Manufacturer Disclosure Statement for BIOFIRE PILIMARRAY* 2.0 SY  Question ID Question DOC-1  Doc-1  Doc-2  Device Description DOC-3  Doc-3  Doc-4  Document ID  DOC-5  Manufacturer Contact Inform		FLM2-PRT-0268-07  BioFire Diagnostics, LLC  The BioFiRe* FILMARRAY* 2.0 SYSTEM is an automated in vitro diagnostic (IVD) device intended for use with FDA cleared or approved IVD BioFiRe* FILMARRAY* anels. The BioFiRe FILMARRAY 2.0 System is intended for use in combination with assay specific reagent pouches to detect multiple nucleic acid targets contained in clinical specimens. The BioFiRe FILMARRAY 2.0 Instrument interacts with the reagent pouch to both purify nucleic acids and amplify targeted nucleic acid sequences using nested multiplex PCR in a closed system. The resulting PCR products are evaluated using DNA melting analysis. The BioFiRe FILMARRAY 2.0 software automatically determines the results and provides a test report.  The BIOFIRE FILMARRAY 2.0 System is composed of one to eight instruments connected to a computer running BIOFIRE FILMARRAY 2.0 Software. The software controls the function of each instrument and collects, analyzes, and stores data generated by each instrument.	11-Jul-2023 See note
Question ID Question DOC-1 Manufacturer Name  DOC-2 Device Description DOC-3 Device Model DOC-4 Document ID		The BIOFIRE* FILMARRAY* 2.0 SYSTEM is an automated in vitro diagnostic (IVD) device intended for use with FDA cleared or approved IVD BIOFIRE* FILMARRAY* Panels. The BIOFIRE FILMARRAY 2.0 System is intended for use in combination with assay specific reagent pouches to detect multiple nucleic acid targets contained in clinical specimens. The BIOFIRE FILMARRAY 2.0 Instrument interacts with the reagent pouch to both purify nucleic acids and amplify targeted nucleic acid sequences using nested multiplex PCR in a closed system. The resulting PCR products are evaluated using DNA melting analysis. The BIOFIRE FILMARRAY 2.0 software automatically determines the results and provides a test report.  The BIOFIRE FILMARRAY 2.0 System is composed of one to eight instruments connected to a computer running BIOFIRE FILMARRAY 2.0 Software. The software controls the function of each instrument and collects, analyzes, and stores data generated by each instrument.  The BIOFIRE FILMARRAY 2.0, hereafter referred to as the "System," is designed to run as a standalone device, but	See note
DOC-1         Manufacturer Name           DOC-2         Device Description           DOC-3         Device Model           DOC-4         Document ID		The BIOFIRE* FILMARRAY* 2.0 SYSTEM is an automated in vitro diagnostic (IVD) device intended for use with FDA cleared or approved IVD BIOFIRE* FILMARRAY* Panels. The BIOFIRE FILMARRAY 2.0 System is intended for use in combination with assay specific reagent pouches to detect multiple nucleic acid targets contained in clinical specimens. The BIOFIRE FILMARRAY 2.0 Instrument interacts with the reagent pouch to both purify nucleic acids and amplify targeted nucleic acid sequences using nested multiplex PCR in a closed system. The resulting PCR products are evaluated using DNA melting analysis. The BIOFIRE FILMARRAY 2.0 software automatically determines the results and provides a test report.  The BIOFIRE FILMARRAY 2.0 System is composed of one to eight instruments connected to a computer running BIOFIRE FILMARRAY 2.0 Software. The software controls the function of each instrument and collects, analyzes, and stores data generated by each instrument.  The BIOFIRE FILMARRAY 2.0, hereafter referred to as the "System," is designed to run as a standalone device, but	See note
DOC-2 Device Description DOC-3 Device Model DOC-4 Document ID		The BIOFIRE* FILMARRAY* 2.0 SYSTEM is an automated in vitro diagnostic (IVD) device intended for use with FDA cleared or approved IVD BIOFIRE* FILMARRAY* Panels. The BIOFIRE FILMARRAY 2.0 System is intended for use in combination with assay specific reagent pouches to detect multiple nucleic acid targets contained in clinical specimens. The BIOFIRE FILMARRAY 2.0 Instrument interacts with the reagent pouch to both purify nucleic acids and amplify targeted nucleic acid sequences using nested multiplex PCR in a closed system. The resulting PCR products are evaluated using DNA melting analysis. The BIOFIRE FILMARRAY 2.0 software automatically determines the results and provides a test report.  The BIOFIRE FILMARRAY 2.0 System is composed of one to eight instruments connected to a computer running BIOFIRE FILMARRAY 2.0 Software. The software controls the function of each instrument and collects, analyzes, and stores data generated by each instrument.  The BIOFIRE FILMARRAY 2.0, hereafter referred to as the "System," is designed to run as a standalone device, but	_
DOC-3 Device Model DOC-4 Document ID		Intended for use with FDA cleared or approved IVD BIOFIRE* FILMARRAY* Panels. The BIOFIRE FILMARRAY 2.0 System is intended for use in combination with assay specific reagent pouches to detect multiple nucleic acid targets contained in clinical specimens. The BIOFIRE FILMARRAY 2.0 Instrument interacts with the reagent pouch to both purify nucleic acids and amplify targeted nucleic acid sequences using nested multiplex PCR in a closed system. The resulting PCR products are evaluated using DNA melting analysis. The BIOFIRE FILMARRAY 2.0 software automatically determines the results and provides a test report.  The BIOFIRE FILMARRAY 2.0 System is composed of one to eight instruments connected to a computer running BIOFIRE FILMARRAY 2.0 Software. The software controls the function of each instrument and collects, analyzes, and stores data generated by each instrument.  The BIOFIRE FILMARRAY 2.0, hereafter referred to as the "System," is designed to run as a standalone device, but	
DOC-3 Device Model DOC-4 Document ID		contained in clinical specimens. The BIOFIRE FILMARRAY 2.0 Instrument interacts with the reagent pouch to both purify nucleic acids and amplify targeted nucleic acid sequences using nested multiplex PCR in a closed system. The resulting PCR products are evaluated using DNA melting analysis. The BIOFIRE FILMARRAY 2.0 software automatically determines the results and provides a test report.  The BIOFIRE FILMARRAY 2.0 System is composed of one to eight instruments connected to a computer running BIOFIRE FILMARRAY 2.0 Software. The software controls the function of each instrument and collects, analyzes, and stores data generated by each instrument.  The BIOFIRE FILMARRAY 2.0, hereafter referred to as the "System," is designed to run as a standalone device, but	
DOC-3 Device Model DOC-4 Document ID		purify nucleic acids and amplify targeted nucleic acid sequences using nested multiplex PCR in a closed system. The resulting PCR products are evaluated using DNA melting analysis. The BIOFIRE FILMARRAY 2.0 software automatically determines the results and provides a test report.  The BIOFIRE FILMARRAY 2.0 System is composed of one to eight instruments connected to a computer running BIOFIRE FILMARRAY 2.0 Software. The software controls the function of each instrument and collects, analyzes, and stores data generated by each instrument.  The BIOFIRE FILMARRAY 2.0, hereafter referred to as the "System," is designed to run as a standalone device, but	
DOC-3 Device Model DOC-4 Document ID		determines the results and provides a test report.  The BIOFIRE FILMARRAY 2.0 System is composed of one to eight instruments connected to a computer running BIOFIRE FILMARRAY 2.0 Software. The software controls the function of each instrument and collects, analyzes, and stores data generated by each instrument.  The BIOFIRE FILMARRAY 2.0, hereafter referred to as the "System," is designed to run as a standalone device, but	
DOC-3 Device Model DOC-4 Document ID		The BIOFIRE FILMARRAY 2.0 System is composed of one to eight instruments connected to a computer running BIOFIRE FILMARRAY 2.0 Software. The software controls the function of each instrument and collects, analyzes, and stores data generated by each instrument.  The BIOFIRE FILMARRAY 2.0, hereafter referred to as the "System," is designed to run as a standalone device, but	
DOC-3 Device Model DOC-4 Document ID		BIOFIRE FILMARRAY 2.0 Software. The software controls the function of each instrument and collects, analyzes, and stores data generated by each instrument.  The BIOFIRE FILMARRAY 2.0, hereafter referred to as the "System," is designed to run as a standalone device, but	
DOC-3 Device Model DOC-4 Document ID		stores data generated by each instrument.  The BIOFIRE FILMARRAY 2.0, hereafter referred to as the "System," is designed to run as a standalone device, but	
DOC-3 Device Model DOC-4 Document ID		The BIOFIRE FILMARRAY 2.0, hereafter referred to as the "System," is designed to run as a standalone device, but	
DOC-3 Device Model DOC-4 Document ID			
DOC-3 Device Model DOC-4 Document ID		includes optional network-connected features. See DOC-6.	
DOC-3 Device Model DOC-4 Document ID			
DOC-4 Document ID			_
		BIOFIRE® FILMARRAY® 2.0 SYSTEM FLM2-PRT-0268-07	_
DOC-5 Manufacturer Contact Inform		BIOFIRE Technical Support	_
DOC-5 Manufacturer Contact Inforn		Email: Biofiresupport@biomerieux.com	
	ation	<u>Phone: +1-801-736-6354, select Option 5</u> 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 optional connectivity software features that can be	
		enabled in a network-connected environment.	
		The System can be configured to interface with a laboratory information system (LIS) to transfer test results from the	
		System to the LIS (unidirectional) or to transfer data to and from the LIS (bidirectional), dependent on the selected	
		configuration. This optional software feature requires a connection to the local area network (LAN) at the facility.	
		The System can be configured to facilitate remote access for customer support activities. Additionally, with this	
		configuration, the end-user can send data from the System to bioMérieux for troubleshooting. This configuration	
		allows software updates to be pushed to the system. This optional software feature requires an Internet connection to pre-defined endpoints.	
		The System can be configured to perform an encrypted outbound transfer of de-identified, aggregated System test data to a cloud-based epidemiology network that collects, compiles and displays test results from participating	
		hospitals and laboratories across the globe. This optional software feature requires an Internet connection to a pre-	
		defined endpoint.	
		The System can be configured to interface with an Institution-specific cloud-based data management portal, inclusive	
		of encrypted outbound transfer of Test and System Data. This optional software feature requires an Internet	
		connection to a pre-defined endpoint.	
DOC-6 Intended use of device in net	work-connected environment:		
DOC-7 Document Release Date		7/11/2023	_
Coordinated Vulnerability Dir	closure: Does the manufacturer		
DOC-8 have a vulnerability disclosur		Yes	_
	t of an Information Sharing and		
DOC-9 Analysis Organization?  Diagram: Is a network or data	flow diagram available that	Yes	
	r system components or expected		
DOC-10 external resources?		Yes	
DOC-11 SaMD: is the device software only, no hardware)?	as a Medical Device (i.e. software-	No	
DOC-11.1 Does the SaMD contain an op		N/A	
Does the SaMD rely on an ow system?	ner/operator provided operating	N/A	
DOC-11.2 System:  DOC-11.3 Is the SaMD hosted by the ma	anufacturer?	N/A	
DOC-11.4 Is the SaMD hosted by the cu	stomer?	N/A	_
		Yes, No,	
		N/A, or	
MANAGEMENT OF PERSO	NALLY IDENTIFIADI E	See Note	Note #
INFORMATION			
Can this device display, trans	mit, store, or modify personally		
identifiable information (e.g. MPII-1 Information (ePHI))?	electronic Protected Health	Saa Notas	Note 1
iniormation (ePHIJ)?		See Notes	Note 1
	sonally identifiable information?	See Notes	Note 2
	sonally identifiable information ry (i.e., until cleared by power-off or		
MPII-2.1 reset)?		No	_
Does the device store person		Con Nation	Nete 2
MPII-2.2 persistently on internal media	mation preserved in the device's	See Notes	Note 3
MPII-2.3 non-volatile memory until ex	olicitly erased?	See Notes	Note 4
	ally identifiable information in a	Soo Notes	Note E
MPII-2.4 database?  Does the device allow configu	ration to automatically delete local	See Notes	Note 5
personally identifiable inform	ation after it is stored to a long		
MPII-2.5 term solution?	rt personally identifiable	See Notes	Note 6
Does the device import/expo information with other syster	rt personally identifiable ns (e.g., a wearable monitoring		
device might export personal	ly identifiable information to a		
MPII-2.6 server)?		See Notes	Note 7
Does the device maintain per	sonally identifiable information		
MPII-2.7 when powered off, or during	power service interruptions?	See Notes	Note 8
	ernal media to be removed by a eparate destruction or customer		
MPII-2.8 retention)?	parate destruction of customer	No	_
Does the device allow person records be stored in a separa	ally identifiable information te location from the device's		
	ary internal drive, alternate drive		
MPII-2.9 partition, or remote storage I		See Notes	Note 9

BioFire Diagnostics, LLC	BIOFIRE® FILMARRAY® 2.0 SYSTEM	FLM2-PRT-0268-07	11-Jul-2023
MPII-3	Does the device have mechanisms used for the transmitting, importing/exporting of personally identifiable information?	See Notes	Note 10
	Does the device display personally identifiable information (e.g.,		
MPII-3.1	video display, etc.)?  Does the device generate hardcopy reports or images containing	See Notes	Note 11
MPII-3.2	personally identifiable information?	See Notes	Note 12
	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-		
MPII-3.3	R/RW, tape, CF/SD card, memory stick, etc.)?  Does the device transmit/receive or import/export personally	See Notes	Note 13
MPII-3.4	identifiable information via dedicated cable connection (e.g., RS-232, RS-423, USB, FireWire, etc.)?	See Notes	Note 14
	Does the device transmit/receive personally identifiable		
MPII-3.5	information via a wired network connection (e.g., RJ45, fiber optic, etc.)?	See Notes	Note 15
	Does the device transmit/receive personally identifiable		
MPII-3.6	information via a wireless network connection (e.g., Wi-Fi, Bluetooth, NFC, infrared, cellular, etc.)?	No	
MPII-3.7	Does the device transmit/receive personally identifiable information over an external network (e.g., Internet)?	See Notes	Note 16
MPII-3.8	Does the device import personally identifiable information via scanning a document?	No	
MPII-3.9	Does the device transmit/receive personally identifiable information via a proprietary protocol?	No	
	Does the device use any other mechanism to transmit, import or		
MPII-3.10	export personally identifiable information?	No.	
