Manufacturer Disclosure Statement for Medical Device Security – MDS^2

DEVICE DESCRIPTION

Device Category	Manufacturer	Document ID	Document Release Date
IVD Class II	BioFire Diagnostics, LLC	FLM2-PRT-0268-05	June 15th 2020

Device Model	Software Revision	Software Release Date
BioFire® FilmArray® 2.0	Version 2	January 8th 2015

	Company Name	Manufacturer Contact Information
Manufacturer or Representative Contact Information	BioFire Diagnostics, LLC	www.biofiredx.com/support Phone: 800-735-6544
	Representative Name/Position Customer Technical Support	

Intended use of **device** in network-connected environment:

The FilmArray 2.0 System is an automated in vitro diagnostic (IVD) device. The FilmArray 2.0 System is intend for use in combination with assay specific reagent pouches to detect multiple nucleic acid targets contained in clinical specimens. The FilmArray 2.0 instrument interacts with the reagent pouch to both purify nucleic acids and amplify targeted nucleic acid sequences using nested multiplex PCR (nmPCR) in a closed system. The resulting PCR products are evaluated using DNA melting analysis. The FilmArray software automatically determines the results and provides a test report.

The FilmArray 2.0 System is composed of one to eight FilmArray 2.0 instruments connected to a computer running FilmArray software. The FilmArray software controls the function of each instrument and collects, analyzes, and stores data generated by each instrument.

Two optional connectivity software products are available for the FilmArray 2.0 System, FilmArray® Link Software and the BioFire® Syndromic Trends Connector. The intended use of the FilmArray Link Software with the FilmArray 2.0 System (referred to as "the System" throughout the document) in a network-connected environment is restricted to interfacing with a laboratory information system (LIS). The FilmArray Link Software facilitates the unidirectional transfer of data from the System to an LIS. The System does not access, pull, or retrieve any information from the LIS. A wired Ethernet connection from the System to the local area network (LAN) at the facility is required. Data are transferred using either shared folder protocol (SMB), file transfer protocol (FTP), or Hypertext Transfer Protocol (HTTP/HTTPS).

The second optional connectivity software that can be installed on the System is the BioFire Syndromic Trends Connector. This software requires an internet connection to perform an encrypted outbound transfer of de-identified, aggregated System test data to the cloud hosted BioFire Syndromic Trends service. This data transfer can be restricted to a pre-defined BioFire endpoint. Additional information can be provided upon request.

MANAGEMENT OF PRIVATE DATA

	Refer to Section 2.3.2 of this standard for the proper interpretation of information requested in this form.	Yes, No, N/A, or See Note	Note #
A	Can this **device** display, transmit, or maintain **private data** (including **electronic Protected Health Information** [ePHI])?	No	1
B	Types of **private data** elements that can be maintained by the **device**:		
	B.1 Demographic (e.g., name, address, location, unique identification number)?	N/A	
	B.2 Medical record (e.g., medical record #, account #, test or treatment date, **device** identification number)?	N/A	
	B.3 Diagnostic/therapeutic (e.g., photo/radiograph, test results, or physiologic data with identifying characteristics)?	N/A	
	B.4 Open, unstructured text entered by **device user/operator**?	N/A	
	B.5 **Biometric data**?	N/A	
	B.6 Personal financial information?	N/A	
C	Maintaining **private data** - Can the **device**:		
	C.1 Maintain **private data** temporarily in volatile memory (i.e., until cleared by power-off or reset)?	N/A	
	C.2 Store **private data** persistently on local media?	N/A	
	C.3 Import/export **private data** with other systems?	N/A	
	C.4 Maintain **private data** during power service interruptions?	N/A	
D	Mechanisms used for the transmitting, importing/exporting of **private data** – Can the **device**:		
	D.1 Display private data (e.g., video display, etc.)?	N/A	
	D.2 Generate hardcopy reports or images containing **private data**?	N/A	

D.3	Retrieve **private data** from or record **private data** to **removable media** (e.g., disk, DVD, CD-ROM, tape, CF/SD card, memory stick, etc.)?	N/A
D.4	Transmit/receive or import/export **private data** via dedicated cable connection (e.g., IEEE 1073, serial port, USB, FireWire, etc.)?	N/A
D.5	Transmit/receive **private data** via a wired network connection (e.g., LAN, WAN, VPN, intranet, Internet, etc.)?	N/A
D.6	Transmit/receive **private data** via an integrated wireless network connection (e.g., WiFi, Bluetooth, infrared, etc.)?	N/A
D.7	Import **private data** via scanning?	N/A
D.8	Other?	N/A

Management of Private Data notes:

Note 1: If Customers follow BioFire's guidance to only use sequentially generated recycled accession numbers in the free text "Sample ID" field, no Protected Health Information ("PHI") as defined by the Health Insurance and Portability and Accountability Act ("HIPAA") is requested, required, displayed, transmitted, or maintained on the device. 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.

