Manufacturer Disclosure Statement for Medical Device Security -- MDS2			
BIOFIRE Diagnostics, LLC	BIOFIRE® SPOTFIRE® SYSTEM	BFR0001-8102-01	22-Feb-2023
Question ID	**Question**		**See note**
DOC-1	Manufacturer Name	BIOFIRE Diagnostics, LLC	__
DOC-2	Device Description	The BIOFIRE SPOTFIRE System is an automated *in vitro* diagnostic (IVD) device intended for use with compatible BioFire IVD Panels to detect multiple nucleic acid targets contained in patient specimens. The BIOFIRE SPOTFIRE System interacts with the reagent pouch to both purify nucleic acids and amplify targeted nucleic acid sequences using nested multiplex polymerase chain reaction (nmPCR) in a closed system. The resulting PCR products are evaluated using DNA melting analysis. The software automatically determines the results and provides a test report. The BIOFIRE SPOTFIRE instrument is composed of one to four SPOTFIRE Modules connected to one SPOTFIRE Control Station running the SPOTFIRE Application Software. The first Module is placed on top of the Control Station, subsequent modules are added as desired (up to four). Each SPOTFIRE Module can be randomly and independently accessed to run a reagent pouch. The SPOTFIRE software (comprised of the following software components: Application Software, Panel Software, and Connectivity Software) facilitates the collection, analysis, and storage of data on the SPOTFIRE System. The BIOFIRE SPOTFIRE System is designed to be used in ambulatory care and clinical acute care testing environments but is expected to be used in a variety of healthcare settings. SPOTFIRE software will be delivered as a single software installation image with multiple components including the SPOTFIRE Application Software, SPOTFIRE Panel Software, and SPOTFIRE Connectivity Software. All software will be delivered to the customer pre-installed on the control station. The BIOFIRE SPOTFIRE System, hereafter referred to as the "System," is designed to run as a standalone device.	__
DOC-3	Device Model	BIOFIRE® SPOTFIRE® SYSTEM	__
DOC-4	Document ID	BFR0001-8102-01	
DOC-5	Manufacturer Contact Information	BIOFIRE Technical Support Email: BioFiresupport@biomerieux.com Phone: +1-801-736-6354, select Option 5	__
DOC-6	Intended use of device in network-connected environment:	The System is supported in a network-connected environment for purposes such as printing or archiving data to a network location. In addition, the System includes the following connectivity software feature that can be enabled in a network-connected environment. The System can be configured to bidirectionally interface with a Point of Care Data Manager to transfer test results from the System. This optional software feature requires a connection to the local area network (LAN) at the facility.	__
DOC-7	Document Release Date	2/22/2023	
DOC-8	Coordinated Vulnerability Disclosure: Does the manufacturer have a vulnerability disclosure program for this device?	Yes	__
DOC-9	ISAO: Is the manufacturer part of an Information Sharing and Analysis Organization?	Yes	__
DOC-10	Diagram: Is a network or data flow diagram available that indicates connections to other system components or expected external resources?	Yes	__
DOC-11	SaMD: Is the device Software as a Medical Device (i.e. software-only, no hardware)?	No	__
DOC-11.1	Does the SaMD contain an operating system?	N/A	__
DOC-11.2	Does the SaMD rely on an owner/operator provided operating system?	N/A	__
DOC-11.3	Is the SaMD hosted by the manufacturer?	N/A	
DOC-11.4	Is the SaMD hosted by the customer?	N/A	__
		Yes, No, N/A, or See Note	Note #
	MANAGEMENT OF PERSONALLY IDENTIFIABLE INFORMATION		
MPII-1	Can this device display, transmit, store, or modify personally identifiable information (e.g. electronic Protected Health Information (ePHI))?	See Notes	Note 1
MPII-2	Does the device maintain personally identifiable information?	See Notes	Note 2
MPII-2.1	Does the device maintain personally identifiable information temporarily in volatile memory (i.e., until cleared by power-off or reset)?	See Notes	Note 3
MPII-2.2	Does the device store personally identifiable information persistently on internal media?	See Notes	Note 4
MPII-2.3	Is personally identifiable information preserved in the device's non-volatile memory until explicitly erased?	See Notes	Note 5
MPII-2.4	Does the device store personally identifiable information in a database?	See Notes	Note 6
MPII-2.5	Does the device allow configuration to automatically delete local personally identifiable information after it is stored to a long term solution?	See Notes	Note 7