	AUTOMATIC LOGOFF (ALOF)		
	The device's ability to prevent access and misuse by		
	unauthorized users if device is left idle for a period of time.		
	Can the device be configured to force reauthorization of logged- in user(s) after a predetermined length of inactivity (e.g., auto-		
ALOF-1	logoff, session lock, password protected screen saver)?	No	
ALOF-2	Is the length of inactivity time before auto-logoff/screen lock user or administrator configurable?	N/A	_
	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?	No	_
AUDT-1.1	Does the audit log record a USER ID?  Does other personally identifiable information exist in the audit	N/A	
AUDT-1.2	trail?	N/A	
	Are events recorded in an audit log? If yes, indicate which of the		
AUDT-2 AUDT-2.1		N/A N/A	
AUDT-2.2 AUDT-2.3		N/A N/A	_
AUDT-2.4 AUDT-2.5	Creation/modification/deletion of users?  Presentation of clinical or PII data (e.g. display, print)?	N/A N/A	_
AUDT-2.6	Creation/modification/deletion of data?	N/A	
AUDT-2.7	Import/export of data from removable media (e.g. USB drive, external hard drive, DVD)?	N/A	_
AUDT-2.8	Receipt/transmission of data or commands over a network or point-to-point connection?	N/A	
AUDT-2.8.1		N/A	
AUDT-2.8.2	Application Programming Interface (API) and similar activity?	N/A	
AUDT-2.9 AUDT-2.10	Other events (e.g., software updates)?	N/A N/A	
AUDT-2.11	Is the audit capability documented in more detail?  Can the owner/operator define or select which events are	N/A	
AUDT-3	recorded in the audit log?  Is a list of data attributes that are captured in the audit log for an	N/A	
AUDT-4	event available?	N/A	
AUDT-4.1	Does the audit log record date/time?  Can date and time be synchronized by Network Time Protocol	N/A	_
AUDT-4.1.1 AUDT-5		N/A N/A	
AUDT-5.1	Via physical media?  Via IHE Audit Trail and Node Authentication (ATNA) profile to	N/A	
AUDT-5.2	Via Other communications (e.g., external service device, mobile	N/A	_
AUDT-5.3	applications)?	N/A	
AUDT-5.4		N/A	
AUDT-6 AUDT-7	Can audit logs be monitored/reviewed by owner/operator?  Are audit logs protected from modification?	N/A N/A	_
AUDT-7.1 AUDT-8	Are audit logs protected from access?	N/A N/A	
NOD1=0	Can additings be analyzed by the devices	IN/A	_
	AUTHORIZATION (AUTH)		
	The ability of the device to determine the authorization of users.		
	Does the device prevent access to unauthorized users through		
AUTH-1	user login requirements or other mechanism?	See Notes	Note 17
AUTH-1.1	Can the device be configured to use federated credentials management of users for authorization (e.g., LDAP, OAuth)?	No	
	, CAULI):	j <del>.</del>	

	DIOCIDE CULTURE DAVE O O CICTERA	51 43 DDT D350 DZ	44
BioFire Diagnostics, LLC	BIOFIRE® FILMARRAY® 2.0 SYSTEM	FLM2-PRT-0268-07	11-Jul-2023
AUTH-1.2	Can the customer push group policies to the device (e.g., Active Directory)?	No	
	Are any special groups, organizational units, or group policies		_
AUTH-1.3	required?  Can users be assigned different privilege levels based on 'role'	No .	_
AUTH-2	(e.g., user, administrator, and/or service, etc.)?	No .	_
	Can the device owner/operator grant themselves unrestricted		
AUTH-3	administrative privileges (e.g., access operating system or application via local root or administrator account)?	See Notes	Note 18
AUTH-4	Does the device authorize or control all API access requests?	See Notes	Note 19
AUTH-5	Does the device run in a restricted access mode, or 'kiosk mode', by default?		
AUTH-5	by default?	No .	_
	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	Yes	
CSUP-2	2.1-2.4.	Yes	
CSUP-2.1	Does the device documentation provide instructions for owner/operator installation of patches or software updates?	See Notes	Note 20
	Does the device require vendor or vendor-authorized service to		100.6 20
CSUP-2.2	install patches or software updates?  Does the device have the capability to receive remote	No .	
CSUP-2.3	installation of patches or software updates?	See Notes	Note 21
	Does the medical device manufacturer allow security updates		
CSUP-2.4	from any third-party manufacturers (e.g., Microsoft) to be installed without approval from the manufacturer?	See Notes	Note 22
CSUP-3	Does the device contain Drivers and Firmware? If yes, complete 3.1-3.4.	Yes	
	Does the device documentation provide instructions for		
CSUP-3.1	owner/operator installation of patches or software updates?	See Notes	Note 23
CSUP-3.2	Does the device require vendor or vendor-authorized service to install patches or software updates?	See Notes	Note 24
CSUP-3.3	Does the device have the capability to receive remote installation of patches or software updates?	No	
	Does the medical device manufacturer allow security updates		
	from any third-party manufacturers (e.g., Microsoft) to be		
CSUP-3.4	installed without approval from the manufacturer?  Does the device contain Anti-Malware Software? If yes,	See Notes	Note 25
CSUP-4	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 26
	Does the device require vendor or vendor-authorized service to		Note 20
CSUP-4.2	install patches or software updates?  Does the device have the capability to receive remote	No .	
CSUP-4.3	installation of patches or software updates?	No .	
	Does the medical device manufacturer allow security updates from any third-party manufacturers (e.g., Microsoft) to be		
CSUP-4.4	installed without approval from the manufacturer?	See Notes	Note 27
	Does the device contain Non-Operating System commercial off-		
CSUP-5	the-shelf components? If yes, complete 5.1-5.4.	Yes	
	Does the device documentation provide instructions for		
CSUP-5.1	owner/operator installation of patches or software updates?  Does the device require vendor or vendor-authorized service to	No .	
CSUP-5.2	install patches or software updates?  Does the device have the capability to receive remote	Yes	
CSUP-5.3	installation of patches or software updates?	See Notes	Note 28
	Does the medical device manufacturer allow security updates		
CSUP-5.4	from any third-party manufacturers (e.g., Microsoft) to be installed without approval from the manufacturer?	No	
	Does the device contain other software components (e.g., asset		
CSUB 5	management software, license management)? If yes, please	No.	
CSUP-6	provide details or reference in notes and complete 6.1-6.4.	No .	
CSUP-6.1	Does the device documentation provide instructions for owner/operator installation of patches or software updates?	N/A	
CSUP-6.2	Does the device require vendor or vendor-authorized service to install patches or software updates?	N/A	
	Does the device have the capability to receive remote		
CSUP-6.3	installation of patches or software updates?	N/A	
	Does the medical device manufacturer allow security updates from any third-party manufacturers (e.g., Microsoft) to be		
CSUP-6.4	installed without approval from the manufacturer?  Does the manufacturer notify the customer when updates are	N/A	
CSUP-7	approved for installation?	Yes	
CSUP-8	Does the device perform automatic installation of software updates?	See Notes	Note 29
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-	N/A	
CSUP-10	party software on the device themselves?  Does the system have mechanism in place to prevent installation		
CSUP-10.1	of unapproved software?	N/A	

	T		I
BioFire Diagnostics, LLC	BIOFIRE® FILMARRAY® 2.0 SYSTEM	FLM2-PRT-0268-07	11-Jul-2023
	Does the manufacturer have a process in place to assess device		
CSUP-11	vulnerabilities and updates?  Does the manufacturer provide customers with review and	Yes	_
CSUP-11.1	approval status of updates?	No	_
CSUP-11.2	Is there an update review cycle for the device?	Yes	_
	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 30
	Does the device support de-identification profiles that comply		
DIDT-1.1	with the DICOM standard for de-identification?	N/A	_
	DATA BACKUP AND DISASTER RECOVERY (DTBK)		
	The ability to recover after damage or destruction of device		
	data, hardware, software, or site configuration information.  Does the device maintain long term primary storage of		
	personally identifiable information / patient information (e.g.		
DTBK-1	PACS)?	See Notes	Note 31
	Does the device have a "factory reset" function to restore the		
DTBK-2	original device settings as provided by the manufacturer?	No	_
DTBK-3	Does the device have an integral data backup capability to removable media?	No	
DTBK-4	Does the device have an integral data backup capability to	No.	
D101~4	remote storage?  Does the device have a backup capability for system	No	
DTDV 5	configuration information, patch restoration, and software	No.	
DTBK-5	restoration?  Does the device provide the capability to check the integrity and	No .	
DTBK-6	authenticity of a backup?	No.	_
	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-		
EMRG-1	glass") feature?	N/A	
	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		
IGAU-1	stored health data (e.g., hash or digital signature)?	No .	
	Does the device provide error/failure protection and recovery		
IGAU-2	mechanisms for stored health data (e.g., RAID-5)?	No .	
	MALWARE DETECTION/PROTECTION (MLDP)  The ability of the device to effectively prevent, detect and		
	remove malicious software (malware).		
