet connection for its intended use? PERSON AUTHENTICATION (PAUT) The ability to configure the device to authenticate users. Does the device support and enforce unique IDs and passwords for all users and roles (including service accounts)? Is the device configurable to authenticate users through an external authentication or unique iDs and passwords for all users and roles (including service accounts)?	Yes Yes No No No No No No No Yes See Notes	Note 39 Note 40 Note 41 Note 42 Note 43 Note 43

PAUT-4 PAUT-5 PAUT-6 PAUT-7 PAUT-8 PAUT-9 PAUT-10 PAUT-11 PAUT-12 PAUT-12	Are all default accounts (e.g., technician service accounts, administrator accounts) listed in the documentation? Can all passwords be changed? Is the device configurable to enforce creation of user account passwords that meet established (organization specific) complexity	No Yes	_
PAUT-5 PAUT-6 PAUT-7 PAUT-8 PAUT-9 PAUT-10 PAUT-11 PAUT-12	administrator accounts) listed in the documentation? Can all passwords be changed? Is the device configurable to enforce creation of user account		
PAUT-5 PAUT-6 PAUT-7 PAUT-8 PAUT-9 PAUT-10 PAUT-11 PAUT-12	Can all passwords be changed? Is the device configurable to enforce creation of user account		_
PAUT-6 PAUT-7 PAUT-8 PAUT-9 PAUT-10 PAUT-11 PAUT-12	Is the device configurable to enforce creation of user account		
PAUT-7 PAUT-8 PAUT-9 PAUT-10 PAUT-11 PAUT-12	nasswords that meet established (organization specific) complexity		_
PAUT-7 PAUT-8 PAUT-9 PAUT-10 PAUT-11 PAUT-12		Con Notes	Notes 40
PAUT-8 PAUT-9 PAUT-10 PAUT-11 PAUT-12	rules? Does the device support account passwords that expire	See Notes	Note 46
PAUT-9 PAUT-10 PAUT-11 PAUT-12	periodically?	No	
PAUT-10 PAUT-11 PAUT-12	Does the device support multi-factor authentication?	No	
PAUT-11 PAUT-12	Does the device support single sign-on (SSO)?	No No	_
PAUT-12	Can user accounts be disabled/locked on the device? Does the device support biometric controls?	No No	
	boes the device support biometric controls:	10	
DALIT 42	Does the device support physical tokens (e.g. badge access)?	See Notes	Note 47
	Does the device support group authentication (e.g. hospital teams)?	No.	
FA01-13	Does the application or device store or manage authentication	NO	
PAUT-14	credentials?	Yes	
PAUT-14.1	Are credentials stored using a secure method?	Yes	
	PHYSICAL LOCKS (PLOK)		
	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		
	Is the device software only? If yes, answer "N/A" to remaining		
PLOK-1	questions in this section.	No	
	Are all device components maintaining personally identifiable		
PLOK-2	information (other than removable media) physically secure (i.e., cannot remove without tools)?	See Notes	Note 48
. LON Z			
	Are all device components maintaining personally identifiable		
DLOK 3	information (other than removable media) physically secured	Con Natos	Note 40
PLOK-3	behind an individually keyed locking device?	See Notes	Note 49
	Does the device have an option for the customer to attach a		
PLOK-4	physical lock to restrict access to removable media?	No	
	ROADMAP FOR THIRD PARTY COMPONENTS IN DEVICE LIFE		
	CYCLE (RDMP)		
	Manufacturer's plans for security support of third-party components		
	within the device's life cycle.		
	Was a secure software development process, such as ISO/IEC 27034		
RDMP-1	or IEC 62304, followed during product development?	See Notes	Note 50
	Does the manufacturer evaluate third-party applications and		
	software components included in the device for secure		
RDMP-2	development practices?	Yes	_
	Does the manufacturer maintain a web page or other source of		
RDMP-3	information on software support dates and updates?	Yes	_
	Does the manufacturer have a plan for managing third-party		
RDMP-4	component end-of-life?	Yes	_
	SOFTWARE BILL OF MATERIALS (SBoM)		
	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 supports controls in the RDMP section.		
SBOM-1	Is the SBoM for this product available?	Yes	_
	Does the SBoM follow a standard or common method in describing		
SBOM-2 SBOM-2.1	software components? Are the software components identified?	Yes Yes	_
	Are the developers/manufacturers of the software components		
SBOM-2.2	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 No	
CDOM 2	Does the device include a command or process method available to	No.	