BIOFIRE Diagnostics, LLC	BIOFIRE® SPOTFIRE® SYSTEM	BFR0001-8102-01	22-Feb-2023
MPII-2.6	Does the device import/export personally identifiable information with other systems (e.g., a wearable monitoring device might export personally identifiable information to a server)?	See Notes	Note 8
MPII-2.7	Does the device maintain personally identifiable information when powered off, or during power service interruptions?	See Notes	Note 9
MPII-2.8	Does the device allow the internal media to be removed by a service technician (e.g., for separate destruction or customer retention)?	Yes	__
MPII-2.9	Does the device allow personally identifiable information records be stored in a separate location from the device's operating system (i.e. secondary internal drive, alternate drive partition, or remote storage location)?	See Notes	Note 10
MPII-3	Does the device have mechanisms used for the transmitting, importing/exporting of personally identifiable information?	See Notes	Note 11
MPII-3.1	Does the device display personally identifiable information (e.g., video display, etc.)?	See Notes	Note 12
MPII-3.2	Does the device generate hardcopy reports or images containing personally identifiable information?	See Notes	Note 13
MPII-3.3	Does the device retrieve personally identifiable information from or record personally identifiable information to removable media (e.g., removable-HDD, USB memory, DVD-R/RW,CD-R/RW, tape, CF/SD card, memory stick, etc.)?	See Notes	Note 14
MPII-3.4	Does the device transmit/receive or import/export personally identifiable information via dedicated cable connection (e.g., RS-232, RS-423, USB, FireWire, etc.)?	See Notes	Note 15
MPII-3.5	Does the device transmit/receive personally identifiable information via a wired network connection (e.g., RJ45, fiber optic, etc.)?	See Notes	Note 16
MPII-3.6	Does the device transmit/receive personally identifiable information via a wireless network connection (e.g., WiFi, Bluetooth, NFC, infrared, cellular, etc.)?	See Notes	Note 17
MPII-3.7	Does the device transmit/receive personally identifiable information over an external network (e.g., Internet)?	No	__
MPII-3.8	Does the device import personally identifiable information via scanning a document?	No	__
MPII-3.9	Does the device transmit/receive personally identifiable information via a proprietary protocol?	No	__
MPII-3.10	Does the device use any other mechanism to transmit, import or export personally identifiable information?	No	__
Management of Private Data notes:			
	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.		
ALOF-1	Can the device be configured to force reauthorization of logged-in user(s) after a predetermined length of inactivity (e.g., auto-logoff, session lock, password protected screen saver)?	Yes	__
ALOF-2	Is the length of inactivity time before auto-logoff/screen lock user or administrator configurable?	Yes	__
	AUDIT CONTROLS (AUDT)		
	The ability to reliably audit activity on the device.		
AUDT-1	Can the medical device create additional audit logs or reports beyond standard operating system logs?	Yes	__
AUDT-1.1	Does the audit log record a USER ID?	Yes	__
AUDT-1.2	Does other personally identifiable information exist in the audit trail?	Yes	
AUDT-2	Are events recorded in an audit log? If yes, indicate which of the following events are recorded in the audit log:	Yes	__
AUDT-2.1	Successful login/logout attempts?	Yes	__
AUDT-2.2	Unsuccessful login/logout attempts?	Yes	__
AUDT-2.3	Modification of user privileges?	Yes	__
AUDT-2.4	Creation/modification/deletion of users?	Yes	__
AUDT-2.5	Presentation of clinical or PII data (e.g. display, print)?	No	__
AUDT-2.6	Creation/modification/deletion of data?	Yes	__
AUDT-2.7	Import/export of data from removable media (e.g. USB drive, external hard drive, DVD)?	Yes	__

BIOFIRE Diagnostics, LLC	BIOFIRE® SPOTFIRE® SYSTEM	BFR0001-8102-01	22-Feb-2023
AUDT-2.8	Receipt/transmission of data or commands over a network or point-to-point connection?	Yes	
AUDT-2.8.1	Remote or on-site support?	No	
AUDT-2.8.2	Application Programming Interface (API) and similar activity?	No	
AUDT-2.9	Emergency access?	No	
AUDT-2.10	Other events (e.g., software updates)?	Yes	
AUDT-2.11	Is the audit capability documented in more detail?	Yes	
AUDT-3	Can the owner/operator define or select which events are recorded in the audit log?	No	
AUDT-4	Is a list of data attributes that are captured in the audit log for an event available?	No	
AUDT-4.1	Does the audit log record date/time?	Yes	
AUDT-4.1.1	Can date and time be synchronized by Network Time Protocol (NTP) or equivalent time source?	No	
AUDT-5	Can audit log content be exported?	Yes	
AUDT-5.1	Via physical media?	Yes	
AUDT-5.2	Via IHE Audit Trail and Node Authentication (ATNA) profile to SIEM?	No	
AUDT-5.3	Via Other communications (e.g., external service device, mobile applications)?	No	
AUDT-5.4	Are audit logs encrypted in transit or on storage media?	No	
AUDT-6	Can audit logs be monitored/reviewed by owner/operator?	Yes	
AUDT-7	Are audit logs protected from modification?	Yes	
AUDT-7.1	Are audit logs protected from access?	Yes	
AUDT-8	Can audit logs be analyzed by the device?	No	
	AUTHORIZATION (AUTH)		
	The ability of the device to determine the authorization of users.		
AUTH-1	Does the device prevent access to unauthorized users through user login requirements or other mechanism?	See Notes	Note 18
AUTH-1.1	Can the device be configured to use federated credentials management of users for authorization (e.g., LDAP, OAuth)?	See Notes	Note 19
AUTH-1.2	Can the customer push group policies to the device (e.g., Active Directory)?	No	
AUTH-1.3	Are any special groups, organizational units, or group policies required?	No	
AUTH-2	Can users be assigned different privilege levels based on 'role' (e.g., user, administrator, and/or service, etc.)?	See Notes	Note 20
AUTH-3	Can the device owner/operator grant themselves unrestricted administrative privileges (e.g., access operating system or application via local root or administrator account)?	See Notes	Note 21
AUTH-4	Does the device authorize or control all API access requests?	Yes	
AUTH-5	Does the device run in a restricted access mode, or 'kiosk mode', by default?	Yes	
	CYBER SECURITY PRODUCT UPGRADES (CSUP)		
	The ability of on-site service staff, remote service staff, or authorized customer staff to install/upgrade device's security patches.		
CSUP-1	Does the device contain any software or firmware which may require security updates during its operational life, either from the device manufacturer or from a third-party manufacturer of the software/firmware? If no, answer "N/A" to questions in this section.	Yes	
CSUP-2	Does the device contain an Operating System? If yes, complete 2.1-2.4.	Yes	
CSUP-2.1	Does the device documentation provide instructions for owner/operator installation of patches or software updates?	See Notes	Note 22
CSUP-2.2	Does the device require vendor or vendor-authorized service to install patches or software updates?	No	
CSUP-2.3	Does the device have the capability to receive remote installation of patches or software updates?	No	
CSUP-2.4	Does the medical device manufacturer allow security updates from any third-party manufacturers (e.g., Microsoft) to be installed without approval from the manufacturer?	See Notes	Note 23
CSUP-3	Does the device contain Drivers and Firmware? If yes, complete 3.1-3.4.	Yes	
CSUP-3.1	Does the device documentation provide instructions for owner/operator installation of patches or software updates?	Yes	

