Manufacturer Disclosure Statement for Medical Device Security – MDS^2

DEVICE DESCRIPTION

Device Category Software Medical Device	Manufacturer ImPACT Applications, Inc.	Document ID QR-16-18	Document Release Date 2/10/22
Device Model ImPACT Customer Center ImPACT/ImPACT Pediatric/ImPACT Quick Test / Cognitive Impairment Screener	Software Revision 2.35.0 4.0 / 1.3 / 2.0 / 1.0		Software Release Date N/A

Manufacturer or Representative Contact Information	Company Name ImPACT Applications, Inc.	Manufacturer Contact Information 2140 Norcor Ave, Ste 150 Coralville, IA 52241
	Representative Name/Position Shawn Maceno, CTO	

Intended use of **device** in network-connected environment:
Computerized cognitive assessment aid for concussion.

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])?	Yes	__
B		Types of **private data** elements that can be maintained by the **device**:		
	B.1	Demographic (e.g., name, address, location, unique identification number)?	Yes	__
	B.2	Medical record (e.g., medical record #, account #, test or treatment date, **device** identification number)?	Yes	__
	B.3	Diagnostic/therapeutic (e.g., photo/radiograph, test results, or physiologic data with identifying characteristics)?	Yes	__
	B.4	Open, unstructured text entered by **device user/operator**?	No	__
	B.5	**Biometric data**?	No	__
	B.6	Personal financial information?	No	__
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)?	Yes	__
	C.2	Store **private data** persistently on local media?	Yes	1
	C.3	Import/export **private data** with other systems?	Yes	2
	C.4	Maintain **private data** during power service interruptions?	Yes	10
D		Mechanisms used for the transmitting, importing/exporting of **private data** – Can the **device**:		
	D.1	Display private data (e.g., video display, etc.)?	Yes	__
	D.2	Generate hardcopy reports or images containing **private data**?	Yes	__
	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.)?	No	__
	D.4	Transmit/receive or import/export **private data** via dedicated cable connection (e.g., IEEE 1073, serial port, USB, FireWire, etc.)?	No	__
	D.5	Transmit/receive **private data** via a wired network connection (e.g., LAN, WAN, VPN, intranet, Internet, etc.)?	Yes	__
	D.6	Transmit/receive **private data** via an integrated wireless network connection (e.g., WiFi, Bluetooth, infrared, etc.)?	Yes	__
	D.7	Import **private data** via scanning?	No	__
	D.8	Other?	N/A	__

Management of Private Data notes:

1. Any PHI stored on local or removable media is done so by the end user.
2. Data can be manually exported in CSV format by authorized users with system mangement permission. The Company does not directly interface with other systems or automatically export or import any data.
10. The datacenters housing our systems employ redundant UPS, redundant deisel generators, redundant HVAC systems, fire supression, audio & video surveilance and redundant network providers to ensure the highest availability for our systems.

Device Category	Manufacturer	Document ID	Document Release Date
Software Medical Device	ImPACT Applications, Inc.	QR-16-18	44602
Device Model	Software Revision		Software Release Date
ImPACT Customer Center	2.35.0		N/A
ImPACT/ImPACT	4.0 / 1.3 / 2.0 / 1.0		
Pediatric/ImPACT Quick Test /			

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)?	Yes	__
	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.)	No	7
	1-1.2 Can auto-logoff/screen lock be manually invoked (e.g., via a shortcut key or proximity sensor, etc.) by the **user**?	No	__
ALOF notes:	7. The ImPACT Customer Center will log out a user after 20 minutes of idle time. The mobile applications will log out when the application is closed.		
2	**AUDIT CONTROLS (AUDT)** The ability to reliably audit activity on the **device**.		
2-1	Can the **medical device** create an **audit trail**?	Yes	__
2-2	Indicate which of the following events are recorded in the audit log:		
	2-2.1 Login/logout	Yes	8
	2-2.2 Display/presentation of data	Yes	8
	2-2.3 Creation/modification/deletion of data	Yes	8
	2-2.4 Import/export of data from **removable media**	Yes	8
	2-2.5 Receipt/transmission of data from/to external (e.g., network) connection	Yes	8
	2-2.5.1 **Remote service** activity	Yes	__
	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	Yes	__
	2-3.2 Date/time	Yes	__
AUDT notes:	8. All access to or modification of PHI is logged in the application's activity log in a date-stampped entry.		
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?	Yes	__
3-2	Can **users** be assigned different privilege levels within an application based on 'roles' (e.g., guests, regular **users**, power **users**, administrators, etc.)?	Yes	__
3-3	Can the **device** owner/**operator** obtain unrestricted administrative privileges (e.g., access operating system or application via local root or admin account)?	No	__
AUTH notes:			

Device Category Software Medical Device	Manufacturer ImPACT Applications, Inc.	Document ID QR-16-18	Document Release Date 44602
Device Model ImPACT Customer Center ImPACT/ImPACT Pediatric/ImPACT Quick Test /	Software Revision 2.35.0 4.0 / 1.3 / 2.0 / 1.0		Software Release Date N/A

	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**?	Yes	16
CNFS notes:	16. Several items allow customization for system administrators, including password age, and user permissions.		
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?	Yes	__
	5-1.1 Can security patches or other software be installed remotely?	Yes	6
CSUP notes:	6. End users are encouraged to maintain their computers in a manner consistent with their IT department policies, including installing appropriate operating system patches, antivirus/antimalware software and definition updates, and other precautions to ensure a safe computing environment.		
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**?	Yes	__
DIDT notes:			
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)?	Yes	4
DTBK notes:	4. All data is backed up hourly, stored in an encrypted format in multiple secure locations for redundancy.		
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?	No	9
EMRG notes:	9. A "break glass" feature doesn't exist in our software.		
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?	Yes	12
IGAU notes:	12. Standard input validations are performed on input forms to make sure the entries are appropriate for the data expected (numbers within an intended range, dates within correct ranges, text fields validated and checked for proper formatting and exclusion of invalid characters or malicious commands). Through our application validations we have verified that the data provided by the test taker is transmitted properly to the servers for storage, and reported as expected on the reports generated by the product.		