SBOM-3 SBOM-4	generate a list of software components installed on the device? Is there an update process for the SBoM?	No Yes	_
	SYSTEM AND APPLICATION HARDENING (SAHD)		
	The device in the court of the		
	The device's inherent resistance to cyber attacks and malware.		
SAHD-1	Is the device hardened in accordance with any industry standards?	No	_
SAHD 2	Has the device received any a thorse suits a satisfactor	No	
SAHD-2	Has the device received any cybersecurity certifications? Does the device employ any mechanisms for software integrity	No	_
SAHD-3	checking	No	_
	Does the device employ any mechanism (e.g., release-specific hash key, checksums, digital signature, etc.) to ensure the installed		
SAHD-3.1	software is manufacturer-authorized?	See Notes	Note 51
	Does the device employ any mechanism (e.g., release-specific hash		
	key, checksums, digital signature, etc.) to ensure the software		
SAHD-3.2	updates are the manufacturer-authorized updates?	Yes	

BIOFIRE Diagnostics, LLC	BIOFIRE® SPOTFIRE® SYSTEM	BFR0001-8102-03	June 17th 2024
	Can the owner/operator perform software integrity checks (i.e.,		
SAHD-4	verify that the system has not been modified or tampered with)?	No .	_
	Is the system configurable to allow the implementation of file-level,		
SAHD-5 SAHD-5.1	patient level, or other types of access controls? Does the device provide role-based access controls?	No Yes	_
SAHU-5.1	Are any system or user accounts restricted or disabled by the	Tes	_
SAHD-6	manufacturer at system delivery?	See Notes	Note 52
SAHD-6.1	Are any system or user accounts configurable by the end user after initial configuration?	No	
<u> </u>			_
SAHD-6.2	Does this include restricting certain system or user accounts, such as service technicians, to least privileged access?	No	
3AHD-0.2	Are all shared resources (e.g., file shares) which are not required for	NO	_
SAHD-7	the intended use of the device disabled?	N/A	_
SAHD-8	Are all communication ports and protocols that are not required for the intended use of the device disabled?	See Notes	Note 53
57415 0	the intended use of the device disabled.	Sec Notes	Note 55
	Are all services (e.g., telnet, file transfer protocol [FTP], internet information server [IIS], etc.), which are not required for the		
SAHD-9	intended use of the device deleted/disabled?	Yes	
	Are all applications (COTS applications as well as OS-included applications, e.g., MS Internet Explorer, etc.) which are not required		
SAHD-10	for the intended use of the device deleted/disabled?	See Notes	Note 54
	Can the device prohibit hand for a second of the second of		
SAHD-11	Can the device prohibit boot from uncontrolled or removable media (i.e., a source other than an internal drive or memory component)?	No	
	Can unauthorized software or hardware be installed on the device		
SAHD-12	without the use of physical tools? Does the product documentation include information on	Yes	_
SAHD-13	operational network security scanning by users?	No	_
SAUD 14	Can the device he hardened beyond the default and ded at 2	See Notes	Note EE
SAHD-14	Can the device be hardened beyond the default provided state?	See Notes	Note 55
SAHD-14.1	Are instructions available from vendor for increased hardening?	See Notes	Note 56
SHAD-15	Can the system prevent access to BIOS or other bootloaders during boot?	No	
SHAD-13	Have additional hardening methods not included in 2.3.19 been	110	
SAHD-16	used to harden the device?	See Notes	Note 57
	SECURITY GUIDANCE (SGUD)		
	Availability of security guidance for operator and administrator of the device and manufacturer sales and service.		