BIOFIRE Diagnostics, LLC	BIOFIRE® SPOTFIRE® SYSTEM	BFR0001-8102-01	22-Feb-2023
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	
CSUP-3.4	Does the medical device manufacturer allow security updates from any third-party manufacturers (e.g., Microsoft) to be installed without approval from the manufacturer?	See Notes	Note 25
CSUP-4	Does the device contain Anti-Malware Software? If yes, complete 4.1-4.4.	Yes	
CSUP-4.1	Does the device documentation provide instructions for owner/operator installation of patches or software updates?	See Notes	Note 26
CSUP-4.2	Does the device require vendor or vendor-authorized service to install patches or software updates?	No	
CSUP-4.3	Does the device have the capability to receive remote installation of patches or software updates?	No	
CSUP-4.4	Does the medical device manufacturer allow security updates from any third-party manufacturers (e.g., Microsoft) to be installed without approval from the manufacturer?	See Notes	Note 27
CSUP-5	Does the device contain Non-Operating System commercial off-the-shelf components? If yes, complete 5.1-5.4.	Yes	
CSUP-5.1	Does the device documentation provide instructions for owner/operator installation of patches or software updates?	No	
CSUP-5.2	Does the device require vendor or vendor-authorized service to install patches or software updates?	Yes	
CSUP-5.3	Does the device have the capability to receive remote installation of patches or software updates?	No	
CSUP-5.4	Does the medical device manufacturer allow security updates from any third-party manufacturers (e.g., Microsoft) to be installed without approval from the manufacturer?	No	
CSUP-6	Does the device contain other software components (e.g., asset management software, license management)? If yes, please provide details or reference in notes and complete 6.1-6.4.	No	
CSUP-6.1	Does the device documentation provide instructions for owner/operator installation of patches or software updates?	N/A	
CSUP-6.2	Does the device require vendor or vendor-authorized service to install patches or software updates?	N/A	
CSUP-6.3	Does the device have the capability to receive remote installation of patches or software updates?	N/A	
CSUP-6.4	Does the medical device manufacturer allow security updates from any third-party manufacturers (e.g., Microsoft) to be installed without approval from the manufacturer?	N/A	
CSUP-7	Does the manufacturer notify the customer when updates are approved for installation?	Yes	
CSUP-8	Does the device perform automatic installation of software updates?	No	
CSUP-9	Does the manufacturer have an approved list of third-party software that can be installed on the device?	No	
CSUP-10	Can the owner/operator install manufacturer-approved third-party software on the device themselves?	N/A	
CSUP-10.1	Does the system have mechanism in place to prevent installation of unapproved software?	N/A	
CSUP-11	Does the manufacturer have a process in place to assess device vulnerabilities and updates?	Yes	
CSUP-11.1	Does the manufacturer provide customers with review and 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 28
DIDT-1.1	Does the device support de-identification profiles that comply with the DICOM standard for de-identification?	N/A	

BIOFIRE Diagnostics, LLC	BIOFIRE® SPOTFIRE® SYSTEM	BFR0001-8102-01	22-Feb-2023
	DATA BACKUP AND DISASTER RECOVERY (DTBK)		
	The ability to recover after damage or destruction of device data, hardware, software, or site configuration information.		
DTBK-1	Does the device maintain long term primary storage of personally identifiable information / patient information (e.g. PACS)?	See Notes	Note 29
DTBK-2	Does the device have a "factory reset" function to restore the original device settings as provided by the manufacturer?	Yes	
DTBK-3	Does the device have an integral data backup capability to removable media?	Yes	
DTBK-4	Does the device have an integral data backup capability to remote storage?	Yes	
DTBK-5	Does the device have a backup capability for system configuration information, patch restoration, and software restoration?	No	
DTBK-6	Does the device provide the capability to check the integrity and authenticity of a backup?	Yes	
	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.		
EMRG-1	Does the device incorporate an emergency access (i.e. "break-glass") feature?	No	
	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.		
IGAU-1	Does the device provide data integrity checking mechanisms of stored health data (e.g., hash or digital signature)?	No	
IGAU-2	Does the device provide error/failure protection and recovery 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?	Yes	
MLDP-2	Does the device support the use of anti-malware software (or other anti-malware mechanism)? Provide details or reference in 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	
MLDP-2.4	Can the device owner/operator independently (re-)configure anti-malware settings?	No	
MLDP-2.5	Does notification of malware detection occur in the device user interface?	No	
MLDP-2.6	Can only manufacturer-authorized persons repair systems when malware has been detected?	See Notes	Note 30
MLDP-2.7	Are malware notifications written to a log?	See Notes	Note 31
MLDP-2.8	Are there any restrictions on anti-malware (e.g., purchase, installation, configuration, scheduling)?	Yes	
MLDP-3	If the answer to MLDP-2 is NO, and anti-malware cannot be installed on the device, are other compensating controls in place or available?	N/A	
MLDP-4	Does the device employ application whitelisting that restricts the software and services that are permitted to be run on the device?	No	
MLDP-5	Does the device employ a host-based intrusion detection/prevention system?	No	