MLDP-1	Is the device capable of hosting executable software?  Does the device support the use of anti-malware software (or	Yes	
	other anti-malware mechanism)? Provide details or reference in		
MLDP-2	notes.	Yes	_
MLDP-2.1	Does the device include anti-malware software by default?	Yes	
MLDP-2.2	Does the device have anti-malware software available as an option?	No	
MLDP-2.3	Does the device documentation allow the owner/operator to install or update anti-malware software?	No	
	Can the device owner/operator independently (re-)configure		
MLDP-2.4	anti-malware settings?  Does notification of malware detection occur in the device user	No .	_
MLDP-2.5	interface?	No	
MLDP-2.6	Can only manufacturer-authorized persons repair systems when malware has been detected?	See Notes	Note 32
MLDP-2.7	Are malware notifications written to a log?	See Notes	Note 33
	Are there any restrictions on anti-malware (e.g., purchase, installation, configuration, scheduling)?	Yes	
MLDP-2.8	installation, configuration, scheduling)?  If the answer to MLDP-2 is NO, and anti-malware cannot be		
MLDP-2.8	installation, configuration, scheduling)?  If the answer to MLDP-2 is NO, and anti-malware cannot be installed on the device, are other compensating controls in place	Yes	
	installation, configuration, scheduling)?  If the answer to MLDP-2 is NO, and anti-malware cannot be installed on the device, are other compensating controls in place or available?  Does the device employ application whitelisting that restricts the	Yes N/A	
MLDP-2.8	installation, configuration, scheduling)?  If the answer to MLDP-2 is NO, and anti-malware cannot be installed on the device, are other compensating controls in place or available?  Does the device employ application whitelisting that restricts the software and services that are permitted to be run on the	Yes N/A	
MLDP-2.8 MLDP-3 MLDP-4	installation, configuration, scheduling)?  If the answer to MLDP-2 is NO, and anti-malware cannot be installed on the device, are other compensating controls in place or available?  Does the device employ application whitelisting that restricts the software and services that are permitted to be run on the device?  Does the device employ a host-based intrusion	Yes N/A No	
MLDP-2.8	installation, configuration, scheduling)?  If the answer to MLDP-2 is NO, and anti-malware cannot be installed on the device, are other compensating controls in place or available?  Does the device employ application whitelisting that restricts the software and services that are permitted to be run on the device?  Does the device employ a host-based intrusion detection/prevention system?	Yes N/A	
MLDP-2.8 MLDP-3 MLDP-4	installation, configuration, scheduling)?  If the answer to MLDP-2 is NO, and anti-malware cannot be installed on the device, are other compensating controls in place or available?  Does the device employ application whitelisting that restricts the software and services that are permitted to be run on the device?  Does the device employ a host-based intrusion detection/prevention system?  Can the host-based intrusion detection/prevention system be configured by the customer?	Yes N/A No	
MLDP-2.8  MLDP-3  MLDP-4  MLDP-5  MLDP-5.1	installation, configuration, scheduling)?  If the answer to MLDP-2 is NO, and anti-malware cannot be installed on the device, are other compensating controls in place or available?  Does the device employ application whitelisting that restricts the software and services that are permitted to be run on the device?  Does the device employ a host-based intrusion detection/prevention system?  Can the host-based intrusion detection/prevention system be configured by the customer?  Can a host-based intrusion detection/prevention system be	Yes  N/A  No  No  No  N/A	Note 34
MLDP-2.8  MLDP-3  MLDP-4  MLDP-5	installation, configuration, scheduling)?  If the answer to MLDP-2 is NO, and anti-malware cannot be installed on the device, are other compensating controls in place or available?  Does the device employ application whitelisting that restricts the software and services that are permitted to be run on the device?  Does the device employ a host-based intrusion detection/prevention system?  Can the host-based intrusion detection/prevention system be configured by the customer?	Yes N/A No No	Note 34
MLDP-2.8  MLDP-3  MLDP-4  MLDP-5  MLDP-5.1	installation, configuration, scheduling)?  If the answer to MLDP-2 is NO, and anti-malware cannot be installed on the device, are other compensating controls in place or available?  Does the device employ application whitelisting that restricts the software and services that are permitted to be run on the device?  Does the device employ a host-based intrusion detection/prevention system?  Can the host-based intrusion detection/prevention system be configured by the customer?  Can a host-based intrusion detection/prevention system be installed by the customer?	Yes  N/A  No  No  No  N/A	Note 34
MLDP-2.8  MLDP-3  MLDP-4  MLDP-5  MLDP-5.1	installation, configuration, scheduling)?  If the answer to MLDP-2 is NO, and anti-malware cannot be installed on the device, are other compensating controls in place or available?  Does the device employ application whitelisting that restricts the software and services that are permitted to be run on the device?  Does the device employ a host-based intrusion detection/prevention system?  Can the host-based intrusion detection/prevention system be configured by the customer?  Can a host-based intrusion detection/prevention system be	Yes  N/A  No  No  No  N/A	Note 34

BioFire Diagnostics, LLC	BIOFIRE® FILMARRAY® 2.0 SYSTEM	FLM2-PRT-0268-07	11-Jul-2023
Sion in Diagnostics, LLC			1130-2023
	Does the device provide/support any means of node		
	authentication that assures both the sender and the recipient of		
NAUT-1	data are known to each other and are authorized to receive transferred information (e.g. Web APIs, SMTP, SNMP)?	See Notes	Note 35
	Are network access control mechanisms supported (E.g., does		
NAUT-2	the device have an internal firewall, or use a network connection white list)?	Yes	
NAUT-2.1	Is the firewall ruleset documented and available for review?	No	
	Does the device use certificate-based network connection		
NAUT-3	authentication?	See Notes	Note 36
	CONNECTIVITY CAPABILITIES (CONN)		
	All network and removable media connections must be		
	considered in determining appropriate security controls. This section lists connectivity capabilities that may be present on the device.		
CONN-1	Does the device have hardware connectivity capabilities?	See Notes	Note 37
CONN-1.1	Does the device support wireless connections?	No	
CONN-1.1.1 CONN-1.1.2	Does the device support Wi-Fi?  Does the device support Bluetooth?	No No	
	Does the device support other wireless network connectivity		
CONN-1.1.3	(e.g. LTE, Zigbee, proprietary)?  Does the device support other wireless connections (e.g.,	No .	
CONN-1.1.4	custom RF controls, wireless detectors)?	No	
CONN-1.2 CONN-1.2.1	Does the device support physical connections?  Does the device have available RJ45 Ethernet ports?	Yes Yes	_
CONN-1.2.2	Does the device have available USB ports?	See Notes	Note 38
CONN-1.2.3	Does the device require, use, or support removable memory devices?	See Notes	Note 39
CONN-1.2.4		No No	_
	Does the manufacturer provide a list of network ports and		
CONN-2	protocols that are used or may be used on the device?	Yes	
CONN-3	Can the device communicate with other systems within the customer environment?	See Notes	Note 40
COMITS		Sec Hotel	11010-10
CONN-4	Can the device communicate with other systems external to the customer environment (e.g., a service host)?	See Notes	Note 41
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?	No	
CONN-7	Does the device support Transport Layer Security (TLS)?	Yes	
CONN-7.1	Is TLS configurable?  Does the device provide operator control functionality from a	No .	
CONN-8	separate device (e.g., telemedicine)?	No	
	PERSON AUTHENTICATION (PAUT)		
	The ability to configure the device to authenticate users.		
PAUT-1	Does the device support and enforce unique IDs and passwords for all users and roles (including service accounts)?	No	
	Does the device enforce authentication of unique IDs and		
PAUT-1.1	passwords for all users and roles (including service accounts)?	N/A	_
	Is the device configurable to authenticate users through an external authentication service (e.g., MS Active Directory, NDS,		
PAUT-2	LDAP, OAuth, etc.)?  Is the device configurable to lock out a user after a certain	No .	
PAUT-3	number of unsuccessful logon attempts?	No	
	Are all default accounts (e.g., technician service accounts,		
PAUT-4	administrator accounts) listed in the documentation?	No No	
PAUT-5	Can all passwords be changed?  Is the device configurable to enforce creation of user account	No .	
	passwords that meet established (organization specific)		
PAUT-6	complexity rules?  Does the device support account passwords that expire	No .	
PAUT-7	periodically?	No	
PAUT-8 PAUT-9	Does the device support multi-factor authentication?  Does the device support single sign-on (SSO)?	No No	
PAUT-10	Can user accounts be disabled/locked on the device?	No	
PAUT-11	Does the device support biometric controls?	No .	
PAUT-12	Does the device support physical tokens (e.g. badge access)?	No	
PAUT-13	Does the device support group authentication (e.g. hospital teams)?	No	
	Does the application or device store or manage authentication		
PAUT-14 PAUT-14.1	credentials?  Are credentials stored using a secure method?	Yes 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		
PLOK-1	Is the device software only? If yes, answer "N/A" to remaining 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 43
	Are all device components maintaining personally identifiable information (other than removable media) physically secured		
PLOK-3	Are all device components maintaining personally identifiable information (other than removable media) physically secured behind an individually keyed locking device?	See Notes	Note 44
PLOK-3	information (other than removable media) physically secured	See Notes	Note 44

			T
BioFire Diagnostics, LLC	BIOFIRE® FILMARRAY® 2.0 SYSTEM	FLM2-PRT-0268-07	11-Jul-2023
	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		
RDMP-1	27034 or IEC 62304, followed during product development?	See Notes	Note 45
	Does the manufacturer evaluate third-party applications and		
RDMP-2	software components included in the device for secure development practices?	Yes	
20140.3	Does the manufacturer maintain a web page or other source of information on software support dates and updates?	Yes	
RDMP-3	Does the manufacturer have a plan for managing third-party	Tes	_
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 Sob for this product available?  Does the Sob follow a standard or common method in describing	Yes	
SBOM-2	software components?	Yes	
SBOM-2.1	Are the software components identified?	Yes	
SBOM-2.2	Are the developers/manufacturers of the software components identified?	Yes	
	Are the major version numbers of the software components		
SBOM-2.3	identified?	Yes	_
SBOM-2.4	Are any additional descriptive elements identified?  Does the device include a command or process method available	No .	
	to generate a list of software components installed on the		
SBOM-3 SBOM-4	device? Is there an update process for the Sob?	No Yes	
3BOIVI-4	is there an update process for the 300:	TES .	
	SYSTEM AND APPLICATION HARDENING (SAHD)		
	The desirate inhouse transition as to substitute and and such some		
	The device's inherent resistance to cyber attacks and malware.  Is the device hardened in accordance with any industry		
SAHD-1	standards?	No	_
SAHD-2	Has the device received any cybersecurity certifications?	No	
JAND-2	Does the device received any cybersecurity certifications:	NO .	
SAHD-3	checking?	No	
	Does the device employ any mechanism (e.g., release-specific		
	hash key, checksums, digital signature, etc.) to ensure the		
SAHD-3.1	installed software is manufacturer-authorized?	See Notes	Note 46
	Does the device employ any mechanism (e.g., release-specific		
	hash key, checksums, digital signature, etc.) to ensure the		
SAHD-3.2	software updates are the manufacturer-authorized updates?	Yes	_
	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-		
SAHD-5	level, patient level, or other types of access controls?	No	
SAHD-5.1	Does the device provide role-based access controls?  Are any system or user accounts restricted or disabled by the	No .	_
SAHD-6	manufacturer at system delivery?	See Notes	Note 47
CALID C 1	Are any system or user accounts configurable by the end user	No.	
SAHD-6.1	after initial configuration?	No .	
	Does this include restricting certain system or user accounts,		
SAHD-6.2	such as service technicians, to least privileged access?  Are all shared resources (e.g., file shares) which are not required	No .	
SAHD-7	for the intended use of the device disabled?	N/A	
	Are all communication ports and protocols that are not required		
SAHD-8	for the intended use of the device disabled?	See Notes	Note 48
	Are all services (e.g., telnet, file transfer protocol [FTP], internet		
CALID O	information server [IIS], etc.), which are not required for the	No	
SAHD-9	intended use of the device deleted/disabled?	No .	
	Are all applications (COTS applications as well as OS-included		
SAHD-10	applications, e.g., MS Internet Explorer, etc.) which are not required for the intended use of the device deleted/disabled?	No	
JAU10-10	can the device prohibit boot from uncontrolled or removable	INO	
	media (i.e., a source other than an internal drive or memory		
SAHD-11	component)?  Can unauthorized software or hardware be installed on the	No .	
SAHD-12	device without the use of physical tools?	Yes	
	Does the product documentation include information on	No.	
SAHD-13	operational network security scanning by users?	No .	_
SAHD-14	Can the device be hardened beyond the default provided state?	See Notes	Note 49
1	Are instructions available from vendor for increased hardening?	San Notes	Note 50
SAHD-14 1	TOTAL INSURCIOUS AVAILABLE IT OFF VEHICUT FOR INCREASED HARDENING?	SEC HOLES	Note 50
SAHD-14.1	Can the system prevent access to BIOS or other bootloaders		
SAHD-14.1 SHAD-15	Can the system prevent access to BIOS or other bootloaders during boot?	Yes	
SHAD-15	Can the system prevent access to BIOS or other bootloaders during boot?  Have additional hardening methods not included in 2.3.19 been		Note 51
	Can the system prevent access to BIOS or other bootloaders during boot?	Yes See Notes	Note 51
SHAD-15	Can the system prevent access to BIOS or other bootloaders during boot?  Have additional hardening methods not included in 2.3.19 been		Note 51

BioFire Diagnostics, LLC	BIOFIRE® FILMARRAY® 2.0 SYSTEM	FLM2-PRT-0268-07	11-Jul-2023
	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?	No Control of the Con	_
SGUD-3	Are all access accounts documented?	No	
SGUD-3.1	Can the owner/operator manage password control for all accounts?	No	
	Does the product include documentation on recommended		
SGUD-4	compensating controls for the device?	No Control of the Con	_
	HEALTH DATA STORAGE CONFIDENTIALITY (STCF)  The ability of the device to ensure unauthorized access does not		
	compromise the integrity and confidentiality of personally		
	identifiable information stored on the device or removable media.		
STCF-1	Can the device encrypt data at rest?	No	_
STCF-1.1 STCF-1.2	Is all data encrypted or otherwise protected?  Is the data encryption capability configured by default?	See Notes N/A	Note 52
	Are instructions available to the customer to configure		
STCF-1.3 STCF-2	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 53
	TRANSMISSION CONFIDENTIALITY (TXCF)  The ability of the device to ensure the confidentiality of		
	transmitted personally identifiable information.		
TXCF-1	Can personally identifiable information be transmitted only via a point-to-point dedicated cable?	No	
	Is personally identifiable information encrypted prior to		
TXCF-2	transmission via a network or removable media?  If data is not encrypted by default, can the customer configure	See Notes	Note 54
TXCF-2.1	encryption options?	N/A	
TXCF-3	Is personally identifiable information transmission restricted to a fixed list of network destinations?	No.	