Device Category	Manufacturer	Document ID	Document Release Date
IVD Class II	BioFire Diagnostics, LLC	FLM2-PRT-0268-05	June 15th 2020
Device Model	**Software Revision**		**Software Release Date**
BioFire® FilmArray® 2.0	Version 2		January 8th 2015

SECURITY CAPABILITIES

	Refer to Section 2.3.2 of this standard for the proper interpretation of information requested in this form.	Yes, No, N/A, or See Note	Note #
1	**AUTOMATIC LOGOFF (ALOF)**		
	The **device**'s ability to prevent access and misuse by unauthorized **users** if **device** is left idle for a period of time.		
1-1	Can the **device** be configured to force reauthorization of logged-in **user**(s) after a predetermined length of inactivity (e.g., auto-logoff, session lock, password protected screen saver)?	No	
1-1.1	Is the length of inactivity time before auto-logoff/screen lock **user** or administrator configurable? (Indicate time [fixed or configurable range] in notes.)	N/A	
1-1.2	Can auto-logoff/screen lock be manually invoked (e.g., via a shortcut key or proximity sensor, etc.) by the **user**?	N/A	
ALOF notes:	N/A		
2	**AUDIT CONTROLS (AUDT)**		
	The ability to reliably audit activity on the **device**.		
2-1	Can the **medical device** create an **audit trail**?	No	1
2-2	Indicate which of the following events are recorded in the audit log:		
2-2.1	Login/logout	N/A	
2-2.2	Display/presentation of data	N/A	
2-2.3	Creation/modification/deletion of data	N/A	
2-2.4	Import/export of data from **removable media**	N/A	
2-2.5	Receipt/transmission of data from/to external (e.g., network) connection	N/A	
2-2.5.1	**Remote service** activity	N/A	
2-2.6	Other events? (describe in the notes section)	N/A	
2-3	Indicate what information is used to identify individual events recorded in the audit log:		
2-3.1	**User** ID	N/A	
2-3.2	Date/time	N/A	
AUDT notes:	Note 1: The System does not create a full audit trail, but does utilize Windows Event logs for logon events. The System computer is hardened with several DoD STIGs.		
3	**AUTHORIZATION (AUTH)**		
	The ability of the device to determine the authorization of users.		
3-1	Can the **device** prevent access to unauthorized **users** through **user** login requirements or other mechanism?	No	1
3-2	Can **users** be assigned different privilege levels within an application based on 'roles' (e.g., guests, regular **users**, power **users**, administrators, etc.)?	No	
3-3	Can the **device** owner/**operator** obtain unrestricted administrative privileges (e.g., access operating system or application via local root or admin account)?	Yes	2
AUTH notes:	Note 1: The System computer is pre-configured to automatically log on to the Windows OS with the FilmArray user account. The FilmArray user account is a Windows Standard User. Note 2: The System is pre-configured with an administrative user account. It is recommended the device owner/operator change the default password for the LabAdmin user account.		

Device Category	Manufacturer	Document ID	Document Release Date
IVD Class II	BioFire Diagnostics, LLC	FLM2-PRT-0268-05	June 15th 2020
Device Model	**Software Revision**		**Software Release Date**
BioFire® FilmArray® 2.0	Version 2		January 8th 2015

	Refer to Section 2.3.2 of this standard for the proper interpretation of information requested in this form.	Yes, No, N/A, or See Note	Note #
4	**CONFIGURATION OF SECURITY FEATURES (CNFS)**		
	The ability to configure/re-configure **device security capabilities** to meet **users'** needs.		
4-1	Can the **device** owner/operator reconfigure product **security capabilities**?	See Note	1
CNFS notes:	Note 1: For additional information about cybersecurity management and procedures (including patch management, antivirus software installation, software updates), please contact BioFire Diagnostics Customer Technical Support.		
5	**CYBER SECURITY PRODUCT UPGRADES (CSUP)**		
	The ability of on-site service staff, remote service staff, or authorized customer staff to install/upgrade **device**'s security patches.		
5-1	Can relevant OS and **device** security patches be applied to the **device** as they become available?	See Note	1
5-1.1	Can security patches or other software be installed remotely?	N/A	
CSUP notes:	Note 1: For additional information about cybersecurity management and procedures (including patch management, antivirus software installation, software updates), please contact BioFire Diagnostics Customer Technical Support.		
6	**HEALTH DATA DE-IDENTIFICATION (DIDT)**		
	The ability of the **device** to directly remove information that allows identification of a person.		
6-1	Does the **device** provide an integral capability to de-identify **private data**?	N/A	
DIDT notes:	N/A		
7	**DATA BACKUP AND DISASTER RECOVERY (DTBK)**		
	The ability to recover after damage or destruction of **device** data, hardware, or software.		
7-1	Does the **device** have an integral data backup capability (i.e., backup to remote storage or **removable media** such as tape, disk)?	No	1
DTBK notes:	Note 1: The System is not configured to automatically backup the hard drive. The System has the ability to archive test data to removable media. This process must be initiated and completed manually by the operator.		
8	**EMERGENCY ACCESS (EMRG)**		
	The ability of **device users** to access **private data** in case of an emergency situation that requires immediate access to stored **private data**.		
8-1	Does the **device** incorporate an **emergency access** ("break-glass") feature?	N/A	
EMRG notes:	N/A		
9	**HEALTH DATA INTEGRITY AND AUTHENTICITY (IGAU)**		
	How the **device** ensures that data processed by the **device** has not been altered or destroyed in an unauthorized manner and is from the originator.		
9-1	Does the **device** ensure the integrity of stored data with implicit or explicit error detection/correction technology?	No	
IGAU notes:	N/A		

