4.1 MD-VIPER Vulnerability Report (with data descriptions and source)

No	Question	Data Definition	Source
1	Report Number (includes 7 digit manufacturer registration number)	The seven digit registration number of the entity responsible for submission of the report of corrective or removal action (if applicable), the month, day, and year that the report is made, and a sequence number (i.e., 001 for the first report, 002 for the second report, 003 etc.), and the report type designation "C" or "R". For example, the complete number for the first correction report submitted on June 1, 1997, will appear as follows for a firm with the registration number 1234567: 1234567-6/1/97-001-C. The second correction report number submitted by the same firm on July 1, 1997, would be 1234567-7/1/97-002-C etc. For removals, the number will appear as follows: 1234567-6/1/97-001-R and 1234567-7/1/97-002-R, etc. Firms that do not have a seven digit registration number may use seven zeros followed by the month, date, year, and sequence number (i.e. 0000000-6/1/97-001-C for corrections and 0000000-7/1/97-001-R for removals). Reports received without a seven digit registration number will be assigned a seven digit central file number by the district office reviewing the reports	FDA Part 806
2	Name, address and telephone number	The name, address, and telephone number of the manufacturer or importer, and the name, title, address, and telephone number of the manufacturer or importer representative responsible for conducting the device correction or removal.	FDA Part 806
3	FDA Classification name of the device	The brand name and the common name, classification name, or usual name of the device and the intended use of the device	FDA Part 806
4	Marketing status	Marketing status of the device, i.e., any applicable *premarket notification number* (*510(k)*), *premarket approval (PMA) number*, or *indication that the device is a preamendment device*, and the *device listing number*. A manufacturer or importer that does not have an FDA establishment registration number shall indicate in the report whether it has ever registered with FDA	FDA Part 806
5	unique device identifier (UDI)	The unique device identifier (UDI) that appears on the device label or on the device package, or the device identifier, universal product code (UPC), model, catalog, or code number of the device and the manufacturing lot or serial number of the device or other identification number.	FDA Part 806
6	Manufacturer	The manufacturer's name, address, telephone number, and contact person if different from that of the person submitting the report.	FDA Part 806
7	Description	A description of	FDA Part 806
7.a.	Description of vulnerability found or exploited	Detailed description of vulnerability of exploit	
7.b.	Device configuration	Basic device configuration	
7.b.i.	Operating System	Operating System (including version and patches, etc.)	US-CERT
7.b.ii.	Application(s)	Applications (including version and patches, etc.)	US-CERT
7.b.iii	System function	System function (e.g., diagnostic, therapeutic, clinical workstation, etc.)	US-CERT
7.b.iv	Anti-Malware	Anti-Malware software installed (including version and latest updates)	US-CERT
7.b.v	Device/System location	System location (city, state, address, building, room, connection point(s))	US-CERT

4.1 MD-VIPER Vulnerability Report (with data descriptions and source)

No	Question	Data Definition	Source
7.c.	Cybersecurity Signals (complete only relevant sections of 7.a.)	Any cybersecurity signals (i.e., any information which indicates the potential for, or confirmation of, a cybersecurity vulnerability or exploit that affects, or could affect a medical device) including details of	
7.c.i	Underlying Event of Incident (complete relevant portions of section 7.a.i if the cybersecurity signal was an event)	Description of any underlying event or incident	
7.c.i. (1)	Event or Incident Category	CAT 1 – Unauthorized Access In this category, some individual gains logical or physical access without permission to a network, system, application, data, or other resource	US-CERT
		CAT 2 – Denial of Service (DoS) An attack that *successfully* prevents or impairs the normal authorized functionality of networks, systems or applications by exhausting resources. This activity includes being the victim or participating in the DoS.	US-CERT
		CAT 3 – Malicious Code *Successful* installation of malicious software (e.g., virus, worm, Trojan horse, or other code-based malicious entity) that infects an operating system or application. It is NOT necessary to report malicious logic that has been *successfully quarantined* by antivirus (AV) software	US-CERT
		CAT 4 – Improper Usage A person violates acceptable computing use policies.	US-CERT
		CAT 5 – Scans /Probes / Attempted Access This category includes any activity that seeks to access or identify a computer, open ports, protocols, service, or any combination for later exploit. This activity does not directly result in a compromise or denial of service.	US-CERT
		CAT 6 – Investigation *Unconfirmed* incidents that are potentially malicious or anomalous activity deemed by the reporting entity to warrant further review.	US-CERT
7.c.i. (2)	Date(s)/time(s)	Event/Incident date and time (including time zone)	US-CERT
7.c.i. (3)	Attack Vector	*Network (e.g., Ethernet, Bluetooth)*	slg
		Internet	slg
		Removable media (e.g., HDD, SSD, tape, USB devices, SD card)	slg
		I/O devices (e.g., keyboard, imaging)	slg
		Other	slg
7.c.i. (4)	Source	Source IP, port and protocol	US-CERT
7.c.i. (5)	Destination	Destination IP, port and protocol	US-CERT