BIOFIRE Diagnostics, LLC	BIOFIRE® SPOTFIRE® SYSTEM	BFR0001-8102-01	22-Feb-2023
MLDP-5.1	Can the host-based intrusion detection/prevention system be configured by the customer?	N/A	
MLDP-5.2	Can a host-based intrusion detection/prevention system be installed by the customer?	See Notes	Note 32
	NODE AUTHENTICATION (NAUT)		
	The ability of the device to authenticate communication partners/nodes.		
NAUT-1	Does the device provide/support any means of node authentication that assures both the sender and the recipient of data are known to each other and are authorized to receive transferred information (e.g. Web APIs, SMTP, SNMP)?	No	
NAUT-2	Are network access control mechanisms supported (E.g., does 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	
NAUT-3	Does the device use certificate-based network connection authentication?	See Notes	Note 33
	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 34
CONN-1.1	Does the device support wireless connections?	Yes	
CONN-1.1.1	Does the device support Wi-Fi?	Yes	
CONN-1.1.2	Does the device support Bluetooth?	No	
CONN-1.1.3	Does the device support other wireless network connectivity (e.g. LTE, Zigbee, proprietary)?	No	
CONN-1.1.4	Does the device support other wireless connections (e.g., custom RF controls, wireless detectors)?	No	
CONN-1.2	Does the device support physical connections?	Yes	
CONN-1.2.1	Does the device have available RJ45 Ethernet ports?	Yes	
CONN-1.2.2	Does the device have available USB ports?	See Notes	Note 35
CONN-1.2.3	Does the device require, use, or support removable memory devices?	See Notes	Note 36
CONN-1.2.4	Does the device support other physical connectivity?	No	
CONN-2	Does the manufacturer provide a list of network ports and protocols that are used or may be used on the device?	No	
CONN-3	Can the device communicate with other systems within the customer environment?	See Notes	Note 37
CONN-4	Can the device communicate with other systems external to the customer environment (e.g., a service host)?	No	
CONN-5	Does the device make or receive API calls?	See Notes	Note 38
CONN-6	Does the device require an internet connection for its intended use?	No	
CONN-7	Does the device support Transport Layer Security (TLS)?	Yes	
CONN-7.1	Is TLS configurable?	No	
CONN-8	Does the device provide operator control functionality from a separate device (e.g., telemedicine)?	Yes	
	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)?	See Notes	Note 39
PAUT-1.1	Does the device enforce authentication of unique IDs and passwords for all users and roles (including service accounts)?	See Notes	Note 40
PAUT-2	Is the device configurable to authenticate users through an external authentication service (e.g., MS Active Directory, NDS, LDAP, OAuth, etc.)?	No	
PAUT-3	Is the device configurable to lock out a user after a certain number of unsuccessful logon attempts?	No	
PAUT-4	Are all default accounts (e.g., technician service accounts, administrator accounts) listed in the documentation?	No	
PAUT-5	Can all passwords be changed?	Yes	

BIOFIRE Diagnostics, LLC	BIOFIRE® SPOTFIRE® SYSTEM	BFR0001-8102-01	22-Feb-2023
PAUT-6	Is the device configurable to enforce creation of user account passwords that meet established (organization specific) complexity rules?	See Notes	Note 41
PAUT-7	Does the device support account passwords that expire periodically?	No	
PAUT-8	Does the device support multi-factor authentication?	No	
PAUT-9	Does the device support single sign-on (SSO)?	No	
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)?	See Notes	Note 42
PAUT-13	Does the device support group authentication (e.g. hospital teams)?	No	
PAUT-14	Does the application or device store or manage authentication credentials?	Yes	
PAUT-14.1	Are credentials stored using a secure method?	Yes	
	PHYSICAL LOCKS (PLOK)		
	Physical locks can prevent unauthorized users with physical access to the device from compromising the integrity and confidentiality of personally identifiable information stored on the device or on removable media		
PLOK-1	Is the device software only? If yes, answer "N/A" to remaining questions in this section.	No	
PLOK-2	Are all device components maintaining personally identifiable information (other than removable media) physically secure (i.e., cannot remove without tools)?	See Notes	Note 43
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-4	Does the device have an option for the customer to attach a physical lock to restrict access to removable media?	No	
	ROADMAP FOR THIRD PARTY COMPONENTS IN DEVICE LIFE CYCLE (RDMP)		
	Manufacturer's plans for security support of third-party components within the device's life cycle.		
RDMP-1	Was a secure software development process, such as ISO/IEC 27034 or IEC 62304, followed during product development?	See Notes	Note 45
RDMP-2	Does the manufacturer evaluate third-party applications and software components included in the device for secure development practices?	Yes	
RDMP-3	Does the manufacturer maintain a web page or other source of information on software support dates and updates?	Yes	
RDMP-4	Does the manufacturer have a plan for managing third-party component end-of-life?	Yes	
	SOFTWARE BILL OF MATERIALS (SBoM)		
	A Software Bill of Material (SBoM) lists all the software components that are incorporated into the device being described for the purpose of operational security planning by the healthcare delivery organization. This section supports controls in the RDMP section.		
SBOM-1	Is the SBoM for this product available?	Yes	
SBOM-2	Does the SBoM follow a standard or common method in describing 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	
SBOM-2.3	Are the major version numbers of the software components identified?	Yes	
SBOM-2.4	Are any additional descriptive elements identified?	No	
SBOM-3	Does the device include a command or process method available to generate a list of software components installed on the device?	No	
SBOM-4	Is there an update process for the SBoM?	Yes	
	SYSTEM AND APPLICATION HARDENING (SAHD)		
	The device's inherent resistance to cyber attacks and malware.		
SAHD-1	Is the device hardened in accordance with any industry standards?	No	