TXCF-4	Are connections limited to authenticated systems?	See Notes	Note 55
TXCF-5	Are secure transmission methods supported/implemented (DICOM, HL7, IEEE 11073)?	See Notes	Note 56
	TRANSMISSION INTEGRITY (TXIG)		
	The ability of the device to ensure the integrity of transmitted		
	data.		
	9010.		
	Does the device support any mechanism (e.g., digital signatures)		
TXIG-1	Does the device support any mechanism (e.g., digital signatures) intended to ensure data is not modified during transmission?	See Notes	Note 57
TXIG-1 TXIG-2	Does the device support any mechanism (e.g., digital signatures)	See Notes Yes	Note 57
	Does the device support any mechanism (e.g., digital signatures) intended to ensure data is not modified during transmission?  Does the device include multiple sub-components connected by		Note 57
	Does the device support any mechanism (e.g., digital signatures) intended to ensure data is not modified during transmission?  Does the device include multiple sub-components connected by external cables?  REMOTE SERVICE (RMOT)		Note 57
	Does the device support any mechanism (e.g., digital signatures) intended to ensure data is not modified during transmission?  Does the device include multiple sub-components connected by external cables?  REMOTE SERVICE (RMOT)  Remote service refers to all kinds of device maintenance		Note 57
	Does the device support any mechanism (e.g., digital signatures) intended to ensure data is not modified during transmission? Does the device include multiple sub-components connected by external cables?  REMOTE SERVICE (RMOT)  Remote service refers to all kinds of device maintenance activities performed by a service person via network or other remote connection.		Note 57
TXIG-2	Does the device support any mechanism (e.g., digital signatures) intended to ensure data is not modified during transmission?  Does the device include multiple sub-components connected by external cables?  REMOTE SERVICE (RMOT)  Remote service refers to all kinds of device maintenance activities performed by a service person via network or other remote connection.  Does the device permit remote service connections for device	Yes	
TXIG-2	Does the device support any mechanism (e.g., digital signatures) intended to ensure data is not modified during transmission? Does the device include multiple sub-components connected by external cables?  REMOTE SERVICE (RMOT) Remote service refers to all kinds of device maintenance activities performed by a service person via network or other remote connection. Does the device permit remote service connections for device analysis or repair? Does the device allow the owner/operator to initiative remote		Note 57
TXIG-2	Does the device support any mechanism (e.g., digital signatures) intended to ensure data is not modified during transmission?  Does the device include multiple sub-components connected by external cables?  REMOTE SERVICE (RMOT)  Remote service refers to all kinds of device maintenance activities performed by a service person via network or other remote connection.  Does the device permit remote service connections for device analysis or repair?	Yes	
TXIG-2	Does the device support any mechanism (e.g., digital signatures) intended to ensure data is not modified during transmission? Does the device include multiple sub-components connected by external cables?  REMOTE SERVICE (RMOT)  Remote service refers to all kinds of device maintenance activities performed by a service person via network or other remote connection.  Does the device permit remote service connections for device analysis or repair?  Does the device allow the owner/operator to initiative remote service sessions for device analysis or repair?	Yes  See Notes	
RMOT-1 RMOT-1.1 RMOT-1.2	Does the device support any mechanism (e.g., digital signatures) intended to ensure data is not modified during transmission?  Does the device include multiple sub-components connected by external cables?  REMOTE SERVICE (RMOT)  Remote service refers to all kinds of device maintenance octivities performed by a service person via network or other remote connection.  Does the device permit remote service connections for device analysis or repair?  Does the device allow the owner/operator to initiative remote service service sessions for device analysis or repair?	Yes  See Notes  No  See Notes	Note 58
RMOT-1 RMOT-1.1 RMOT-1.2 RMOT-1.3	Does the device support any mechanism (e.g., digital signatures) intended to ensure data is not modified during transmission?  Does the device include multiple sub-components connected by external cables?  REMOTE SERVICE (RMOT)  Remote service refers to all kinds of device maintenance activities performed by a service person via network or other remote connection.  Does the device permit remote service connections for device analysis or repair?  Does the device allow the owner/operator to initiative remote service sessions for device analysis or repair?  Is there an indicator for an enabled and active remote session?  Can patient data be accessed or viewed from the device during the remote session?  Does the device permit or use remote service connections for	Yes  See Notes  No  See Notes  See Notes	Note 58 Note 59 Note 60
RMOT-1 RMOT-1.1 RMOT-1.2	Does the device support any mechanism (e.g., digital signatures) intended to ensure data is not modified during transmission? Does the device include multiple sub-components connected by external cables?  REMOTE SERVICE (RMOT)  Remote service refers to all kinds of device maintenance activities performed by a service person via network or other remote connection.  Does the device permit remote service connections for device analysis or repair?  Does the device allow the owner/operator to initiative remote service sessions for device analysis or repair?  Is there an indicator for an enabled and active remote session?  Can patient data be accessed or viewed from the device during the remote session?	Yes  See Notes  No  See Notes  See Notes  See Notes  See Notes	Note 58
RMOT-1 RMOT-1.1 RMOT-1.2 RMOT-1.3	Does the device support any mechanism (e.g., digital signatures) intended to ensure data is not modified during transmission?  Does the device include multiple sub-components connected by external cables?  REMOTE SERVICE (RMOT)  Remote service refers to all kinds of device maintenance activities performed by a service person via network or other remote connection.  Does the device permit remote service connections for device analysis or repair?  Does the device allow the owner/operator to initiative remote service sessions for device analysis or repair?  Is there an indicator for an enabled and active remote session?  Can patient data be accessed or viewed from the device during the remote session?  Does the device permit or use remote service connections for predictive maintenance data?	Yes  See Notes  No  See Notes  See Notes  See Notes  See Notes	Note 58 Note 59 Note 60
RMOT-1 RMOT-1.1 RMOT-1.2 RMOT-1.3 RMOT-2	Does the device support any mechanism (e.g., digital signatures) intended to ensure data is not modified during transmission?  Does the device include multiple sub-components connected by external cables?  REMOTE SERVICE (RMOT)  Remote service refers to all kinds of device maintenance activities performed by a service person via network or other remote connection.  Does the device allow the owner/operator to initiative remote service allow the owner/operator to initiative remote service sessions for device analysis or repair?  Is there an indicator for an enabled and active remote session?  Can patient data be accessed or viewed from the device during the remote session?  Does the device have any other remote service connections for predictive maintenance data?  Does the device have any other remotely accessible functionality	Yes  See Notes  No See Notes See Notes See Notes	Note 58  Note 59  Note 60  Note 61
RMOT-1 RMOT-1.1 RMOT-1.2 RMOT-1.3 RMOT-2	Does the device support any mechanism (e.g., digital signatures) intended to ensure data is not modified during transmission?  Does the device include multiple sub-components connected by external cables?  REMOTE SERVICE (RMOT)  Remote service refers to all kinds of device maintenance activities performed by a service person via network or other remote connection.  Does the device allow the owner/operator to initiative remote service allow the owner/operator to initiative remote service sessions for device analysis or repair?  Is there an indicator for an enabled and active remote session?  Can patient data be accessed or viewed from the device during the remote session?  Does the device have any other remote service connections for predictive maintenance data?  Does the device have any other remotely accessible functionality	Yes  See Notes  No See Notes See Notes See Notes	Note 58  Note 59  Note 60  Note 61
RMOT-1 RMOT-1.1 RMOT-1.2 RMOT-1.3 RMOT-2	Does the device support any mechanism (e.g., digital signatures) intended to ensure data is not modified during transmission? Does the device include multiple sub-components connected by external cables?  REMOTE SERVICE (RMOT)  Remote service refers to all kinds of device maintenance activities performed by a service person via network or other remote connection.  Does the device permit remote service connections for device analysis or repair?  Does the device allow the owner/operator to initiative remote service sessions for device analysis or repair?  Is there an indicator for an enabled and active remote session?  Can patient data be accessed or viewed from the device during the remote session?  Does the device permit or use remote service connections for predictive maintenance data?  Does the device have any other remotely accessible functionality (e.g. software updates, remote training)?	Yes  See Notes  No See Notes See Notes See Notes	Note 58  Note 59  Note 60  Note 61
RMOT-1 RMOT-1.1 RMOT-1.2 RMOT-1.3 RMOT-2	Does the device support any mechanism (e.g., digital signatures) intended to ensure data is not modified during transmission?  Does the device include multiple sub-components connected by external cables?  REMOTE SERVICE (RMOT)  Remote service refers to all kinds of device maintenance activities performed by a service person via network or other remote connection.  Does the device allow the owner/operator to initiative remote service allow the owner/operator to initiative remote service sessions for device analysis or repair?  Is there an indicator for an enabled and active remote session?  Can patient data be accessed or viewed from the device during the remote session?  Does the device have any other remote service connections for predictive maintenance data?  Does the device have any other remotely accessible functionality	Yes  See Notes  No See Notes See Notes See Notes	Note 58  Note 59  Note 60  Note 61
RMOT-1 RMOT-1.1 RMOT-1.2 RMOT-1.3 RMOT-2	Does the device support any mechanism (e.g., digital signatures) intended to ensure data is not modified during transmission? Does the device include multiple sub-components connected by external cables?  REMOTE SERVICE (RMOT)  Remote service refers to all kinds of device maintenance activities performed by a service person via network or other remote connection.  Does the device permit remote service connections for device analysis or repair?  Does the device allow the owner/operator to initiative remote service sessions for device analysis or repair?  Is there an indicator for an enabled and active remote session?  Can patient data be accessed or viewed from the device during the remote session?  Does the device permit or use remote service connections for predictive maintenance data?  Does the device have any other remotely accessible functionality (e.g. software updates, remote training)?  OTHER SECURITY CONSIDERATIONS (OTHR)	Yes  See Notes  No See Notes See Notes See Notes	Note 58  Note 59  Note 60  Note 61
RMOT-1 RMOT-1.1 RMOT-1.2 RMOT-1.3 RMOT-2	Does the device support any mechanism (e.g., digital signatures) intended to ensure data is not modified during transmission?  Does the device include multiple sub-components connected by external cables?  REMOTE SERVICE (RMOT)  Remote service refers to all kinds of device maintenance activities performed by a service person via network or other remote connection.  Does the device permit remote service connections for device analysis or repair?  Does the device allow the owner/operator to initiative remote service sessions for device analysis or repair?  Is there an indicator for an enabled and active remote during the remote session?  Can patient data be accessed or viewed from the device during the remote session?  Does the device permit or use remote service connections for predictive maintenance data?  Does the device have any other remotely accessible functionality (e.g. software updates, remote training)?  OTHER SECURITY CONSIDERATIONS (OTHR)  NOME  Notes:  The following data fields are associated with each test on the	Yes  See Notes  No See Notes See Notes See Notes	Note 58  Note 59  Note 60  Note 61
RMOT-1 RMOT-1.1 RMOT-1.2 RMOT-1.3 RMOT-2	Does the device support any mechanism (e.g., digital signatures) intended to ensure data is not modified during transmission? Does the device include multiple sub-components connected by external cables?  REMOTE SERVICE (RMOT)  Remote service refers to all kinds of device maintenance activities performed by a service person via network or other remote connection.  Does the device allow the owner/operator to initiative remote service allow the owner/operator to initiative remote service sessions for device analysis or repair?  Is there an indicator for an enabled and active remote session?  Can patient data be accessed or viewed from the device during the remote session?  Does the device permit or use remote service connections for predictive maintenance data?  Does the device permit or use remote service connections for predictive maintenance data?  Does the device have any other remotely accessible functionality (e.g. software updates, remote training)?  OTHER SECURITY CONSIDERATIONS (OTHR)  NONE  Notes:  The following data fields are associated with each test on the System: Run Date, Serial Number (of consumable), Lot Number	Yes  See Notes  No See Notes See Notes See Notes	Note 58  Note 59  Note 60  Note 61
RMOT-1 RMOT-1.1 RMOT-1.2 RMOT-1.3 RMOT-2	Does the device support any mechanism (e.g., digital signatures) intended to ensure data is not modified during transmission? Does the device include multiple sub-components connected by external cables?  REMOTE SERVICE (RMOT)  Remote service refers to all kinds of device maintenance activities performed by a service person via network or other remote connection.  Does the device permit remote service connections for device analysis or repair?  Does the device allow the owner/operator to initiative remote service sessions for device analysis or repair?  Is there an indicator for an enabled and active remote session?  Can patient data be accessed or viewed from the device during the remote session?  Does the device permit or use remote service connections for predictive maintenance data?  Does the device permit or use remote service connections for predictive maintenance data?  Does the device have any other remotely accessible functionality (e.g. software updates, remote training)?  OTHER SECURITY CONSIDERATIONS (OTHR)  NONE  NOTE:  The following data fields are associated with each test on the System: Run Date, Serial Number (of consumable), Lot Number (of co	See Notes No See Notes See Notes See Notes See Notes	Note 58  Note 59  Note 60  Note 61