4.1 MD-VIPER Vulnerability Report (with data descriptions and source)

No	Question	Data Definition	Source
7.c.i. (6)	Methods used to identify incident	Method used to identify incident (e.g., IDS, audit log analysis, system administrator)	US-CERT
7.c.i. (7)	Impact to organization	Degree of operational, financial, reputational impact (i.e., negligible, minor, serious, critical, catastrophic)	US-CERT
7.c.i. (8)	Impact to patients	Degree of impact to patients' safety and health (i.e., negligible, minor, serious, critical, catastrophic)	Slg
7.c.ii.	Analyses (complete section 7.a.ii if the cybersecurity signal was from an analysis)	Description of risk analyses & threat modeling, analyses of threat sources, threat detection, internal investigations / postmarket surveillance that led	Slg highlights from FDA Cyber Guide
7.c.iii.	Testing (complete section 7.a.iii if the cybersecurity signal was from a vulnerability testing)	Description of in-house vulnerability testing results (e.g., PEN testing)	slg highlights from FDA Cyber Guide
7.c.iv.	Reports (complete section 7.a.iv if the cybersecurity signal was from a 3rd party report)	Reports including those from 3rd party (e.g., service records, complaints, owner/user reports, hardware/software suppliers, security experts, ISAOs, etc.)	slg highlights from FDA Cyber Guide
7.c.v.	Other (complete section 7.a.v if the cybersecurity signal was from other)	Other	slg
7.d.	Vulnerability Score	Factors in determining exploitability of an identified medical device vulnerability	FDA vulnerability characterization & assessment
7.d.i	Attack Vector	Attack vector (physical, local, adjacent, network)	CVSS
7.d.ii	Attack complexity	Attack complexity (high, low)	CVSS
7.d.iii	Privileges required	Privileges required (none, low, required)	CVSS
7.d.iv	User interaction	User interaction (none, required)	CVSS
7.d.v	Scope	Scope (changed, unchanged)	CVSS
7.d.vi	Confidentiality Impact	Confidentiality Impact (high, low, none)	CVSS
7.d.vii	Integrity Impact	Integrity Impact (high, low, none)	CVSS
7.d.viii	Availability Impact	Availability Impact (high, low, none)	CVSS

4.1 MD-VIPER Vulnerability Report (with data descriptions and source)

No	Question	Data Definition	Source
7.d.ix	Exploit Code Maturity	Exploit Code Maturity (high, functional, proof-of-concept, unproven)	CVSS
7.d.x	Remediation Level	Remediation Level (unavailable, work-around, temporary fix, official fix, not defined)	CVSS
7.d.xi	Report Confidence	Report Confidence (confirmed, reasonable, unknown, not defined)	CVSS
7.e.	Actions taken (or to be taken)	Any corrective and removal actions that have been, and are expected to be taken	FDA Part 806
7.f.	Timeline		pe
7.f.i	Date mfg first learned	Date manufacturer first learned of vulnerability	pe
7.f.ii	Date mfg first communicated	Date manufacturer first communicated with customers and user community regarding vulnerability	pe
7.f.iii	Date mfg fixed	Date manufacturer fixed, validated fix and distributed fix to customers and user community	pe
8	Any illness or injuries that have occurred with use of the device (include medical device report number is applicable)	Any illness or injuries that have occurred with use of the device. If applicable, include the medical device report numbers.	FDA Part 806
9	Total number of devices	The total number of devices manufactured or distributed subject to the correction or removal and the number in the same batch, lot, or equivalent unit of production subject to the correction or removal.	FDA Part 806
10	Date of manufacture or distribution and the devices expiration date or expected life	The date of manufacture or distribution and the device's expiration date or expected life.	FDA Part 806
11	Names, addresses and phone numbers of all domestic and foreign consignees of device distributed to each such consignee	The names, addresses, and telephone numbers of all domestic and foreign consignees of the device and the dates and number of devices distributed to each such consignee.	FDA Part 806
12	Copy of all communication regarding the correction or removal	A copy of all communications regarding the correction or removal	FDA Part 806
13	If any required information is not	If any required information is not immediately available, a statement as to why it is not available and when it will be submitted.	FDA Part 806

4.1 MD-VIPER Vulnerability Report (with data descriptions and source)

No	Question	Data Definition	Source
	immediately available, a statement as to why and when it will be submitted		