	Does the device include security documentation for the		
SGUD-1	owner/operator?	Yes	_
	Does the device have the capability, and provide instructions, for		
SGUD-2	the permanent deletion of data from the device or media?	See Notes	Note 58
SGUD-3	Are all access accounts documented?	See Notes	Note 59
SGUD-3.1	Can the owner/operator manage password control for all accounts? Does the product include documentation on recommended	See Notes	Note 60
SGUD-4	compensating controls for the device?	No	_
	HEALTH DATA STORAGE CONFIDENTIALITY (STCF)		
	The ability of the device to ensure unauthorized access does not		
	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 STCF-1.1	Can the device encrypt data at rest? Is all data encrypted or otherwise protected?	No See Notes	Note 61
STCF-1.1	Is the data encryption capability configured by default?	N/A	
STCE 1 2	Are instructions available to the sustament	N/A	
STCF-1.3 STCF-2	Are instructions available to the customer to configure encryption? Can the encryption keys be changed or configured?	N/A N/A	_
STCF-3	Is the data stored in a database located on the device?	Yes	_
STCF-4	Is the data stored in a database external to the device?	See Notes	Note 62
_	TRANSMISSION CONFIDENTIALITY (TXCF)		
	The ability of the device to ensure the confidentiality of transmitted personally identifiable information.		
	Can personally identifiable information be transmitted only via a		
TXCF-1	point-to-point dedicated cable?	No	_
TXCF-2	Is personally identifiable information encrypted prior to transmission via a network or removable media?	See Notes	Note 63
	If data is not encrypted by default, can the customer configure		
TXCF-2.1	encryption options? Is personally identifiable information transmission restricted to a	No .	_
TXCF-3	fixed list of network destinations?	No	_
TXCF-4	Are connections limited to authenticated systems? Are secure transmission methods supported/implemented (DICOM,	See Notes	Note 64
TXCF-5	HL7, IEEE 11073)?	See Notes	Note 65
	TRANSMISSION INTEGRITY (TXIG)		
	The ability of the device to ensure the integrity of transmitted data.		

	I		1
BIOFIRE Diagnostics, LLC	BIOFIRE® SPOTFIRE® SYSTEM	BFR0001-8102-03	June 17th 2024
TXIG-1	Does the device support any mechanism (e.g., digital signatures) intended to ensure data is not modified during transmission?	See Notes	Note 66
TXIG-2	Does the device include multiple sub-components connected by external cables?	No .	note of
	REMOTE SERVICE (RMOT) 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?	See Notes	Note 67
RMOT-1.1	Does the device allow the owner/operator to initiative remote service sessions for device analysis or repair?	No	
RMOT-1.2	Is there an indicator for an enabled and active remote session? Can patient data be accessed or viewed from the device during the	See Notes	Note 68
RMOT-1.3	remote session?	See Notes	Note 69
RMOT-2	Does the device permit or use remote service connections for predictive maintenance data?	See Notes	Note 70
NWO1-2	Does the device have any other remotely accessible functionality	Jee Notes	Note 70
RMOT-3	(e.g. software updates, remote training)?	See Notes	Note 71
	OTHER SECURITY CONSIDERATIONS (OTHR)		
	NONE		
	Notes:		
	The following data fields are associated with each test on the System: Run Start Time and Run End Time, Serial Number (of consumable), Lot Number (of consumable), Operator, Module Serial Number, Sample Type, Pouch Type, and a Sample ID.		
Note 1	The "Sample ID" field is a free text field, and bioMérieux issues guidance to use sequentially generated recycled accession numbers in the "Sample ID" field. Consistent with this guidance, do not enter patient names, addresses, demographic information, financial information, medical record numbers, Social Security numbers, and any other unique identifying number, characteristic, or code in the Sample ID field.		
	To the extent the information contained in any these fields is personally identifiable information, as defined in ANSI/NEMA HN 1-2019, such information is displayed and stored on the System. As an optional feature, the System may be configured to transmit such information.		
Note 2	The following data fields are associated with each test on the System: Run Start Time and Run End Time, Serial Number (of consumable), Lot Number (of consumable), Operator, Module Serial Number, Sample Type, Pouch Type, and a Sample ID. The "Sample ID" field is a free text field, and bioMérieux issues guidance to use sequentially generated recycled accession numbers in the "Sample ID" field. Consistent with this guidance, do not enter patient names, addresses, demographic information, financial information, medical record numbers, Social Security numbers, and any other unique identifying number, characteristic, or code in the Sample ID field. To the extent the information contained in any these fields is personally identifiable information, as defined in ANSI/NEMA HN 1-2019, such information is maintained on the System.		