BIOFIRE Diagnostics, LLC	BIOFIRE® SPOTFIRE® SYSTEM	BFR0001-8102-01	22-Feb-2023
SAHD-2	Has the device received any cybersecurity certifications?	No	
SAHD-3	Does the device employ any mechanisms for software integrity checking	No	
SAHD-3.1	Does the device employ any mechanism (e.g., release-specific hash key, checksums, digital signature, etc.) to ensure the installed software is manufacturer-authorized?	See Notes	Note 46
SAHD-3.2	Does the device employ any mechanism (e.g., release-specific hash key, checksums, digital signature, etc.) to ensure the software updates are the manufacturer-authorized updates?	Yes	
SAHD-4	Can the owner/operator perform software integrity checks (i.e., verify that the system has not been modified or tampered with)?	No	
SAHD-5	Is the system configurable to allow the implementation of file-level, patient level, or other types of access controls?	No	
SAHD-5.1	Does the device provide role-based access controls?	Yes	
SAHD-6	Are any system or user accounts restricted or disabled by the manufacturer at system delivery?	See Notes	Note 47
SAHD-6.1	Are any system or user accounts configurable by the end user after initial configuration?	No	
SAHD-6.2	Does this include restricting certain system or user accounts, such as service technicians, to least privileged access?	No	
SAHD-7	Are all shared resources (e.g., file shares) which are not required for the intended use of the device disabled?	N/A	
SAHD-8	Are all communication ports and protocols that are not required for the intended use of the device disabled?	See Notes	Note 48
SAHD-9	Are all services (e.g., telnet, file transfer protocol [FTP], internet information server [IIS], etc.), which are not required for the intended use of the device deleted/disabled?	Yes	
SAHD-10	Are all applications (COTS applications as well as OS-included applications, e.g., MS Internet Explorer, etc.) which are not required for the intended use of the device deleted/disabled?	See Notes	Note 49
SAHD-11	Can the device prohibit boot from uncontrolled or removable media (i.e., a source other than an internal drive or memory component)?	No	
SAHD-12	Can unauthorized software or hardware be installed on the device without the use of physical tools?	Yes	
SAHD-13	Does the product documentation include information on operational network security scanning by users?	No	
SAHD-14	Can the device be hardened beyond the default provided state?	See Notes	Note 50
SAHD-14.1	Are instructions available from vendor for increased hardening?	See Notes	Note 51
SHAD-15	Can the system prevent access to BIOS or other bootloaders during boot?	No	
SAHD-16	Have additional hardening methods not included in 2.3.19 been used to harden the device?	See Notes	Note 52
	SECURITY GUIDANCE (SGUD)		
	Availability of security guidance for operator and administrator of the device and manufacturer sales and service.		
SGUD-1	Does the device include security documentation for the owner/operator?	Yes	
SGUD-2	Does the device have the capability, and provide instructions, for the permanent deletion of data from the device or media?	See Notes	Note 53
SGUD-3	Are all access accounts documented?	See Notes	Note 54
SGUD-3.1	Can the owner/operator manage password control for all accounts?	See Notes	Note 55
SGUD-4	Does the product include documentation on recommended compensating controls for the device?	No	
	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	

BIOFIRE Diagnostics, LLC	BIOFIRE® SPOTFIRE® SYSTEM	BFR0001-8102-01	22-Feb-2023
STCF-1.1	Is all data encrypted or otherwise protected?	See Notes	Note 56
STCF-1.2	Is the data encryption capability configured by default?	N/A	
STCF-1.3	Are instructions available to the customer to configure encryption?	N/A	
STCF-2	Can the encryption keys be changed or configured?	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?	No	__
	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	__
TXCF-2	Is personally identifiable information encrypted prior to transmission via a network or removable media?	See Notes	Note 57
TXCF-2.1	If data is not encrypted by default, can the customer configure encryption options?	No	__
TXCF-3	Is personally identifiable information transmission restricted to a fixed list of network destinations?	No	__
TXCF-4	Are connections limited to authenticated systems?	No	__
TXCF-5	Are secure transmission methods supported/implemented (DICOM, HL7, IEEE 11073)?	No	__
	TRANSMISSION INTEGRITY (TXIG)		
	The ability of the device to ensure the integrity of transmitted data.		
TXIG-1	Does the device support any mechanism (e.g., digital signatures) intended to ensure data is not modified during transmission?	No	__
TXIG-2	Does the device include multiple sub-components connected by external cables?	No	__
	REMOTE SERVICE (RMOT)		
	Remote service refers to all kinds of device maintenance activities performed by a service person via network or other remote connection.		
RMOT-1	Does the device permit remote service connections for device analysis or repair?	No	__
RMOT-1.1	Does the device allow the owner/operator to initiative remote service sessions for device analysis or repair?	N/A	__
RMOT-1.2	Is there an indicator for an enabled and active remote session?	N/A	__
RMOT-1.3	Can patient data be accessed or viewed from the device during the remote session?	N/A	__
RMOT-2	Does the device permit or use remote service connections for predictive maintenance data?	No	__
RMOT-3	Does the device have any other remotely accessible functionality (e.g. software updates, remote training)?	See Notes	Note 58
	OTHER SECURITY CONSIDERATIONS (OTHR)		
	NONE		
	Notes:		

BIOFIRE Diagnostics, LLC	BIOFIRE® SPOTFIRE® SYSTEM	BFR0001-8102-01	22-Feb-2023
Note 1	The following data fields are associated with each test on the System: Run Start Time and Run End Time, Serial Number (of consumable), Lot Number (of consumable), Operator, Module Serial Number, Sample Type, Pouch Type, and a Sample ID. The "Sample ID" field is a free text field, and bioMérieux issues guidance to use sequentially generated recycled accession numbers in the "Sample ID" field. Consistent with this guidance, do not enter patient names, addresses, demographic information, financial information, medical record numbers, Social Security numbers, and any other unique identifying number, characteristic, or code in the Sample ID field. To the extent the information contained in any these fields is personally identifiable information, as defined in ANSI/NEMA HN 1-2019, such information is displayed and stored on the System. As an optional feature, the System may be configured to transmit such information.		
Note 2	The following data fields are associated with each test on the System: Run Start Time and Run End Time, Serial Number (of consumable), Lot Number (of consumable), Operator, Module Serial Number, Sample Type, Pouch Type, and a Sample ID. The "Sample ID" field is a free text field, and bioMérieux issues guidance to use sequentially generated recycled accession numbers in the "Sample ID" field. Consistent with this guidance, do not enter patient names, addresses, demographic information, financial information, medical record numbers, Social Security numbers, and any other unique identifying number, characteristic, or code in the Sample ID field. To the extent the information contained in any these fields is personally identifiable information, as defined in ANSI/NEMA HN 1-2019, such information is maintained on the System.		
Note 3	The following data fields are associated with each test on the System: Run Start Time and Run End Time, Serial Number (of consumable), Lot Number (of consumable), Operator, Module Serial Number, Sample Type, Pouch Type, and a Sample ID. The "Sample ID" field is a free text field, and bioMérieux issues guidance to use sequentially generated recycled accession numbers in the "Sample ID" field. Consistent with this guidance, do not enter patient names, addresses, demographic information, financial information, medical record numbers, Social Security numbers, and any other unique identifying number, characteristic, or code in the Sample ID field. To the extent the information contained in any these fields is personally identifiable information, as defined in ANSI/NEMA HN 1-2019, such information is maintained on the System. The system does have the ability to clear personally identifiable information through a Factory Reset Feature.		