RMOT-1 RMOT-1.1 RMOT-1.2 RMOT-1.3 RMOT-2	Does the device support any mechanism (e.g., digital signatures) intended to ensure data is not modified during transmission? Does the device include multiple sub-components connected by external cables?  REMOTE SERVICE (RMOT)  Remote service refers to all kinds of device maintenance activities performed by a service person via network or other remote connection.  Does the device permit remote service connections for device analysis or repair?  Does the device allow the owner/operator to initiative remote service sessions for device analysis or repair?  Is there an indicator for an enabled and active remote session?  Can patient data be accessed or viewed from the device during the remote session?  Does the device permit or use remote service connections for predictive maintenance data?  Does the device have any other remotely accessible functionality (e.g. software updates, remote training)?  OTHER SECURITY CONSIDERATIONS (OTHR)  NONE  NOTHER SECURITY CONSIDERATIONS (OTHR)  NONE  The following data fields are associated with each test on the system: Run Date, Serial Number (of consumable), Uperator, Instrument Serial Number, Protocol and Pouch (consumable) Type, and a Sample ID. The "Sample ID" field is a free text field, and bioMérieux issues guidance to use	See Notes No See Notes See Notes See Notes See Notes	Note 58  Note 59  Note 60  Note 61
RMOT-1 RMOT-1.1 RMOT-1.2 RMOT-1.3 RMOT-2	Does the device support any mechanism (e.g., digital signatures) intended to ensure data is not modified during transmission? Does the device include multiple sub-components connected by external cables?  REMOTE SERVICE (RMOT)  Remote service refers to all kinds of device maintenance activities performed by a service person via network or other remote connection.  Does the device permit remote service connections for device analysis or repair?  Is there an indicator for an enabled and active remote service sessions for device analysis or repair?  Is there an indicator for an enabled and active remote session?  Can patient data be accessed or viewed from the device during the remote session?  Does the device permit or use remote service connections for predictive maintenance data?  Does the device permit or use remote service connections for predictive maintenance data?  Does the device have any other remotely accessible functionality (e.g. software updates, remote training)?  OTHER SECURITY CONSIDERATIONS (OTHR)  NONE  Notes:  The following data fields are associated with each test on the System: Run Date, Serial Number (of consumable), Lor Number (of consumable), Upgrator, Instrument Serial Number, Protocol and Pouch (consumable) Type, and a Sample ID. The "Sample ID" field is a free text field, and bioMérieux issues guidance, do not enter "Sample ID" field. Consistent with this guidance, do not enter	See Notes No See Notes See Notes See Notes See Notes	Note 58  Note 59  Note 60  Note 61
RMOT-1 RMOT-1.1 RMOT-1.2 RMOT-1.3 RMOT-2	Does the device support any mechanism (e.g., digital signatures) intended to ensure data is not modified during transmission?  Does the device include multiple sub-components connected by external cables?  REMOTE SERVICE (RMOT)  Remote service refers to all kinds of device maintenance activities performed by a service person via network or other remote connection.  Does the device permit remote service connections for device analysis or repair?  Does the device allow the owner/operator to initiative remote service sessions for device analysis or repair?  Sethere an indicator for an enabled and active remote session?  Can patient data be accessed or viewed from the device during the remote session?  Does the device permit or use remote service connections for predictive maintenance data?  Does the device have any other remotely accessible functionality (e.g. software updates, remote training)?  NOTHER SECURITY CONSIDERATIONS (OTHR)  NONE  Notes:  The following data fields are associated with each test on the system: Run Date, Serial Number (of consumable), Lot Number (of consumable), Operator, Instrument Serial Number, Protocol and Pouch (consumable) Type, and a Sample ID. The "Sample ID" field is a free text field, and blookfreiux 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	See Notes No See Notes See Notes See Notes See Notes	Note 58  Note 59  Note 60  Note 61
RMOT-1 RMOT-1.1 RMOT-1.2 RMOT-1.3 RMOT-2	Does the device support any mechanism (e.g., digital signatures) intended to ensure data is not modified during transmission?  Does the device include multiple sub-components connected by external cables?  REMOTE SERVICE (RMOT)  Remote service refers to all kinds of device maintenance activities performed by a service person via network or other remote connection.  Does the device allow the owner/operator to initiative remote service allow the owner/operator to initiative remote service sessions for device analysis or repair?  Does the device allow the owner/operator to initiative remote service sessions for device analysis or repair?  Is there an indicator for an enabled and active remote session?  Can patient data be accessed or viewed from the device during the remote session?  Does the device permit or use remote service connections for predictive maintenance data?  Does the device permit or use remote service connections for predictive maintenance data?  Does the device have any other remotely accessible functionality (e.g. software updates, remote training)?  OTHER SECURITY CONSIDERATIONS (OTHR)  NONE  Notes:  The following data fields are associated with each test on the System: Run Date, Serial Number (of consumable), Uperator, Instrument Serial Number, Protocol and Pouch (consumable) Type, and a Sample ID. 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	Yes  See Notes  No  See Notes  See Notes  See Notes  See Notes	Note 58  Note 59  Note 60  Note 61
RMOT-1 RMOT-1.1 RMOT-1.2 RMOT-1.3 RMOT-2	Does the device support any mechanism (e.g., digital signatures) intended to ensure data is not modified during transmission?  Does the device include multiple sub-components connected by external cables?  REMOTE SERVICE (RMOT)  Remote service refers to all kinds of device maintenance activities performed by a service person via network or other remote connection.  Does the device permit remote service connections for device analysis or repair?  Does the device allow the owner/operator to initiative remote service sessions for device analysis or repair?  Is there an indicator for an enabled and active remote session?  Can patient data be accessed or viewed from the device during the remote session?  Does the device permit or use remote service connections for predictive maintenance data?  Does the device permit or use remote service connections for predictive maintenance data?  Does the device have any other remotely accessible functionality (e.g. software updates, remote training)?  OTHER SECURITY CONSIDERATIONS (OTHR)  NOVE:  The following data fields are associated with each test on the System: Run Date, Serial Number (of consumable), Lot Number (of consumable), Operator, Instrument Serial Number, Protocol and Pouch (consumable) (ppe, 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,	Yes  See Notes  No  See Notes  See Notes  See Notes  See Notes	Note 58  Note 59  Note 60  Note 61
RMOT-1 RMOT-1.1 RMOT-1.2 RMOT-1.3 RMOT-2	Does the device support any mechanism (e.g., digital signatures) intended to ensure data is not modified during transmission?  Does the device include multiple sub-components connected by external cables?  REMOTE SERVICE (RMOT)  Remote service refers to all kinds of device maintenance activities performed by a service person via network or other remote connection.  Does the device allow the owner/operator to initiative remote service allow the owner/operator to initiative remote service assists or repair?  Does the device allow the owner/operator to initiative remote service sessions for device analysis or repair?  Is there an indicator for an enabled and active remote session?  Can patient data be accessed or viewed from the device during the remote session?  Does the device permit or use remote service connections for predictive maintenance data?  Does the device have any other remotely accessible functionality (e.g. software updates, remote training)?  OTHER SECURITY CONSIDERATIONS (OTHR)  NONE	Yes  See Notes  No  See Notes  See Notes  See Notes	Note 58  Note 59  Note 60  Note 61
RMOT-1 RMOT-1.1 RMOT-1.2 RMOT-1.3 RMOT-2	Does the device support any mechanism (e.g., digital signatures) intended to ensure data is not modified during transmission?  Does the device include multiple sub-components connected by external cables?  REMOTE SERVICE (RMOT)  Remote service refers to all kinds of device maintenance activities performed by a service person via network or other remote connection.  Does the device permit remote service connections for device analysis or repair?  Does the device allow the owner/operator to initiative remote service sessions for device analysis or repair?  Is there an indicator for an enabled and active remote session?  Can patient data be accessed or viewed from the device during the remote session?  Does the device permit or use remote service connections for predictive maintenance data?  Does the device permit or use remote service connections for predictive maintenance data?  Does the device have any other remotely accessible functionality (e.g. software updates, remote training)?  OTHER SECURITY CONSIDERATIONS (OTHR)  NOVE:  The following data fields are associated with each test on the System: Run Date, Serial Number (of consumable), Lot Number (of consumable), Operator, Instrument Serial Number, Protocol and Pouch (consumable), Use Number (of consumable), Operator, Instrument Serial Number, Protocol and Pouch (consumable), Use Number (ifield 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 "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	Yes  See Notes  No  See Notes  See Notes  See Notes	Note 58  Note 59  Note 60  Note 61
RMOT-1 RMOT-1.1 RMOT-1.2 RMOT-1.3 RMOT-2	Does the device support any mechanism (e.g., digital signatures) intended to ensure data is not modified during transmission?  Does the device include multiple sub-components connected by external cables?  REMOTE SERVICE (RMOT)  Remote service refers to all kinds of device maintenance activities performed by a service person via network or other remote connection.  Does the device permit remote service connections for device analysis or repair?  Does the device allow the owner/operator to initiative remote service sessions for device analysis or repair?  Does the device allow the owner/operator to initiative remote service sessions for device analysis or repair?  Does the device allow the owner/operator to device during the remote session?  Can patient data be accessed or viewed from the device during the remote session?  Does the device permit or use remote service connections for predictive maintenance data?  Does the device have any other remotely accessible functionality (e.g. software updates, remote training)?  OTHER SECURITY CONSIDERATIONS (OTHR)  NONE  The following data fields are associated with each test on the System: Run Date, Serial Number (of consumable), to Number (of consumable), Operator, instrument Serial Number, Protocol and Pouch (consumable) 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 displayed and stored on the System. As an optional feature, the System may be configured to	Yes  See Notes  No  See Notes  See Notes  See Notes	Note 58  Note 59  Note 60  Note 61
RMOT-1 RMOT-1.1 RMOT-1.2 RMOT-1.3 RMOT-2	Does the device support any mechanism (e.g., digital signatures) intended to ensure data is not modified during transmission?  Does the device include multiple sub-components connected by external cables?  REMOTE SERVICE (RMOT)  Remote service refers to all kinds of device maintenance activities performed by a service person via network or other remote connection.  Does the device permit remote service connections for device analysis or repair?  Does the device allow the owner/operator to initiative remote service sessions for device analysis or repair?  Is there an indicator for an enabled and active remote session?  Can patient data be accessed or viewed from the device during the remote session?  Does the device permit or use remote service connections for predictive maintenance data?  Does the device have any other remotely accessible functionality (e.g. software updates, remote training)?  OTHER SECURITY CONSIDERATIONS (OTHR)  NONE  Notes:  The following data fields are associated with each test on the System: Run Date, Serial Number (of consumable), Operator, Instrument Serial Number, Protocol and Pouch (consumable) (appearor, Instrument Serial Number, Protocol and Pouch (consumable) and pouch (consumable) (perator, instrument Serial Number, Protocol and Pouch (consumable) and pouch (consumable) (perator, instrument Serial Number, Protocol and Pouch (consumable) (perator, instrument Serial Number, Protocol and Pouch (consumable) (perator, instrument Serial Number, Protocol 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 is a free text field, and sidnay and sample for or other patient names, addresses, demographic information, financial information, is displayed and stored on the System.	Yes  See Notes  No  See Notes  See Notes  See Notes	Note 58  Note 59  Note 60  Note 61
RMOT-1 RMOT-1.1 RMOT-1.2 RMOT-1.3 RMOT-2	Does the device support any mechanism (e.g., digital signatures) intended to ensure data is not modified during transmission?  Does the device include multiple sub-components connected by external cables?  REMOTE SERVICE (RMOT)  Remote service refers to all kinds of device maintenance activities performed by a service person via network or other remote connection.  Does the device permit remote service connections for device analysis or repair?  Does the device allow the owner/operator to initiative remote service sessions for device analysis or repair?  Does the device allow the owner/operator to initiative remote service sessions for device analysis or repair?  Does the device allow the owner/operator to device during the remote session?  Can patient data be accessed or viewed from the device during the remote session?  Does the device permit or use remote service connections for predictive maintenance data?  Does the device have any other remotely accessible functionality (e.g. software updates, remote training)?  OTHER SECURITY CONSIDERATIONS (OTHR)  NONE  The following data fields are associated with each test on the System: Run Date, Serial Number (of consumable), to Number (of consumable), Operator, instrument Serial Number, Protocol and Pouch (consumable) 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 displayed and stored on the System. As an optional feature, the System may be configured to	Yes  See Notes  No  See Notes  See Notes  See Notes	Note 58  Note 59  Note 60  Note 61