BIOFIRE Diagnostics, LLC	BIOFIRE® SPOTFIRE® SYSTEM	BFR0001-8102-03	June 17th 2024
Note 3	The following data fields are associated with each test on the System: Run Start Time and Run End Time, Serial Number (of consumable), Lot Number (of consumable), Derator, Module Serial Number, Sample Type, Pouch Type, and a Sample ID. The "Sample ID" field is a free text field, and bioMérieux issues guidance to use sequentially generated recycled accession numbers in the "Sample ID" field. Consistent with this guidance, do not enter patient names, addresses, demographic information, financial information, medical record numbers, Social Security numbers, and any other unique identifying number, characteristic, or code in the Sample ID field. To the extent the information contained in any these fields is personally identifiable information, as defined in ANSI/NEMA HN 1-2019, such information is maintained on the System. The system does have the ability to clear personally identifiable information through a Factory Reset Feature.		
Note 4	The following data fields are associated with each test on the System: Run Start Time and Run End Time, Serial Number (of consumable), Lot Number (of consumable), Derator, Module Serial Number, Sample Type, Pouch Type, and a Sample ID. The "Sample ID" field is a free text field, and bioMérieux issues guidance to use sequentially generated recycled accession numbers in the "Sample ID" field. Consistent with this guidance, do not enter patient names, addresses, demographic information, financial information, medical record numbers, Social Security numbers, and any other unique identifying number, characteristic, or code in the Sample ID field. To the extent the information contained in any these fields is personally identifiable information, as defined in ANSI/NEMA HN 1-2019, such information is stored on internal media within the System.		
Note 5	The following data fields are associated with each test on the System: Run Start Time and Run End Time, Serial Number (of consumable), Lot Number (of consumable). Operator, Module Serial Number, Sample Type, Pouch Type, and a Sample ID. The "Sample ID" field is a free text field, and bioMérieux issues guidance to use sequentially generated recycled accession numbers in the "Sample ID" field. Consistent with this guidance, do not enter patient names, addresses, demographic information, financial information, medical record numbers, Social Security numbers, and any other unique identifying number, characteristic, or code in the Sample ID field. To the extent the information contained in any these fields is personally identifiable information, as defined in ANSI/NEMA HN 1-2019, such information is preserved in the System's nonvolatile memory until explicitly erased.		
Note 6	The following data fields are associated with each test on the System: Run Start Time and Run End Time, Serial Number (of consumable), Lot Number (of consumable), Operator, Module Serial Number, Sample Type, Pouch Type, and a Sample ID. The "Sample ID" field is a free text field, and bioMérieux issues guidance to use sequentially generated recycled accession numbers in the "Sample ID" field. Consistent with this guidance, do not enter patient names, addresses, demographic information, financial information, medical record numbers, Social Security numbers, and any other unique identifying number, characteristic, or code in the Sample ID field. To the extent the information contained in any these fields is personally identifiable information, as defined in ANSI/NEMA HN 1-2019, such information is stored in a database within the System.		

BIOFIRE Diagnostics, LLC	BIOFIRE® SPOTFIRE® SYSTEM	BFR0001-8102-03	June 17th 2024
Note 7	The following data fields are associated with each test on the System: Run Start Time and Run End Time, Serial Number (of consumable), Lot Number (of consumable), Operator, Module Serial Number, Sample Type, Pouch Type, and a Sample ID. The "Sample ID" field is a free text field, and bioMérieux issues guidance to use sequentially generated recycled accession numbers in the "Sample ID" field. Consistent with this guidance, do not enter patient names, addresses, demographic information, financial information, medical record numbers, Social Security numbers, and any other unique identifying number, characteristic, or code in the Sample ID field. To the extent the information contained in any these fields is personally identifiable information, as defined in ANSI/NEMA HN 1-2019, such information may be deleted by the software. As an optional feature, the System may be configured to transmit such information.		
Note 8	The following data fields are associated with each test on the System: Run Start Time and Run End Time, Serial Number (of consumable), Lot Number (of consumable), Operator, Module Serial Number, Sample Type, Pouch Type, and a Sample ID. The "Sample ID" field is a free text field, and bioMerieux issues guidance to use sequentially generated recycled accession numbers in the "Sample ID" field. Consistent with this guidance, do not enter patient names, addresses, demographic information, financial information, medical record numbers, Social Security numbers, and any other unique identifying number, characteristic, or code in the Sample ID field. To the extent the information contained in any these fields is personally identifiable information, as defined in ANSI/NEMA HN 1-2019, such information may be imported/exported with other systems via configuration of optional connectivity features.		