Device Category	Manufacturer	Document ID	Document Release Date
Software Medical Device	ImPACT Applications, Inc.	QR-16-18	44602
Device Model	Software Revision		Software Release Date
ImPACT Customer Center ImPACT/ImPACT Pediatric/ImPACT Quick Test /	2.35.0 4.0 / 1.3 / 2.0 / 1.0		N/A

	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)?	N/A	6
	10-1.1 Can the **user** independently re-configure **anti-malware** settings?	N/A	6
	10-1.2 Does notification of **malware** detection occur in the **device user** interface?	N/A	6
	10-1.3 Can only manufacturer-authorized persons repair systems when **malware** has been detected?	N/A	6
10-2	Can the device owner install or update **anti-virus software**?	N/A	6
10-3	Can the device owner/**operator** (technically/physically) update virus definitions on manufacturer-installed **anti-virus software**?	N/A	6
MLDP notes:	6. End users are encouraged to maintain their computers in a manner consistent with their IT department policies, including installing appropriate operating system patches, antivirus/antimalware software and definition updates, and other precautions to ensure a safe computing environment.		
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?	Yes	__
NAUT notes:	The ImPACT system uses HTTPS to negotiate a secure tunnel from the end-user's browser to our systems to ensure proper encryption and security of data.		
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**?	Yes	__
	12-1.1 Does the device support unique **user/operator**-specific IDs and passwords for multiple users?	Yes	__
12-2	Can the **device** be configured to authenticate **users** through an external authentication service (e.g., MS Active Directory, NDS, LDAP, etc.)?	Yes	18
12-3	Can the **device** be configured to lock out a **user** after a certain number of unsuccessful logon attempts?	Yes	19
12-4	Can default passwords be changed at/prior to installation?	Yes	__
12-5	Are any shared **user** IDs used in this system?	No	__
12-6	Can the **device** be configured to enforce creation of **user** account passwords that meet established complexity rules?	Yes	__
12-7	Can the **device** be configured so that account passwords expire periodically?	Yes	__
PAUT notes:	18. Customers can configure SAML 2.0 based SSO to integrate with their authentication environment. 19. 5 failed logins cause an account to be locked out for 60 minutes from the most recent failed login attempt.		
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)?	Yes	3
PLOK notes:	3. All servers are on a private network, in a locked cabinet, in a secure datacenter facility.		

Device Category Software Medical Device	Manufacturer ImPACT Applications, Inc.	Document ID QR-16-18	Document Release Date 44602
Device Model ImPACT Customer Center ImPACT/ImPACT Pediatric/ImPACT Quick Test /	Software Revision 2.35.0 4.0 / 1.3 / 2.0 / 1.0		Software Release Date N/A

	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	15
14-2	Is a list of other third party applications provided by the manufacturer available?	Yes	__

RDMP notes: 15. System utilizes CentOS 7 operating system.

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	13
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?	Yes	__
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	__
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?	Yes	__
15-7	Are all communication ports which are not required for the **intended use** of the **device** closed/disabled?	Yes	__
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?	Yes	__
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?	Yes	__
15-10	Can the **device** boot from uncontrolled or **removable media** (i.e., a source other than an internal drive or memory component)?	No	__
15-11	Can software or hardware not authorized by the **device** manufacturer be installed on the device without the use of tools?	No	__

SAHD notes: 13. The Company has created standard server build sheets that are followed when creating and setting up an environment and the servers therin. We use the CentOS 'minimal install' method and only install packages that are required for servers desired function. All servers have a host-based intrusion detection system installed and configured to notify the Company system administrators immediately of any anomalies.

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**?	Yes	__
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)?	Yes	__

SGUD notes:

Device Category	Manufacturer	Document ID	Document Release Date
Software Medical Device	ImPACT Applications, Inc.	QR-16-18	44602
Device Model	Software Revision		Software Release Date
ImPACT Customer Center ImPACT/ImPACT Pediatric/ImPACT Quick Test /	2.35.0 4.0 / 1.3 / 2.0 / 1.0		N/A

	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?	Yes	17
STCF notes:	17. Data is encrypted using AES-128 bit encryption in the database.		
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?	No	11
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.)	Yes	11
18-3	Is **private data** transmission restricted to a fixed list of network destinations?	No	11
TXCF notes:	11. Our system doesn't share PHI externally. Any electronic reports saved are done by the end user, stored in a location of their choice. It is the responsibility of the end user to ensure the security of the data when saved to their computer. Data transmitted from the end-user's browser to our servers is done via HTTPS secured connection.		
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.)	Yes	14
TXIG notes:	HTTPS by nature does not allow the modification of encrypted traffic.		
20	**OTHER SECURITY CONSIDERATIONS (OTHR)** Additional security considerations/notes regarding **medical device** security.		
20-1	Can the **device** be serviced remotely?	Yes	5
20-2	Can the **device** restrict remote access to/from specified devices or **users** or network locations (e.g., specific IP addresses)?	Yes	__
	20-2.1 Can the **device** be configured to require the local **user** to accept or initiate remote access?	No	__
OTHR notes:	5. As our application is SaaS, the "device" is served from a set of servers in a secure datacenter facility. Our system administrators use remote access VPN with two-factor authentication to access theses servers, perform patches and updates, and deploy updated software to the environment.		