RMOT-1 RMOT-1.1 RMOT-1.2 RMOT-1.3 RMOT-2	Does the device support any mechanism (e.g., digital signatures) intended to ensure data is not modified during transmission?  Does the device include multiple sub-components connected by external cables?  REMOTE SERVICE (RMOT)  Remote service refers to all kinds of device maintenance activities performed by a service person via network or other remote connection.  Does the device permit remote service connections for device analysis or repair?  Does the device allow the owner/operator to initiative remote service sessions for device analysis or repair?  Does the device allow the owner/operator to initiative remote service sessions for device analysis or repair?  Does the device allow the owner/operator to device during the remote session?  Can patient data be accessed or viewed from the device during the remote session?  Does the device permit or use remote service connections for predictive maintenance data?  Does the device have any other remotely accessible functionality (e.g. software updates, remote training)?  OTHER SECURITY CONSIDERATIONS (OTHR)  NONE  The following data fields are associated with each test on the System: Run Date, Serial Number (of consumable), to Number (of consumable), Operator, instrument Serial Number, Protocol and Pouch (consumable) 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 displayed and stored on the System. As an optional feature, the System may be configured to	Yes  See Notes  No  See Notes  See Notes  See Notes	Note 58  Note 59  Note 60  Note 61
TXIG-2  RMOT-1  RMOT-1.1  RMOT-1.2  RMOT-1.3  RMOT-2	Does the device support any mechanism (e.g., digital signatures) intended to ensure data is not modified during transmission?  Does the device include multiple sub-components connected by external cables?  REMOTE SERVICE (RMOT)  Remote service refers to all kinds of device maintenance activities performed by a service person via network or other remote connection.  Does the device permit remote service connections for device analysis or repair?  Does the device allow the owner/operator to initiative remote service sessions for device analysis or repair?  Does the device allow the owner/operator to initiative remote service sessions for device analysis or repair?  Does the device allow the owner/operator to device during the remote session?  Can patient data be accessed or viewed from the device during the remote session?  Does the device permit or use remote service connections for predictive maintenance data?  Does the device have any other remotely accessible functionality (e.g. software updates, remote training)?  OTHER SECURITY CONSIDERATIONS (OTHR)  NONE  The following data fields are associated with each test on the System: Run Date, Serial Number (of consumable), to Number (of consumable), Operator, instrument Serial Number, Protocol and Pouch (consumable) 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 displayed and stored on the System. As an optional feature, the System may be configured to	Yes  See Notes  No  See Notes  See Notes  See Notes	Note 58  Note 59  Note 60  Note 61

Transfer Responses, ILC  The following single for the content of t				
Squares and the control formation of constrainting is the Number Information of the Constrainting Constraints of the Constrainting Constraints of the Constrainting Constraints of the Constraint in Constraints of the Constra	BioFire Diagnostics, LLC	BIOFIRE® FILMARRAY® 2.0 SYSTEM	FLM2-PRT-0268-07	11-Jul-2023
The following data fields are associated with each test on the System: Man Date, Senial Number of Consumability, Use Mumber (or Consumability, Use Number) (or Consumability) (or Consumabil		System: Run Date, Serial Number (of consumable), Lot Number (of consumable), Operator, Instrument Serial Number, Protocol and Pouch (consumable) 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		
The following data fields are associated with each test on the System: Man Date, Senial Number of Consumability, Use Mumber (or Consumability, Use Number) (or Consumability) (or Consumabil	Note 2			
The following data fields are associated with each test on the System: Run Date, Serial Number (or commanble), Operator, Instrument Serial Number (or Commanble) (or Berlin State) (or		System: Run Date, Serial Number (of consumable), Lot Number (of consumable), Operator, Instrument Serial Number, Protocol and Pouch (consumable) 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		
The following data fields are associated with each test on the System: Run Date, Serial Number (or commable), Operator, Instrument Serial Number (or Commable) (or Gonzella) (				
The following data fields are associated with each test on the System: Run Date, Serial Number (of consumable), Lot Number (of consumable), Operator, Instrument Serial Number, Protocol and Pouch (consumable) 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: Run Date, Serial Number (of consumable), Lot Number (of consumable), Operator, Instrument Serial Number, Protocol and Pouch (consumable) 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 non-		
System: Run Date, Serial Number (of consumable), Lot Number (of consumable), Operator, Instrument Serial Number, Protocol and Pouch (consumable) 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	Note 4			
Note 5		System: Run Date, Serial Number (of consumable), Lot Number (of consumable), Operator, Instrument Serial Number, Protocol and Pouch (consumable) 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		

Page 9

BioFire Diagnostics, LLC	BIOFIRE® FILMARRAY® 2.0 SYSTEM	FLM2-PRT-0268-07	11-Jul-2023
Significants, LLC			11 701-2023
	The following data fields are associated with each test on the System: Run Date, Serial Number (of consumable), Lot Number (of consumable), Operator, Instrument Serial Number, Protocol and Pouch (consumable) 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, inancial 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 ANS/NEMA HN 1-2019, the System does have mechanisms used for transmitting and importing/exporting such information.		
Note 10	The following data fields are associated with each test on the		
	system: Run Date, Serial Number (of consumable), Lot Number (of consumable), Operator, Instrument Serial Number, Protocol and Pouch (consumable) 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 displayed by the System.		
Note 11	The following data fields are associated with each test on the		
	System: Run Date, Serial Number (of consumable), Lot Number (of consumable), Operator, Instrument Serial Number, Protocol and Pouch (consumable) 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 12	The following data fields are associated with each test on the		
	Ine following data lielos are associated with each test on the System: Run Date, Serial Number (of consumable), Lot Number (of consumable), Operator, Instrument Serial Number, Protocol and Pouch (consumable) Type, and a Sample ID. The "Sample IO" field is a free text field, and bioMérieux issues guidance to use sequentially generated recycled accession numbers in the "Sample IO" 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 ANS/NEMA HN 1-2019, such information may be retrieved from or recorded to		
Note 13	removable media.		
==	•		1

BioFire Diagnostics, LLC	BIOFIRE® FILMARRAY® 2.0 SYSTEM	FLM2-PRT-0268-07	11-Jul-2023
	The following data fields are associated with each test on the System: Run Date, Serial Number (of consumable), Lot Number (of consumable), Operator, Instrument Serial Number Protocol and Pouch (consumable) 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 14			
	The following data fields are associated with each test on the System: Run Date, Serial Number (of consumable), Lot Number (of consumable), Operator, Instrument Serial Number, Protocol and Pouch (consumable) 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 via a wired network connection.		
Note 15	The following data fields are associated with each test on the		
	System: Run Date, Serial Number (of consumable), Lot Number (of consumable), Operator, Instrument Serial Number, Protocol and Pouch (consumable) 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 16	The System is pre-configured to log on to Windows using the FilmArray user account automatically. The FilmArray 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.		
Note 17			
Note 18	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 allows API interface but the user has to interact to complete the processes presented.		
Note 19	Instructions for the owner/operator installation of Operating System patches are within BFR0001-6037 Microsoft OS Patch Policy Tech Note and BFR0002-4468 System Update Microsoft Patch Policy Tech Note.		

BioFire Diagnostics, LLC	BIOFIRE® FILMARRAY® 2.0 SYSTEM	FLM2-PRT-0268-07	11-Jul-2023
	Manual instructions for the owner/operator installation of		
	Operating System patches are within BFR0001-6037 Microsoft		
	OS Patch Policy Tech Note and BFR0002-4468 System Update Microsoft Patch Policy Tech Note. If optional connectivity		
	features are enabled, the System has the capability to receive remote installation of patches or software updates.		
	Terrote installation of patches of software updates.		
Note 21			
	The recommended installation process for updates from third party manufactures (e.g. Microsoft) is available within BFR0001-		
	6037 Microsoft OS Patch Policy Tech Note and BFR0002-4468		
	System Update Microsoft Patch Policy Tech Note.		
Note 22	Documentation for Driver and Firmware patches or updates, if		
	required, will be distributed by bioMérieux BIOFIRE Technical		
Note 23	Support team.		
	Vendor authorized service is required for most firmware updates. Driver update or patches may be installed by the		
	owner/operator.		
Note 24			
	The recommended installation process for updates from third party manufactures (e.g. Microsoft) is available within BFR0001-		
	6037 Microsoft OS Patch Policy Tech Note and BFR0002-4468 System Update Microsoft Patch Policy Tech Note.		
Note 25	,		
Note 23	Instructions for the owner/operator installation of Anti-Malware		
	Software patches are within BFR0001-6037 Microsoft OS Patch Policy Tech Note and BFR0002-4468 System Update Microsoft		
	Patch Policy Tech Note.		
Note 26			
	The recommended installation process for updates from third party manufactures (e.g. Microsoft) is available within BFR0001-		
	6037 Microsoft OS Patch Policy Tech Note and BFR0002-4468 System Update Microsoft Patch Policy Tech Note.		
	system opaute microsoft attain only reconside.		
Note 27			
	If optional connectivity features are enabled, the System has the capability to receive remote installation of patches or software		
	updates for Non-Operating System commercial off-the-shelf		
	components.		
Note 28	If the optional interface with an Institution-specific cloud-based		
	data management portal is 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 29	The following data fields are associated with each test on the		
	System: Run Date, Serial Number (of consumable), Lot Number		
	(of consumable), Operator, Instrument Serial Number, Protocol and Pouch (consumable) 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 30			
	The System is not intended to maintain long term primary storage of data. See the System Operator's Manual for data		
	archiving guidance.		
Note 31	If a Custom is holioused to be imposted by		
	If a System is believed to be impacted by malware, please contact the BIOFIRE Technical Support team for assistance.		
Note 32			
	Operating system and security event auditing utilizes Windows		
Note 33	logging features.		
	Installation and maintenance of antivirus, intrusion detection, and other detection/prevention systems is the responsibility of		
	the end user.		
Note 34			
Note 34	If the System is configured with optional connectivity features,		
	node authentication may be utilized.		
Note 35	If the System is configured with optional connectivity features,		
	certificate-based network connection authentication may be utilized.		
Note 36	denzeo.		
	'		

Response to the Scholars Opportune - Nava Date of Control Control Response to the Scholars Opportune - Nava Date of Control Response to the Scholars Opportune - Nava Date of Control Response to the Scholars - Nava Date of	BioFire Diagnostics, LLC	BIOFIRE® FILMARRAY® 2.0 SYSTEM	FLM2-PRT-0268-07	11-Jul-2023
Minister B. Marieran in Projection (Proposed's Absoration desiration in the Marieran in Projection (Proposed's Absoration desiration in the Marieran in Marieran in Projection (Proposed's Marieran in		Reference the 2.0 Operator's Manual for the System's hardware		
Section on Program Cycles and Control on Program Cycles and Control on Control  And Section as the State of Control on Control  And Section as the State of Control on Control  And Section as the State of Control on Control  And Section as the State of Control on Control  And Section as the State of Control on Control  And Section as the State of Control on Control  And Section as the State of Control on Control  And Section as the State of Control on Control  And Section as the State of Control on Control  And Section as the State of Control on Control  And Section as the State of Control on Control  And Section as the State of Control on Control  And Section as the State of Control on Control  And Section as the State of Control on Control  And Section as the State of Control  And Section as the State of Control  And Section as the State of Control on Control  And Section as the State of Control  And Section as the State of Control on Control  And Section as the State of Con				
The set of the control of the contro	Note 37			
Inflation with the Spears of Spears and Production Spears and Spears of	Note 38			
Table 25  Table 25  Table 26  Table 26  Table 27  Table 26  Table 27  Table 26  Table 27  Table 27  Table 27  Table 27  Table 28  Table 28  Table 28  Table 29  Table		Reference the System Operator's Manual for details on the		
Section 1  Section 1  Section 2  Section 2  Section 2  Section 3	Note 39			
1956 40 concentration of southern and search and popular in the concentration of southern and search and searc				
state of extending to the continue of the cont	Note 40	environment.		
1966 43 Provinced Control of System may be a special of the Sy				
Index 42 Index of recision APT calls.  The system investment is described computer with internal hard with referred hard with r	Note 41	environment.		