Note 9	The following data fields are associated with each test on the System: Run Start Time and Run End Time, Serial Number (of consumable), Lot Number (of consumable), Operator, Module Serial Number, Sample Type, Pouch Type, and a Sample ID. The "Sample ID" field is a free text field, and bioMérieux issues guidance to use sequentially generated recycled accession numbers in the "Sample ID" field. Consistent with this guidance, do not enter patient names, addresses, demographic information, financial information, medical record numbers, Social Security numbers, and any other unique identifying number, characteristic, or code in the Sample ID field. To the extent the information contained in any these fields is personally identifiable information, as defined in ANSI/NEMA HN 1-2019, such information may be maintained when powered off, or during power service interruptions.		
Note 10	The following data fields are associated with each test on the System: Run Start Time and Run End Time, Serial Number (of consumable), Lot Number (of consumable), Operator, Module Serial Number, Sample Type, Pouch Type, and a Sample ID. The "Sample ID" field is a free text field, and bioMérieux issues guidance to use sequentially generated recycled accession numbers in the "Sample ID" field. Consistent with this guidance, do not enter patient names, addresses, demographic information, financial information, medical record numbers, Social Security numbers, and any other unique identifying number, characteristic, or code in the Sample ID field. To the extent the information contained in any these fields is personally identifiable information, as defined in ANSI/NEMA HN 1-2019, such information may be stored in a separate location from the System's operating system.		

BIOFIRE Diagnostics, LLC	BIOFIRE® SPOTFIRE® SYSTEM	BFR0001-8102-03	June 17th 2024
Note 11	The following data fields are associated with each test on the System: Run Start Time and Run End Time, Serial Number (of consumable), Lot Number (of consumable), Operator, Module Serial Number, Sample Type, Pouch Type, and a Sample ID. The "Sample ID" field is a free text field, and bioMérieux issues guidance to use sequentially generated recycled accession numbers in the "Sample ID" field. Consistent with this guidance, do not enter patient names, addresses, demographic information, financial information, medical record numbers, Social Security numbers, and any other unique identifying number, characteristic, or code in the Sample ID field. To the extent the information contained in any these fields is personally identifiable information, as defined in ANSI/NEMA HN 1-2019, the System does have mechanisms used for transmitting and importing/exporting such information.		
Note 12	The following data fields are associated with each test on the System: Run Start Time and Run End Time, Serial Number (of consumable), Lot Number (of consumable), Operator, Module Serial Number, Sample Type, Pouch Type, and a Sample ID. The "Sample ID" field is a free text field, and bioMérieux issues guidance to use sequentially generated recycled accession numbers in the "Sample ID" field. Consistent with this guidance, do not enter patient names, addresses, demographic information, financial information, medical record numbers, Social Security numbers, and any other unique identifying number, characteristic, or code in the Sample ID field. To the extent the information contained in any these fields is personally identifiable information, as defined in ANSI/NEMA HN 1-		
Note 13	2019, such information is displayed by the System. The following data fields are associated with each test on the System: Run Start Time and Run End Time, Serial Number (of consumable), Lot Number (of consumable), Operator, Module Serial Number, Sample Type, Pouch Type, and a Sample ID. The "Sample ID" field is a free text field, and bioMérieux issues guidance to use sequentially generated recycled accession numbers in the "Sample ID" field. Consistent with this guidance, do not enter patient names, addresses, demographic information, financial information, medical record numbers, Social Security numbers, and any other unique identifying number, characteristic, or code in the Sample ID field. To the extent the information contained in any these fields is personally identifiable information, as defined in ANSI/NEMA HN 1-2019, such information may be contained on generated hard copy reports or images.		
Note 14	The following data fields are associated with each test on the System: Run Start Time and Run End Time, Serial Number (of consumable), Lot Number (of consumable), Operator, Module Serial Number, Sample Type, Pouch Type, and a Sample ID. The "Sample ID" field is a free text field, and bioMérieux issues guidance to use sequentially generated recycled accession numbers in the "Sample ID" field. Consistent with this guidance, do not enter patient names, addresses, demographic information, financial information, medical record numbers, Social Security numbers, and any other unique identifying number, characteristic, or code in the Sample ID field. To the extent the information contained in any these fields is personally identifiable information, as defined in ANSI/NEMA HN 1-2019, such information may be retrieved from or recorded to removable media.		