BIOFIRE Diagnostics, LLC	BIOFIRE® SPOTFIRE® SYSTEM	BFR0001-8102-01	22-Feb-2023
Note 4	The following data fields are associated with each test on the System: Run Start Time and Run End Time, Serial Number (of consumable), Lot Number (of consumable), Operator, Module Serial Number, Sample Type, Pouch Type, and a Sample ID. The "Sample ID" field is a free text field, and bioMérieux issues guidance to use sequentially generated recycled accession numbers in the "Sample ID" field. Consistent with this guidance, do not enter patient names, addresses, demographic information, financial information, medical record numbers, Social Security numbers, and any other unique identifying number, characteristic, or code in the Sample ID field. To the extent the information contained in any these fields is personally identifiable information, as defined in ANSI/NEMA HN 1-2019, such information is stored on internal media within the System.		
Note 5	The following data fields are associated with each test on the System: Run Start Time and Run End Time, Serial Number (of consumable), Lot Number (of consumable), Operator, Module Serial Number, Sample Type, Pouch Type, and a Sample ID. The "Sample ID" field is a free text field, and bioMérieux issues guidance to use sequentially generated recycled accession numbers in the "Sample ID" field. Consistent with this guidance, do not enter patient names, addresses, demographic information, financial information, medical record numbers, Social Security numbers, and any other unique identifying number, characteristic, or code in the Sample ID field. To the extent the information contained in any these fields is personally identifiable information, as defined in ANSI/NEMA HN 1-2019, such information is preserved in the System's nonvolatile memory until explicitly erased.		
Note 6	The following data fields are associated with each test on the System: Run Start Time and Run End Time, Serial Number (of consumable), Lot Number (of consumable), Operator, Module Serial Number, Sample Type, Pouch Type, and a Sample ID. The "Sample ID" field is a free text field, and bioMérieux issues guidance to use sequentially generated recycled accession numbers in the "Sample ID" field. Consistent with this guidance, do not enter patient names, addresses, demographic information, financial information, medical record numbers, Social Security numbers, and any other unique identifying number, characteristic, or code in the Sample ID field. To the extent the information contained in any these fields is personally identifiable information, as defined in ANSI/NEMA HN 1-2019, such information is stored in a database within the System.		

BIOFIRE Diagnostics, LLC	BIOFIRE® SPOTFIRE® SYSTEM	BFR0001-8102-01	22-Feb-2023
Note 7	The following data fields are associated with each test on the System: Run Start Time and Run End Time, Serial Number (of consumable), Lot Number (of consumable), Operator, Module Serial Number, Sample Type, Pouch Type, and a Sample ID. The "Sample ID" field is a free text field, and bioMérieux issues guidance to use sequentially generated recycled accession numbers in the "Sample ID" field. Consistent with this guidance, do not enter patient names, addresses, demographic information, financial information, medical record numbers, Social Security numbers, and any other unique identifying number, characteristic, or code in the Sample ID field. To the extent the information contained in any these fields is personally identifiable information, as defined in ANSI/NEMA HN 1-2019, such information may be deleted by the software. As an optional feature, the System may be configured to transmit such information.		
Note 8	The following data fields are associated with each test on the System: Run Start Time and Run End Time, Serial Number (of consumable), Lot Number (of consumable), Operator, Module Serial Number, Sample Type, Pouch Type, and a Sample ID. The "Sample ID" field is a free text field, and 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 imported/exported with other systems via configuration of optional connectivity features.		
Note 9	The following data fields are associated with each test on the System: Run Start Time and Run End Time, Serial Number (of consumable), Lot Number (of consumable), Operator, Module Serial Number, Sample Type, Pouch Type, and a Sample ID. The "Sample ID" field is a free text field, and bioMérieux issues guidance to use sequentially generated recycled accession numbers in the "Sample ID" field. Consistent with this guidance, do not enter patient names, addresses, demographic information, financial information, medical record numbers, Social Security numbers, and any other unique identifying number, characteristic, or code in the Sample ID field. To the extent the information contained in any these fields is personally identifiable information, as defined in ANSI/NEMA HN 1-2019, such information may be maintained when powered off, or during power service interruptions.		

BIOFIRE Diagnostics, LLC	BIOFIRE® SPOTFIRE® SYSTEM	BFR0001-8102-01	22-Feb-2023
Note 10	The following data fields are associated with each test on the System: Run Start Time and Run End Time, Serial Number (of consumable), Lot Number (of consumable), Operator, Module Serial Number, Sample Type, Pouch Type, and a Sample ID. The "Sample ID" field is a free text field, and bioMérieux issues guidance to use sequentially generated recycled accession numbers in the "Sample ID" field. Consistent with this guidance, do not enter patient names, addresses, demographic information, financial information, medical record numbers, Social Security numbers, and any other unique identifying number, characteristic, or code in the Sample ID field. To the extent the information contained in any these fields is personally identifiable information, as defined in ANSI/NEMA HN 1-2019, such information may be stored in a separate location from the System's operating system.		
Note 11	The following data fields are associated with each test on the System: Run Start Time and Run End Time, Serial Number (of consumable), Lot Number (of consumable), Operator, Module Serial Number, Sample Type, Pouch Type, and a Sample ID. The "Sample ID" field is a free text field, and bioMérieux issues guidance to use sequentially generated recycled accession numbers in the "Sample ID" field. Consistent with this guidance, do not enter patient names, addresses, demographic information, financial information, medical record numbers, Social Security numbers, and any other unique identifying number, characteristic, or code in the Sample ID field. To the extent the information contained in any these fields is personally identifiable information, as defined in ANSI/NEMA HN 1-2019, the System does have mechanisms used for transmitting and importing/exporting such information.		
Note 12	The following data fields are associated with each test on the System: Run Start Time and Run End Time, Serial Number (of consumable), Lot Number (of consumable), Operator, Module Serial Number, Sample Type, Pouch Type, and a Sample ID. The "Sample ID" field is a free text field, and bioMérieux issues guidance to use sequentially generated recycled accession numbers in the "Sample ID" field. Consistent with this guidance, do not enter patient names, addresses, demographic information, financial information, medical record numbers, Social Security numbers, and any other unique identifying number, characteristic, or code in the Sample ID field. To the extent the information contained in any these fields is personally identifiable information, as defined in ANSI/NEMA HN 1-2019, such information is displayed by the System.		