The type and includes a decision compact with internal value of the compact of th	Note 42			
International contraction of the System's applicate protecting international internati		The System includes a desktop computer with internal hard		
Identification information of the System malatines pressuring seatesting with the System seatesting				
Iz be elevent fur the the System munitation personality desired indicated information in the immediate in physical years, the in ord elevent in the control of the control				
Information, such information physically secure, but in otol behand on methods in femotional physically secure, but in otol behand on methods in femotional physically secure plants particle for methods from the physical plants on the physical plants of	Note 43	The state of the s		
additional information or the flycative sality to creatable parts and the flycative sality to creatable parts and the flycative sality to creatable parts and the flycative sality salit				
decirable information				
The software was developed in accordance with EC (2014).  Output Processor of Windows Capacity (1994).  Output Processor of Windows Capacity (1994).  Note 40.  The Microsoft Windows Capacity (1994).  Note 40.  The Microsoft Windows Capacity (1994).  Note 40.  If you have any questions or concerns about the promote that are enabled on the system is available upon request.  Note 40.  If you have any questions or concerns about 1995 (1994).  Note 40.  If you have any questions or concerns about 1995 (1994).  Note 40.  If you have any questions or concerns about 1995 (1994).  Note 40.  If you have any questions or concerns about 1995 (1994).  Note 40.  If you have any questions or concerns about 1995 (1994).  Note 40.  If you have any questions or concerns about 1995 (1994).  Note 50.  Support team for autoissance.  Department of petitions also places concerns about 1995 (1994).  Note 51.  Output petitions of the systems of the Systems Androne (1994).  Note 51.  Output petitions of the systems of the Systems Androne (1994).  Note 52.  Output petitions of the systems of the				
Note 50  Casility Assurance processes conducted during the System's assurable ensure the Installed software is remarkative.  The Microsoft Workshow Operating System Towards account is capable on the System and protection that are enabled on the System as available equity respect.  As let of communication ports and protection that are enabled on the System as available upon respect.  As let of communication ports and protection that are enabled on the System as available upon respect.  As let of communication ports and protection that are enabled on the System as available upon respect.  As of port have any exercision or concerns about system hardware, beyond the default state, please context the third DRIPE Technical species of the default state, please context the third DRIPE Technical species of the default state, please context the third DRIPE Technical species of the default state, please context the third DRIPE Technical species of the default state, please context the third protection of the default state, please context the third protection of the post of the default state, please context the third protection of the post of the post of the default state, please context the third protection of the post of the default state, please context the third protection of the post of t	Note 44			
Clausin Assurance processes conducted during the hyperin's assembly personner in manufactures.  Note: 4.7  Clausine St. 1	Note 45	ine soπware was developed in accordance with IEC 62304.		
Note 45 admired by defeated.  Note 47 admired by defeated.  Note 48 admired by defeated.  Note 48 admired by defeated.  Note 49 admired by defeated by defeated by the season of the posterior of the season of the posterior by defeated by the season of the posterior by defeated by defeated by the season of the posterior by defeated by defeated by the season of the posterior by defeated by defeat				
Indicated by default.  All sof communication ports and prosocios that are enabled on the System's available upon request.  Note 48  If you have any question or concerns about system hardening beyond the default state, places contact the BOPRE recinical places.  Note 49  If you have any question or concerns about system hardening beyond the default state, places contact the BOPRE recinical places.  Note 50  Support team for availation.  Department of Defenses's Security Technical implementation Guides have been used to harden the Microsoft Windows  Support team for availation.  Department of Defenses's Security Technical implementation Guides have been used to harden the Microsoft Windows  Support team for availation.  Department of Defenses's Security Technical implementation Guides have been used to harden the Microsoft Windows  Support team for availation.  Department of Defenses's Security Technical implementation Guides have been used to harden the Microsoft Windows  Support team for availation.  Department of Defenses's Security Technical implementation Guides have been used to harden the Microsoft Windows  Support team for available to the Microsoft Windows  Support team for available to the Confederation of the Microsoft Windows  Department of the Confederation of the Microsoft Windows  Support team for the Confederation of	Note 46	authorized.		
A last of communicacy periods and protocols that are enabled on the System is available upon request.  Note 48  If you have any questions or concerns about system hardering beyond the default state, please contact the silvoller Technical Mode 59  If you have any questions or concerns about system hardering beyond the default state, please contact the silvoller Technical Sopport state and parallel so or concerns about system hardering beyond the default state, please contact the silvoller Technical Sopport state of a sostance.  Department of Defaults Security Technical Implementation Sought Security Security Technical Implementation Sought Security Security Technical Implementation Sought Security	Note 47			
Note 48  If you have any questions or concerns about system hardening beyond the default state, please contact the BOPRE Technical Support team for assistance.  If you have any questions or concerns about system hardening beyond the default state, please contact the BOPRE Technical Support team for assistance.  If you have any questions or concerns about system hardening beyond the default state, please contact the BOPRE Technical Supports and the state of	Note 47	A list of communication ports and protocols that are enabled on		
If you have any questions or concerns about system hardening beyond the default state, please contact the BIORIE Technical Support team for assistance.  If you have any questions or concerns about system hardening beyond the default state, please contact the BIORIE Technical Desauth of the State of Support team of a sistance.  Note 50  Operating System.  Obta protection mechanisms is place on the system induse password precision of the contact the Microrott Windows Operating System.  Obta protection mechanisms is place on the system induse password precision of the local database, annomination of the run data when exporting anonymously, and data burdle assword prefix of the local database, and the system of the run data when exporting anonymously, and data burdle database.  Note 52  If the System's optional connectivity features are enabled, data may be stored in an external database.  Note 54  If the System's optional connectivity features are enabled, the connections may or to be entrypted prior to transmission.  Note 55  If the System's optional connectivity features are enabled, the connections may or may be supported implemented.  If the System's optional connectivity features are enabled, the connections may or may be supported implemented.  If the System's optional connectivity features are enabled, the connections may or may be supported implemented.  If the System's optional connectivity features are enabled and a remote session is connections. If the System's optional connectivity features are enabled and a remote session is connections. The System's optional connectivity features are enabled and the centre of analysis or repair.  Note 59  If the System's optional connectivity features are enabled and the central patient data may be on the System, through a central search of a may be considered to enable and to the central patient data may be on the System, through a central patient data may		the System is available upon request.		
Seyond the default state, please contact the BIORIET rechnical  If you have any questions or concerns about system hardening beyond the default state, please contact the BIORIET rechnical beyond the default state, please contact the BIORIET rechnical beyond the default state, please contact the BIORIET rechnical Department of Defames Security Fechical implementation Open state of Default state, please contact the BIORIET rechnical Open state of Default state, please contact the BIORIET rechnical Open state of Default state, please contact the BIORIET rechnical Open state of Default state, please contact the BIORIET rechnical Open state of Default state, please contact the BIORIET rechnical Open state of Default state, please contact the BIORIET rechnical Open state of Default state, please contact the BIORIET rechnical Open state of Default state, please contact the BIORIET rechnical Open state of Default state, please contact the BIORIET rechnical Open state of Default state, please contact the BIORIET rechnical Open state of Default state, please contact the BIORIET rechnical Open state of Default state, please contact the BIORIET rechnical Open state of Default state, please contact the BIORIET rechnical Open state of Default state, please contact the BIORIET rechnical Open state of Default state, please state of Default sta	Note 48	If you have any questions or concerns about system hardening		
If you have any questions or concerns about system hardening beyond the default state, please contact the Biolified Technical support team for assistance.  Department of Defense's Security Technical implementation dualets have been used to harden the Micropolif Windows Outset Sa.  Despartment of Defense's Security Technical implementation dualets have been used to harden the Micropolif Windows Despartment of Defense's Security Technical implementation dualets have been used to harden the Micropolif Windows Outset Sa.  Note Sa.  Outse for Security of the Security Security of the Security Security of the United Security of the United Security Security of the United Security Security of the United Security Security of the Security Sec		beyond the default state, please contact the BIOFIRE Technical		
beyond the default state, please contact the BIORIET Technical Support term for assistance.  Department of Defenes's Security Technical Implementation (Sudies have been used to have the Microsoft Windows (Sudies have been used to have the Microsoft Windows (Sudies have been used to have the Microsoft Windows (Sudies have been used to have the Microsoft Windows (Sudies have been used to have the Microsoft Windows (Sudies have been used to ha	Note 49			
Department of Defense's Security Technical Implementation Guides have been used to harden the Microsoft Windows Operating System.  Data protection mechanisms in place on the system include password protection of the local databases, anonymization of the run data where exporting anonymously, and data bundle  In the System's optional connectivity features are enabled, data may be stored in an external database.  Note 53  Data is encrypted prior to transmission via removable media. If the System's optional connectivity features are enabled, that may be may not be encrypted prior to transmission.  Note 54  If the System's optional connectivity features are enabled, the connections may not be immedial patients.  If the System's optional connectivity features are enabled, the connections may not be immedial or seemabled, the connections may not be immedial or seemabled, secure transmission methods may be supported/implemented.  If the System's optional connectivity features are enabled, the System supports mechanisms intended to resize data is not modified during transmission.  Note 57  The System's optional connectivity features are enabled, the System supports mechanisms intended to resize or data is not modified during transmission.  Note 57  The System's intended use does not require nor permit remote service connections. If the System optional connectivity features are enabled, the System optional connectivity features are enabled, the System optional connectivity features are enabled on the connections features are enabled and a remote session is active, there is an indicator.  Note 59  If the System's optional connectivity features are enabled and to the extent patient data may be on the System, it may be accessed or viewed during the remote service connections for analysis or repair.  If the System's optional connectivity features are enabled, the years is secured to viewed during the remote service connections for analysis or repair.  If the System's optional connectivity features are enabled, the years is s		beyond the default state, please contact the BIOFIRE Technical		
Guides have been used to harden the Microsoft Windows	Note 50			
Outs protection mechanisms in place on the system include password protection of the local databases, anonymization of the run data when exporting anonymously, and data bundle creation.  If the System's optional connectivity features are enabled, data may be stored in an external database.  Note 53  Outs is encrypted prior to transmission via removable media. If the System's optional connectivity features are enabled, data may or may not be encrypted prior to transmission.  If the System's optional connectivity features are enabled, the connections may not be encrypted prior to transmission.  If the System's optional connectivity features are enabled, the connections may not be encrypted prior to transmission.  Note 55  If the System's optional connectivity features are enabled, the secure transmission methods may be supported/implemented.  Note 56  If the System's optional connectivity features are enabled, the System's aptional connectivity features are enabled and a remove excess of a subject of repair.  Note 57  The System's intended use does not require nor permit remote service connections if the System's optional connectivity features are enabled and a remove excess of a subject to the service data of the extent patient data may be on the System's in the soft patient and the extent patient data may be on the System's in it may be on the System's in the soft patient data of the extent patient data may be on the System's in it may be used for predictive maintenance data.  If the System's optional connectivity features are enabled, other remote service to excess the provided of predictive maintenance data.		Guides have been used to harden the Microsoft Windows		
the run data when exporting anonymously, and data bundle creation.  If the System's optional connectivity features are enabled, data may be stored in an external database.  Note 53  Data is encrypted prior to transmission via removable media. If the System's optional connectivity features are enabled, data may or may not be encrypted prior to transmission.  Note 54  If the System's optional connectivity features are enabled, the connections may not be immission.  If the System's optional connectivity features are enabled, the connections may not be limited to authenticated systems.  Note 55  If the System's optional connectivity features are enabled, secure transmission methods may be supported/implemented.  Note 56  If the System's optional connectivity features are enabled, the System supports mechanisms interiored to ensure data is not modified during transmission.  Note 57  The System's intended use does not require nor permit remote service connections. If the System syptem are enabled, the System may permit remote service connections of analysis or regain.  Note 58  If the System's optional connectivity features are enabled and a emote service connections for analysis or regain.  Note 59  If the System's optional connectivity features are enabled and a emote service shows the extent patient data may be on the System, it may be a accessed or viewed during the remote session.  Note 50  If the System's optional connectivity features are enabled and the extent patient data may be on the System, it may be a accessed or viewed during the remote session.  Note 60  If the System's optional connectivity features are enabled, the system's remote service connections may be used for predictive maintenance data.  If the System's optional connectivity features are enabled, other emotely accessible functionally may be included.  Occumentation for features are not provided	Note 51			
Note 52 cration.  If the System's optional connectivity features are enabled, data may be stored in an external database.  Note 53  Data is encrypted prior to transmission was removable media. If the System's optional connectivity features are enabled, data may or may not be encrypted prior to transmission.  Note 54  If the System's optional connectivity features are enabled, the connections may not be limited to authenticated systems.  Note 55  If the System's optional connectivity features are enabled, descure transmission methods may be supported/implemented.  Note 56  If the System's optional connectivity features are enabled, the System may permit remote service connections if the System's optional connectivity features are enabled and a remote session is active, there is an indicator.  Note 59  If the System's optional connectivity features are enabled and to the extent painted data may be on the System's microse review connections. If the System's optional connectivity features are enabled, the Psystem's optional connectivity features are enabled, t				