BIOFIRE Diagnostics, LLC	BIOFIRE® SPOTFIRE® SYSTEM	BFR0001-8102-03	June 17th 2024
Note 15	The following data fields are associated with each test on the System: Run Start Time and Run End Time, Serial Number (of consumable), Lot Number (of consumable), Operator, Module Serial Number, Sample Type, Pouch Type, and a Sample ID. The "Sample ID" field is a free text field, and bioMérieux issues guidance to use sequentially generated recycled accession numbers in the "Sample ID" field. Consistent with this guidance, do not enter patient names, addresses, demographic information, financial information, medical record numbers, Social Security numbers, and any other unique identifying number, characteristic, or code in the Sample ID field. To the extent the information contained in any these fields is personally identifiable information, as defined in ANSI/NEMA HN 1-2019, such information may be transmitted/received or imported/exported via dedicated cable connection.		
Note 16	The following data fields are associated with each test on the System: Run Start Time and Run End Time, Serial Number (of consumable), Lot Number (of consumable), Operator, Module Serial Number, Sample Type, Pouch Type, and a Sample ID. The "Sample ID" field is a free text field, and bioMérieux issues guidance to use sequentially generated recycled accession numbers in the "Sample ID" field. Consistent with this guidance, do not enter patient names, addresses, demographic information, financial information, medical record numbers, Social Security numbers, and any other unique identifying number, characteristic, or code in the Sample ID field. Sample ID field. To the extent the information contained in any these fields is personally identifiable information, as defined in ANSI/NEMA HN 1-2019, such information may be transmitted/received via a wired network connection.		
Note 17	The following data fields are associated with each test on the System: Run Start Time and Run End Time, Serial Number (of consumable), Lot Number (of consumable), Operator, Module Serial Number, Sample Type, Pouch Type, and a Sample ID. The "Sample ID" field is a free text field, and bioMérieux issues guidance to use sequentially generated recycled accession numbers in the "Sample ID" field. Consistent with this guidance, do not enter patient names, addresses, demographic information, financial information, medical record numbers, Social Security numbers, and any other unique identifying number, characteristic, or code in the Sample ID field. To the extent the information contained in any these fields is personally identifiable information, as defined in ANSI/NEMA HN 1-2019, such information may be transmitted/received over an external network if the System is configured with an optional connectivity feature.		
Note 18	When optional remote access features are installed remote access audit logs are available through the feature's administrator account. These logs are not stored on the System.		
Note 19	SpotFire Control Stations date and time synchronization with NTP is configurable by the customer.		
Note 20	The System is pre-configured to log on to Windows using the SPOTFIRE user account automatically. The SPOTFIRE user account is a Windows Standard User with its equivalent access rights. The System computer is also pre-configured with an administrative user account (LabAdmin). It is recommended the System owner/operator change the default password for the LabAdmin user account as the account has local administrative privileges. SPOTFIRE has a set operator list which only allows the SPOTFIRE application software to be accessed.		

BIOFIRE Diagnostics, LLC	BIOFIRE® SPOTFIRE® SYSTEM	BFR0001-8102-03	June 17th 2024
Note 21	When optional connectivity features are enabled (specifically, the POCT01-A2 interface), application user credentials may be maintained by a centralized data-management system and distributed over a network to one or multiple connected devices according to the customer's organizational requirements. In this configuration, application user credentials on the device cannot be modified or shared with other devices.		
Note 22	The system allows operators to be created with or without administrator privileges.		
Note 23	The System is operated using a Windows Operating System User Account that does not have administrative privileges. Configuration changes require administrative privileges using an administrative Windows user account pre-configured on the computer. The System application software does not allow operators to modify their own administrator privileges.		
Note 24	Instructions for the owner/operator installation of Operating System patches are within BFR0001-6037 Microsoft OS Patch Policy Tech Note.		
Note 25	Instructions for the owner/operator installation of Operating System patches are within BFR0001-6037 Microsoft OS Patch Policy Tech Note.		
Note 26	Documentation for Driver and Firmware patches or updates, if required, will be distributed by bioMérieux's BIOFIRE Technical Support team.		
Note 27	The recommended installation process for updates from third party manufactures (e.g. Microsoft) is available within BFR0001-6037 Microsoft OS Patch Policy Tech Note.		