BIOFIRE Diagnostics, LLC	BIOFIRE® SPOTFIRE® SYSTEM	BFR0001-8102-01	22-Feb-2023
Note 13	The following data fields are associated with each test on the System: Run Start Time and Run End Time, Serial Number (of consumable), Lot Number (of consumable), Operator, Module Serial Number, Sample Type, Pouch Type, and a Sample ID. The "Sample ID" field is a free text field, and bioMérieux issues guidance to use sequentially generated recycled accession numbers in the "Sample ID" field. Consistent with this guidance, do not enter patient names, addresses, demographic information, financial information, medical record numbers, Social Security numbers, and any other unique identifying number, characteristic, or code in the Sample ID field. To the extent the information contained in any these fields is personally identifiable information, as defined in ANSI/NEMA HN 1-2019, such information may be contained on generated hard copy reports or images.		
Note 14	The following data fields are associated with each test on the System: Run Start Time and Run End Time, Serial Number (of consumable), Lot Number (of consumable), Operator, Module Serial Number, Sample Type, Pouch Type, and a Sample ID. The "Sample ID" field is a free text field, and bioMérieux issues guidance to use sequentially generated recycled accession numbers in the "Sample ID" field. Consistent with this guidance, do not enter patient names, addresses, demographic information, financial information, medical record numbers, Social Security numbers, and any other unique identifying number, characteristic, or code in the Sample ID field. To the extent the information contained in any these fields is personally identifiable information, as defined in ANSI/NEMA HN 1-2019, such information may be retrieved from or recorded to removable media.		
Note 15	The following data fields are associated with each test on the System: Run Start Time and Run End Time, Serial Number (of consumable), Lot Number (of consumable), Operator, Module Serial Number, Sample Type, Pouch Type, and a Sample ID. The "Sample ID" field is a free text field, and bioMérieux issues guidance to use sequentially generated recycled accession numbers in the "Sample ID" field. Consistent with this guidance, do not enter patient names, addresses, demographic information, financial information, medical record numbers, Social Security numbers, and any other unique identifying number, characteristic, or code in the Sample ID field. To the extent the information contained in any these fields is personally identifiable information, as defined in ANSI/NEMA HN 1-2019, such information may be transmitted/received or imported/exported via dedicated cable connection.		

BIOFIRE Diagnostics, LLC	BIOFIRE® SPOTFIRE® SYSTEM	BFR0001-8102-01	22-Feb-2023
Note 16	The following data fields are associated with each test on the System: Run Start Time and Run End Time, Serial Number (of consumable), Lot Number (of consumable), Operator, Module Serial Number, Sample Type, Pouch Type, and a Sample ID. The "Sample ID" field is a free text field, and bioMérieux issues guidance to use sequentially generated recycled accession numbers in the "Sample ID" field. Consistent with this guidance, do not enter patient names, addresses, demographic information, financial information, medical record numbers, Social Security numbers, and any other unique identifying number, characteristic, or code in the Sample ID field. To the extent the information contained in any these fields is personally identifiable information, as defined in ANSI/NEMA HN 1-2019, such information may be transmitted/received via a wired network connection.		
Note 17	The following data fields are associated with each test on the System: Run Start Time and Run End Time, Serial Number (of consumable), Lot Number (of consumable), Operator, Module Serial Number, Sample Type, Pouch Type, and a Sample ID. The "Sample ID" field is a free text field, and bioMérieux issues guidance to use sequentially generated recycled accession numbers in the "Sample ID" field. Consistent with this guidance, do not enter patient names, addresses, demographic information, financial information, medical record numbers, Social Security numbers, and any other unique identifying number, characteristic, or code in the Sample ID field. To the extent the information contained in any these fields is personally identifiable information, as defined in ANSI/NEMA HN 1-2019, such information may be transmitted/received over an external network if the System is configured with an optional connectivity feature.		
Note 18	The System is pre-configured to log on to Windows using the SPOTFIRE user account automatically. The SPOTFIRE user account is a Windows Standard User with its equivalent access rights. The System computer is also pre-configured with an administrative user account (LabAdmin). It is recommended the System owner/operator change the default password for the LabAdmin user account as the account has local administrative privileges. SPOTFIRE has a set operator list which only allows the SPOTFIRE application software to be accessed.		
Note 19	When optional connectivity features are enabled, application user credentials may be maintained by a centralized data-management system and distributed over a network to one or multiple connected devices according to the customer's organizational requirements. In this configuration, application user credentials on the device cannot be modified or shared with other devices.		
Note 20	The system allows operators to be created with or without administrator privileges.		
Note 21	The System is operated using a Windows Operating System User Account that does not have administrative privileges. Configuration changes require administrative privileges using an administrative Windows user account pre-configured on the computer. The System application software does not allow operators to modify their own administrator privileges.		
Note 22	Instructions for the owner/operator installation of Operating System patches are within BFR0001-6037 Microsoft OS Patch Policy Tech Note.		
Note 23	Instructions for the owner/operator installation of Operating System patches are within BFR0001-6037 Microsoft OS Patch Policy Tech Note.		