may be stored in an external database.  Data is encrypted prior to transmission via removable media. If the System's optional connectivity features are enabled, data may or may not be encrypted prior to transmission.  Note 54  If the System's optional connectivity features are enabled, the connections may not be limited to authenticated systems.  Note 55  If the System's optional connectivity features are enabled, secure transmission methods may be supported/implemented.  Note 56  If the System's optional connectivity features are enabled, the System's optional connectivity features of modified during transmission.  Note 57  The System's intended use does not require nor permit remote service connections. If the System's optional connectivity features are enabled the System's optional connectivity features are enabled and a remote service connections for analysis or repair.  Note 58  If the System's optional connectivity features are enabled and a remote service connections for analysis or repair.  Note 59  If the System's optional connectivity features are enabled and to the extent patient data may be on the System, it may be a crossed or viewed during the remote session.  Note 60  If the System's optional connectivity features are enabled, the System's optional connectivity features are enabled, the System's spotional connectivity features are enabled, the System's spotional connectivity features are enabled, the System's optional connectivity features are enabled, the System's spotional connectivity features are enabled, other remotely accessible functionality may be included.  Documentation for Remote Service features are benyteded	Note 52			
Data is encrypted prior to transmission via removable media. If the System's optional connectivity features are enabled, data may or may not be encrypted prior to transmission.  Note 54  If the System's optional connectivity features are enabled, the connections may not be limited to authenticated systems.  Note 55  If the System's optional connectivity features are enabled, the connections may not be limited to authenticated systems.  Note 56  If the System's optional connectivity features are enabled, the System supports mechanisms intended to ensure data is not modified during transmission.  Note 57  The System's intended use does not require nor permit remote service connections. If the System may permit remote service connections. If the System may permit remote service connections for analysio or repair.  Note 58  If the System's optional connectivity features are enabled and a remote session is active, there is an indicator.  Note 59  If the System's optional connectivity features are enabled and to the extent patent data may be on the System, it may be accessed or viewed during the remote session.  Note 60  If the System's optional connectivity features are enabled, other remotely accessible functionality may be included. Documentation for Remote Sexifice Residues can be provided				
the System's optional connectivity features are enabled, data may or may not be encrypted prior to transmission.  Note 54  If the System's optional connectivity features are enabled, the connections may not be limited to authenticated systems.  If the System's optional connectivity features are enabled, secure transmission methods may be supported/implemented.  Note 56  If the System's optional connectivity features are enabled, the System supports mechanisms intended to ensure data is not modified during transmission.  Note 57  The System's intended use does not require nor permit remote service connections. If the System's optional connectivity features are enabled and a remote service connections for analysis or repair.  Note 58  If the System's optional connectivity features are enabled and a remote session is active, there is an indicator.  Note 59  If the System's optional connectivity features are enabled and to the extent patient data may be on the System, it may be accessed or viewed during the remote session.  Note 60  If the System's optional connectivity features are enabled, the System's optional connectivity features are enabled, the System's optional connectivity features are enabled, the System's optional connectivity features are enabled and to the extent patient data may be on the System, it may be accessed or viewed during the remote session.  Note 60  If the System's optional connectivity features are enabled, the System's remote service connections may be used for predictive maintenance data.  If the System's optional connectivity features are enabled, other remote spaces of the functionally may be included.  Documentation for Remote Service features can be provided	Note 53			
may or may not be encrypted prior to transmission.  If the System's optional connectivity features are enabled, the connections may not be limited to authenticated systems.  If the System's optional connectivity features are enabled, secure transmission methods may be supported/implemented.  Note 56  If the System's optional connectivity features are enabled, the System supports mechanisms intended to ensure data is not modified during transmission.  Note 57  The System's intended use does not require nor permit remote service connections if the System's optional connectivity features are enabled, the System say permit remote service connections if the System's optional connectivity features are enabled, the System's optional connectivity features are enabled and a remote session is active, there is an indicator.  Note 59  If the System's optional connectivity features are enabled and to the extent patient data may be on the System, it may be accessed or viewed during the remote session.  Note 60  If the System's optional connectivity features are enabled, the System's remote service connections may be used for predictive maintenance data.  If the System's optional connectivity features are enabled, other remotely accessible functionality may be included.  Documentation for Remote Service deatures can be provided  Documentation for Remote Service deatures can be provided				
If the System's optional connectivity features are enabled, the connections may not be limited to authenticated system.  Note 56  If the System's optional connectivity features are enabled, secure transmission methods may be supported/implemented.  Source for many the supports mechanisms intended to ensure data is not modified during transmission.  Note 57  The System's intended use does not require nor permit remote service connections. If the System's optional connectivity features are enabled, the System's optional connectivity features are enabled, the System's optional connectivity features are enabled, and so the System and permit remote service connections for analysis or repair.  Note 58  If the System's optional connectivity features are enabled and a remote session is active, there is an indicator.  Note 59  If the System's optional connectivity features are enabled and to the extent patient data may be on the System, it may be accessed or viewed during the remote session.  Note 60  If the System's optional connectivity features are enabled, the System's remote session or view of the system's optional connectivity features are enabled, the System's remote session for Remote Service features can be provided				
connections may not be limited to authenticated systems.  If the System's optional connectivity features are enabled, secure transmission methods may be supported/implemented.  Note 56  If the System's optional connectivity features are enabled, the System supports mechanisms intended to ensure data is not modified during transmission.  Note 57  The System's intended use does not require nor permit remote service connections. If the System's optional connectivity features are enabled, the System's optional connectivity features are enabled, the System's optional connectivity features are enabled and a remote service connections is active, there is an indicator.  If the System's optional connectivity features are enabled and to the extent patient data may be on the System, it may be accessed or viewed during the remote service.  Note 60  If the System's optional connectivity features are enabled, other remotely accessible functionality may be included.  Documentation for Remote Service features can be provided	Note 54	If the System's optional connectivity features are enabled, the		
If the System's optional connectivity features are enabled, secure transmission methods may be supported/implemented.  Note 57  The System's optional connectivity features are enabled, the System supports mechanisms intended to ensure data is not modified during transmission.  Note 57  The System's intended use does not require nor permit remote service connections. If the System's optional connectivity features are enabled, the System may permit remote service connections for analysis or repair.  Note 58  If the System's optional connectivity features are enabled and a remote session is a citive, there is an indicator.  Note 59  If the System's optional connectivity features are enabled and to the extent patient data may be on the System, it may be accessed or viewed during the remote session.  Note 60  If the System's optional connectivity features are enabled, the System's remote service connections may be used for predictive maintenance data.  If the System's optional connectivity features are enabled, the System's remote service connections may be used for predictive maintenance data.  If the System's optional connectivity features are enabled, other remotely accessible functionality may be included.  Documentation for Remote Service features can be provided	Nete FF			
secure transmission methods may be supported/implemented.  If the System's optional connectivity features are enabled, the System supports mechanisms intended to ensure data is not modified during transmission.  Note 57  The System's intended use does not require nor permit remote service connections. If the System's optional connectivity features are enabled, the System's optional connectivity features are enabled, the System's optional connectivity features are enabled and a remote session is active, there is an indicator.  Note 59  If the System's optional connectivity features are enabled and to the extent patient data may be on the System, it may be accessed or viewed during the remote session.  Note 60  If the System's optional connectivity features are enabled, the System's remote service connections may be used for predictive maintenance data.  If the System's optional connectivity features are enabled, the System's remote service connections may be used for predictive maintenance data.  If the System's optional connectivity features are enabled, other remotely accessible functionality may be included.  Documentation for Remote Service features can be provided	Note 55	If the System's optional connectivity features are enabled,		
If the System's optional connectivity features are enabled, the System supports mechanisms intended to ensure data is not modified during transmission.  Note 57  The System's intended use does not require nor permit remote service connections. If the System supports mechanisms optional connectivity features are enabled, the System may permit remote service connections for analysis or repair.  Note 58  If the System's optional connectivity features are enabled and a remote session is active, there is an indicator.  Note 59  If the System's optional connectivity features are enabled and to the extent patient data may be on the System, it may be accessed or viewed during the remote session.  Note 60  If the System's optional connectivity features are enabled, the System's remote service connections may be used for predictive maintenance data.  If the System's optional connectivity features are enabled, other remotely accessible functionality may be included.  Documentation for Remote Service described included.	Note 56	secure transmission methods may be supported/implemented.		
modified during transmission.  The System's intended use does not require nor permit remote service connections. If the System's optional connectivity features are enabled, the System may permit remote service connections for analysis or repair.  Note 58  If the System's optional connectivity features are enabled and a remote session is active, there is an indicator.  Note 59  If the System's optional connectivity features are enabled and to the extent patient data may be on the System, it may be accessed or viewed during the remote session.  Note 60  If the System's optional connectivity features are enabled, the System's remote service connections may be used for predictive maintenance data.  If the System's optional connectivity features are enabled, other remotely accessible functionality may be included.  Documentaling for Remote Service can be provided	11010 30			
Note 57  The System's intended use does not require nor permit remote service connections. If the System soptional connectivity features are enabled, the System may permit remote service connections for analysis or repair.  Note 58  If the System's optional connectivity features are enabled and a remote session is active, there is an indicator.  Note 59  If the System's optional connectivity features are enabled and to the extent patient data may be on the System, it may be accessed or viewed during the remote session.  Note 60  If the System's remote service connections may be used for predictive maintenance data.  If the System's optional connectivity features are enabled, other remotely accessible functionality may be included.  Documentation for Remote Service describes Service describes Service described.				
The System's intended use does not require nor permit remote service connections. If the System's optional connectivity features are enabled, the System may permit remote service connections for analysis or repair.  Note 58  If the System's optional connectivity features are enabled and a remote session is active, there is an indicator.  Note 59  If the System's optional connectivity features are enabled and to the extent patient data may be on the System, it may be accessed or viewed during the remote session.  Note 60  If the System's optional connectivity features are enabled, the System's remote service connections may be used for predictive maintenance data.  If the System's optional connectivity features are enabled, other remotely accessible functionality may be included.  Documentation for Remote Service features can be provided	Note 57	dung darismission.		
features are enabled, the System may permit remote service connections for analysis or repair.  Note 58  If the System's optional connectivity features are enabled and a remote session is active, there is an indicator.  Note 59  If the System's optional connectivity features are enabled and to the extent patient data may be on the System, it may be accessed or viewed during the remote session.  Note 60  If the System's optional connectivity features are enabled, the System's remote service connections may be used for predictive maintenance data.  If the System's optional connectivity features are enabled, other remotely accessible functionality may be included.  Documentation for Remote Service describes				
connections for analysis or repair.  If the System's optional connectivity features are enabled and a remote session is active, there is an indicator.  Note 59  If the System's optional connectivity features are enabled and to the extent patient data may be on the System, it may be accessed or viewed during the remote session.  Note 60  If the System's optional connectivity features are enabled, the System's remote service connections may be used for predictive maintenance data.  If the System's optional connectivity features are enabled, other remotely accessible functionality may be included.  Documentation for Remote Service can be provided				
If the System's optional connectivity features are enabled and a remote session is active, there is an indicator.  Note 59  If the System's optional connectivity features are enabled and to the extent patient data may be on the System, it may be accessed or viewed during the remote session.  Note 60  If the System's optional connectivity features are enabled, the System's remote service connections may be used for predictive maintenance data.  If the System's optional connectivity features are enabled, other remotely accessible functionality may be included.  Documentation for Remote Service features and be provided	Note E9			
remote session is active, there is an indicator.  If the System's optional connectivity features are enabled and to the extent patient data may be on the System, it may be accessed or viewed during the remote session.  Note 60  If the System's optional connectivity features are enabled, the System's remote service connections may be used for predictive maintenance data.  If the System's optional connectivity features are enabled, other remotely accessible functionality may be included.  Documentation for Remote Service can be provided	Note 36	If the System's optional connectivity features are enabled and a		
If the System's optional connectivity features are enabled and to the extent patient data may be on the System, it may be accessed or viewed during the remote session.  Note 60  If the System's optional connectivity features are enabled, the System's remote service connections may be used for predictive maintenance data.  If the System's optional connectivity features are enabled, other remotely accessible functionality may be included.  Documentation for Remote Service can be provided	Note 59			
accessed or viewed during the remote session.  If the System's optional connectivity features are enabled, the System's remote service connections may be used for predictive maintenance data.  Note 61 If the System's optional connectivity features are enabled, other remotely accessible functionality may be included.  Documentation for Remote Service features can be provided				
Note 60  If the System's optional connectivity features are enabled, the System's remote service connections may be used for predictive maintenance data.  If the System's optional connectivity features are enabled, other remotely accessible functionality may be included.  Documentation for Remote Service features can be provided				
System's remote service connections may be used for predictive maintenance data.  If the System's optional connectivity features are enabled, other remotely accessible functionality may be included.  Documentation for Remote Service features can be provided	Note 60			
Note 61 maintenance data.  If the System's optional connectivity features are enabled, other remotely accessible functionality may be included.  Documentation for Remote Service features can be provided				
remotely accessible functionality may be included.  Documentation for Remote Service features can be provided	Note 61	maintenance data.		
Documentation for Remote Service features can be provided				
Note 62   upon request.	L	Documentation for Remote Service features can be provided		
	Note 62	Jupon request.		