Note 28	Instructions for the owner/operator installation of AntiMalware Software patches are within BFR0001-6037 Microsoft OS Patch Policy Tech Note.		
Note 29	The recommended installation process for updates from third party manufactures (e.g. Microsoft) is available within BFR0001-6037 Microsoft OS Patch Policy Tech Note.		
Note 30	If the optional interface with an Institution-specific cloud-based data management portal or remote support features are configured, the device does have the capability to perform a limited scope of automatic updates. The potential updates do not impact the intended use of the device nor alter intended use workflows.		
Note 31	The following data fields are associated with each test on the System: Run Start Time and Run End Time, Serial Number (of consumable), Lot Number (of consumable), Cot Number (of consumable), Cot Number (of consumable). Operator, Module Serial Number, Sample Type, Pouch Type, and a Sample ID. The "Sample ID" field is a free text field, and bioMérieux issues guidance to use sequentially generated recycled accession numbers in the "Sample ID" field. Consistent with this guidance, do not enter patient names, addresses, demographic information, financial information, medical record numbers, Social Security numbers, and any other unique identifying number, characteristic, or code in the Sample ID field. To the extent the information contained in any these fields is personally identifiable information, as defined in ANSI/NEMA HN 1-2019, the System has the capability to remove such information upon export.		
Note 32	The System is not intended to maintain long term primary storage of data. See the System Operator's Manual for data archiving guidance.		
Note 33	If a System is believed to be impacted by malware, please contact the BIOFIRE Technical Support team for assistance.		
Note 34	Operating system and security event auditing utilizes Windows logging features.		
Note 35	Installation and maintenance of antivirus, intrusion detection, and other detection/prevention systems is the responsibility of the end user. If the System is configured with optional connectivity features, node		
Note 36	authentication may be utilized. Certificate-based network connection authentication may be		
Note 37	utilized through the Windows Operating System. Reference the System Operator's Manual for the System's hardware		
Note 38	connectivity capabilities. Reference the System Operator's Manual for details on the System's		
Note 39	available USB ports. Reference the System Operator's Manual for details on the System's		
Note 40	capability to use or support removable memory devices.		

If optional connectivity features are enabled, the System may communicate with other systems within the customer environment but does not communicate with other SPOTFIRE Systems. If optional connectivity features are enabled, the System may communicate with other systems external to the customer environment. The System makes internal API calls only. The System does not expose or call any APIs to/from external systems. Device operation requires all users to authenticate with a unique user ID/password combination or barcode number maintained through the application software. Windows user accounts may be separately used to access to the operating system, as follows: - Windows administrator-level accounts require authentication with a unique of unique of the application software. Windows user accounts may be separately used to access to the operating system, as follows: - Windows administrator-level accounts require authentication with a unique user ID/password combination	
communicate with other systems within the customer environment but does not communicate with other SPOTFIRE Systems. If optional connectivity features are enabled, the System may communicate with other systems external to the customer environment. The System makes internal API calls only. The System does not expose or call any APIs to/from external systems. Device operation requires all users to authenticate with a unique user ID/password combination or barcode number maintained through the application software. Windows user accounts may be separately used to access to the operating system, as follows: - Windows administrator-level accounts require authentication with	
Note 42 communicate with other systems external to the customer environment. The System makes internal API calls only. The System does not expose or call any APIs to/from external systems. Device operation requires all users to authenticate with a unique user ID/password combination or barcode number maintained through the application software. Windows user accounts may be separately used to access to the operating system, as follows: - Windows administrator-level accounts require authentication with	
Note 43 expose or call any APIs to/from external systems. Device operation requires all users to authenticate with a unique user ID/password combination or barcode number maintained through the application software. Windows user accounts may be separately used to access to the operating system, as follows: - Windows administrator-level accounts require authentication with	
user ID/password combination or barcode number maintained through the application software. Windows user accounts may be separately used to access to the operating system, as follows: - Windows administrator-level accounts require authentication with	
- Windows user-level account requires a unique user ID only (no password)	
Device operation requires all users to authenticate with a unique user ID/password combination or barcode number maintained through the application software. Windows user accounts may be separately used to access to the operating system, as follows: - Windows administrator-level accounts require authentication with a unique user ID/password combination - Windows user-level account requires a unique user ID only (no password)	
The system application software (SPOTFIRE) enforces user account passwords that meet established complexity rules. Note 46 The Windows administrator-level accounts do not enforce user account passwords that meet established complexity rules.	