BIOFIRE Diagnostics, LLC	BIOFIRE® SPOTFIRE® SYSTEM	BFR0001-8102-01	22-Feb-2023
Note 24	Documentation for Driver and Firmware patches or updates, if required, will be distributed by bioMérieux's BIOFIRE Technical Support team.		
Note 25	The recommended installation process for updates from third party manufactures (e.g. Microsoft) is available within BFR0001-6037 Microsoft OS Patch Policy Tech Note.		
Note 26	Instructions for the owner/operator installation of AntiMalware Software patches are within BFR0001-6037 Microsoft OS Patch Policy Tech Note.		
Note 27	The recommended installation process for updates from third party manufactures (e.g. Microsoft) is available within BFR0001-6037 Microsoft OS Patch Policy Tech Note.		
Note 28	The following data fields are associated with each test on the System: Run Start Time and Run End Time, Serial Number (of consumable), Lot Number (of consumable), Operator, Module Serial Number, Sample Type, Pouch Type, and a Sample ID. The "Sample ID" field is a free text field, and bioMérieux issues guidance to use sequentially generated recycled accession numbers in the "Sample ID" field. Consistent with this guidance, do not enter patient names, addresses, demographic information, financial information, medical record numbers, Social Security numbers, and any other unique identifying number, characteristic, or code in the Sample ID field. To the extent the information contained in any these fields is personally identifiable information, as defined in ANSI/NEMA HN 1-2019, the System has the capability to remove such information upon export.		
Note 29	The System is not intended to maintain long term primary storage of data. See the System Operator's Manual for data archiving guidance.		
Note 30	If a System is believed to be impacted by malware, please contact the BIOFIRE Technical Support team for assistance.		
Note 31	Operating system and security event auditing utilizes Windows logging features.		
Note 32	Installation and maintenance of antivirus, intrusion detection, and other detection/prevention systems is the responsibility of the end user.		
Note 33	Certificate-based network connection authentication may be utilized through the Windows Operating System.		
Note 34	Reference the System Operator's Manual for the System's hardware connectivity capabilities.		
Note 35	Reference the System Operator's Manual for details on the System's available USB ports.		
Note 36	Reference the System Operator's Manual for details on the System's capability to use or support removable memory devices.		
Note 37	If optional connectivity features are enabled, the System may communicate with other systems within the customer environment but does not communicate with other SPOTFIRE Systems.		
Note 38	The System only makes internal API calls.		
Note 39	Device operation requires all users to authenticate with a unique user ID/password combination or barcode number maintained through the application software. Windows user accounts may be separately used to access to the operating system, as follows: - Windows administrator-level accounts require authentication with a unique user ID/password combination - Windows user-level account requires a unique user ID only (no password)		
Note 40	Device operation requires all users to authenticate with a unique user ID/password combination or barcode number maintained through the application software. Windows user accounts may be separately used to access to the operating system, as follows: - Windows administrator-level accounts require authentication with a unique user ID/password combination - Windows user-level account requires a unique user ID only (no password)		

BIOFIRE Diagnostics, LLC	BIOFIRE® SPOTFIRE® SYSTEM	BFR0001-8102-01	22-Feb-2023
Note 41	The system application software (SPOTFIRE) enforces user account passwords that meet established complexity rules. The Windows administrator-level accounts do not enforce user account passwords that meet established complexity rules.		
Note 42	The system application software (SPOTFIRE) allows an admin operator to optionally enable barcode badge access which can be used by all operators. When enabled, all operators can associate a unique barcode that can be used for their authentication.		
Note 43	To the extent that the System maintains personally identifiable information, such information is physically secure. (See **Note 2** for additional information on the System's ability to maintain patient identifiable information)		
Note 44	To the extent that the System maintains personally identifiable information, such information is physically secure, but is not behind an individually keyed locking device. (See **Note 2** for additional information on the System's ability to maintain patient identifiable information)		
Note 45	The software was developed in accordance with IEC 62304.		
Note 46	Quality Assurance processes conducted during the System's assembly ensure the installed software is manufacturer authorized.		
Note 47	The Microsoft Windows Operating System "BMX_Guest" account is disabled by default.		
Note 48	The System is configured to block inbound connection requests on all network ports. However, if optional connectivity features are enabled, outbound connections are allowed on any available network port (1-65535). No port exclusions are currently configured.		
Note 49	The system uses a modified Windows 10 IoT Enterprise 2019 LTSC Version 1809 image which includes deleting and/or disabling many features that are not required for the intended use of the device.		
Note 50	If you have any questions or concerns about system hardening beyond the default state, please contact the BIOFIRE Technical Support team for assistance.		
Note 51	If you have any questions or concerns about system hardening beyond the default state, please contact the BIOFIRE Technical Support team for assistance.		
Note 52	Department of Defense's Security Technical Implementation Guides have been used to harden the Microsoft Windows Operating System.		
Note 53	The SPOTFIRE application software has a Factory Reset feature that will remove all data from the system.		
Note 54	Windows operating system accounts are not documented. SPOTFIRE application software role-based access accounts are documented in the Operators Manual.		
Note 55	The SPOTFIRE application software allows admin operators to manage password control. The SPOTFIRE application software cannot make changes directly to the Windows OS accounts. If the 'Switch to Windows OS' is used the owner then has access to manage password control for the Windows accounts.		
Note 56	Data protection mechanisms in place on the system include password protection of the local databases, anonymization of the run data when exporting anonymously, the use of API keys protecting our services, and data bundle creation.		
Note 57	Data is encrypted prior to transmission via removable media. If the System's optional connectivity features are enabled, data is not encrypted prior to transmission through the optional connectivity features, the removable media encryption remains the same.		
Note 58	If optional connectivity features are enabled, operator profiles and software settings can be remotely configured.		