Device Category	Manufacturer	Document ID	Document Release Date
IVD Class II	BioFire Diagnostics, LLC	FLM2-PRT-0268-05	June 15th 2020
Device Model	**Software Revision**		**Software Release Date**
BioFire® FilmArray® 2.0	Version 2		January 8th 2015

	Refer to Section 2.3.2 of this standard for the proper interpretation of information requested in this form.	Yes, No, N/A, or See Note	Note #
10	**MALWARE DETECTION/PROTECTION (MLDP)**		
	The ability of the **device** to effectively prevent, detect and remove malicious software (**malware**).		
10-1	Does the **device** support the use of **anti-malware** software (or other **anti-malware** mechanism)?	See Note	1
10-1.1	Can the **user** independently re-configure **anti-malware** settings?	See Note	1
10-1.2	Does notification of **malware** detection occur in the **device user** interface?	See Note	1
10-1.3	Can only manufacturer-authorized persons repair systems when **malware** has been detected?	See Note	1
10-2	Can the device owner install or update **anti-virus software**?	Yes	1
10-3	Can the device owner/**operator** (technically/physically) update virus definitions on manufacturer-installed **anti-virus software**?	Yes	1
MLDP notes:	Note 1: The System is not pre-configured with specific antimalware/antivirus software. If antimalware/antivirus software, or third party organizational software is installed onto the System, it is the responsiblity of the owner/operator to install the software and verify proper functionality of the System.		
11	**NODE AUTHENTICATION (NAUT)**		
	The ability of the **device** to authenticate communication partners/nodes.		
11-1	Does the **device** provide/support any means of node authentication that assures both the sender and the recipient of data are known to each other and are authorized to receive transferred information?	No	
NAUT notes:	N/A		
12	**PERSON AUTHENTICATION (PAUT)**		
	Ability of the **device** to authenticate **users**		
12-1	Does the **device** support **user/operator**-specific username(s) and password(s) for at least one **user**?	No	1
12-1.1	Does the device support unique **user/operator**-specific IDs and passwords for multiple users?	N/A	
12-2	Can the **device** be configured to authenticate **users** through an external authentication service (e.g., MS Active Directory, NDS, LDAP, etc.)?	No	
12-3	Can the **device** be configured to lock out a **user** after a certain number of unsuccessful logon attempts?	No	
12-4	Can default passwords be changed at/prior to installation?	Yes	2
12-5	Are any shared **user** IDs used in this system?	Yes	1
12-6	Can the **device** be configured to enforce creation of **user** account passwords that meet established complexity rules?	Yes	2
12-7	Can the **device** be configured so that account passwords expire periodically?	No	
PAUT notes:	Note 1: All operators access the System through the same Windows user account. Note 2: BioFire Diagnostics recommends the owner/operator change the default password to the LabAdmin administrator account. The System is pre-configured to enforce complexity rules for administrative access.		
13	**PHYSICAL LOCKS (PLOK)**		
	Physical locks can prevent unauthorized **users** with physical access to the **device** from compromising the integrity and confidentiality of **private data** stored on the **device** or on **removable media**.		
13-1	Are all **device** components maintaining **private data** (other than **removable media**) physically secure (i.e., cannot remove without tools)?	N/A	
PLOK notes:	N/A		

Device Category	Manufacturer	Document ID	Document Release Date
IVD Class II	BioFire Diagnostics, LLC	FLM2-PRT-0268-05	June 15th 2020
Device Model	**Software Revision**		**Software Release Date**
BioFire® FilmArray® 2.0	Version 2		January 8th 2015