The system application software (SPOTFIRE) allows an admin operator to optionally enable barcode badge access which can be used by all operators. When enabled, all operators can associate a unique barcode that can be used for their authentication.	
To the extent that the System maintains personally identifiable information, such information is physically secure. (See Note 2 for additional information on the System's ability to maintain patient identifiable information)	
To the extent that the System maintains personally identifiable information, such information is physically secure, but is not behind an individually keyed locking device. (See Note 2 for additional information on the System's ability to maintain patient identifiable information)	
Note 50 The software was developed in accordance with IEC 62304.	
Quality Assurance processes conducted during the System's Note 51 assembly ensure the installed software is manufacturer authorized.	
The Microsoft Windows Operating System "BMX_Guest" account is disabled by default.	
If optional connectivity features are enabled, the System restricts inbound connections from external systems to specific TCP ports corresponding to the configured network protocol (e.g. port 21 for File Transfer Protocol). Outbound connections initiated by the System are allowed on any available TCP port (1-65535). No outbound port exclusions are currently configured.	
The system uses a modified Windows 10 IoT Enterprise 2019 LTSC Version 1809 image which includes deleting and/or disabling many Note 54 Reatures that are not required for the intended use of the device.	
If you have any questions or concerns about system hardening Note 55 beyond the default state, please contact the BIOFIRE Technical Support team for assistance.	
If you have any questions or concerns about system hardening Note 56 beyond the default state, please contact the BIOFIRE Technical Support team for assistance.	
Department of Defense's Security Technical Implementation Guides Note 57 Note 57 System. Department of Defense's Security Technical Implementation Guides have been used to harden the Microsoft Windows Operating System.	
The SPOTFIRE application software has a Factory Reset feature that will remove all data from the system.	

	DISTRICT CONTRACT CHARTS	0.500.001 0.400 0.0	
BIOFIRE Diagnostics, LLC	BIOFIRE® SPOTFIRE® SYSTEM	BFR0001-8102-03	June 17th 2024
	Windows operating system accounts are not documented.		
Note 59	SPOTFIRE application software role-based access accounts are		
	documented in the Operators Manual.		
	The SPOTFIRE application software allows admin operators to		
	manage password control. The SPOTFIRE application software		
Note 60	cannot make changes directly to the Windows OS accounts. If the		
	'Switch to Windows OS' is used the owner then has access to		
Note 60	manage password control for the Windows accounts.		
	Data protection mechanisms in place on the system include		
	password protection of the local databases, anonymization of the		
Note 61	run data when exporting anonymously, the use of API keys		
Note of	protecting our services, and data bundle creation.		
	If the System's optional connectivity features are enabled, data may		
	be stored in an external database.		
Note 62			
	Data is encrypted prior to transmission via removable media. If the		
	System's optional connectivity features are enabled, data is not encrypted prior to transmission through the optional connectivity		
Note 63	features, the removable media encryption remains the same.		
	reactives, are removable media eneryption remains are same.		
<u> </u>	If optional connectivity features are enabled, the server limits		
Note 64	connections to authenticated SpotFire systems.		
Note 04			
	If the System's optional connectivity features are enabled, secure		
	transmission methods may be supported/implemented depending		
Note 65	on the configured networking protocol.		
	If the System's optional connectivity features are enabled, the		
Note 66	System supports mechanisms intended to ensure data is not		
	modified during transmission.		
1	The System's intended use does not require nor permit remote		
	service connections. If the System's optional connectivity features		
Note 67	are enabled, the System may permit remote service connections for analysis or repair.		
	- Cpun		
	If the System's optional connectivity features are enabled and a		
Note 68	remote session is active, there is an indicator.		
Note bo			
	If the System's optional connectivity features are enabled and to the		
Note 69	extent patient data may be on the System, it may be accessed or		
	viewed during the remote session.		
1			
	If the System's optional connectivity features are enabled, the		
Note 70	System's remote service connections may be used for predictive		
	maintenance data.		
Note 71	If the System's optional connectivity features are enabled, other		
	remotely accessible functionality may be included. Documentation		
Note /1	for Remote Service features can be provided upon request.		
		·	