	Refer to Section 2.3.2 of this standard for the proper interpretation of information requested in this form.	Yes, No, N/A, or See Note	Note #
14	**ROADMAP FOR THIRD PARTY COMPONENTS IN DEVICE LIFE CYCLE (RDMP)**		
	Manufacturer's plans for security support of 3rd party components within **device** life cycle.		
14-1	In the notes section, list the provided or required (separately purchased and/or delivered) operating system(s) - including version number(s).	See Note	1
14-2	Is a list of other third party applications provided by the manufacturer available?	Yes	
RDMP notes:	Note 1: The System computer is delivered with Windows 10 Enterprise IoT LTSC version 1809 64-bit operating system pre-installed.		
15	**SYSTEM AND APPLICATION HARDENING (SAHD)**		
	The **device**'s resistance to cyber attacks and **malware**.		
15-1	Does the **device** employ any hardening measures? Please indicate in the notes the level of conformance to any industry-recognized hardening standards.	Yes	1
15-2	Does the **device** employ any mechanism (e.g., release-specific hash key, checksums, etc.) to ensure the installed program/update is the manufacturer-authorized program or software update?	No	
15-3	Does the **device** have external communication capability (e.g., network, modem, etc.)?	Yes	
15-4	Does the file system allow the implementation of file-level access controls (e.g., New Technology File System (NTFS) for MS Windows platforms)?	Yes	2
15-5	Are all accounts which are not required for the **intended use** of the **device** disabled or deleted, for both **users** and applications?	Yes	
15-6	Are all shared resources (e.g., file shares) which are not required for the **intended use** of the **device**, disabled?	No	
15-7	Are all communication ports which are not required for the **intended use** of the **device** closed/disabled?	No	
15-8	Are all services (e.g., telnet, file transfer protocol [FTP], internet information server [IIS], etc.), which are not required for the **intended use** of the **device** deleted/disabled?	No	
15-9	Are all applications (COTS applications as well as OS-included applications, e.g., MS Internet Explorer, etc.) which are not required for the **intended use** of the **device** deleted/disabled?	No	
15-10	Can the **device** boot from uncontrolled or **removable media** (i.e., a source other than an internal drive or memory component)?	Yes	
15-11	Can software or hardware not authorized by the **device** manufacturer be installed on the device without the use of tools?	Yes	
SAHD notes:	Note 1: The System computer is hardened with several DoD STIGs. Note 2: The System hard drive is formatted NTFS and managed by the Windows OS.		
16	**SECURITY GUIDANCE (SGUD)**		
	The availability of security guidance for **operator** and administrator of the system and manufacturer sales and service.		
16-1	Are security-related features documented for the **device user**?	No	
16-2	Are instructions available for **device**/media sanitization (i.e., instructions for how to achieve the permanent deletion of personal or other sensitive data)?	No	
SGUD notes:	N/A		

Device Category	Manufacturer	Document ID	Document Release Date
IVD Class II	BioFire Diagnostics, LLC	FLM2-PRT-0268-05	June 15th 2020
Device Model	**Software Revision**		**Software Release Date**
BioFire® FilmArray® 2.0	Version 2		January 8th 2015

	Refer to Section 2.3.2 of this standard for the proper interpretation of information requested in this form.	Yes, No, N/A, or See Note	Note #
17	**HEALTH DATA STORAGE CONFIDENTIALITY (STCF)**		
	The ability of the **device** to ensure unauthorized access does not compromise the integrity and confidentiality of **private data** stored on **device** or **removable media**.		
17-1	Can the **device** encrypt data at rest?	N/A	
STCF notes:	N/A		
18	**TRANSMISSION CONFIDENTIALITY (TXCF)**		
	The ability of the **device** to ensure the confidentiality of transmitted **private data**.		
18-1	Can **private data** be transmitted only via a point-to-point dedicated cable?	N/A	
18-2	Is **private data** encrypted prior to transmission via a network or **removable media**? (If yes, indicate in the notes which encryption standard is implemented.)	N/A	
18-3	Is **private data** transmission restricted to a fixed list of network destinations?	N/A	
TXCF notes:	N/A		
19	**TRANSMISSION INTEGRITY (TXIG)**		
	The ability of the **device** to ensure the integrity of transmitted **private data**.		
19-1	Does the **device** support any mechanism intended to ensure data is not modified during transmission? (If yes, describe in the notes section how this is achieved.)	N/A	
TXIG notes:	N/A		
20	**OTHER SECURITY CONSIDERATIONS (OTHR)**		
	Additional security considerations/notes regarding **medical device** security.		
20-1	Can the **device** be serviced remotely?	No	
20-2	Can the **device** restrict remote access to/from specified devices or **users** or network locations (e.g., specific IP addresses)?	N/A	
20-2.1	Can the **device** be configured to require the local **user** to accept or initiate remote access?	N/A	
OTHR notes:	N/A		