IoMT Risk Analysis Report

u5539006

Introduction **2**
Critical Analysis of Research into the Use of IoMT Devices **3**
Risk Analysis of Named IoMT Devices **4**
Standards and Policies 4
Methodology 4
Scope 4
Contextual Responsibilities 5
Contextual Goals 5
Risk Assessment Components 6
Asset Ranking 6
Threat Identification 8
Vulnerability Identification 10
Risk Register 14
Risk Evaluation 18
Risk Control 18
Critical Evaluation of the Most Severe Risks 21
Attacker controls insulin delivery to patients 21
Hard-coded Credentials for Telnet 21
Attacker can steal passwords from configuration file 21
Critical Evaluation of the Top Vulnerabilities 22
Code Execution Vulnerability in NeuroWorks Version 8 22
Exposure of Sensitive Information from Signa HDx 22
Missing Authentication in Axeda Agent 23
Recommendations **24**
References **25**

Introduction

This document is composed of a brief review of research conducted into the use of IoMT (Internet of Medical Things) devices, followed by a comprehensive risk analysis and recommendations for one of the largest hospitals in the UK. The risk analysis is laid out in logical steps conforming to the structure outlined in ISO/IEC 27005:2018.

Critical Analysis of Research into the Use of IoMT Devices

It is clear that research into IoMT devices is split, mostly, into two sections: surveys and trends of implementation and usage, and security of these devices. It is generally agreed that they are a wonderful addition to healthcare treatment to “enhance precision, reliability, consistency and productivity” (Mathkor et al., 2024), but the papers focusing on implementation and usage generally have a small sample size or are entirely theoretical.
The papers that are focused on security conclude that due to the widespread usage and quick adoption of these devices (particularly during the COVID-19 pandemic) has left many exposed vulnerabilities because of the lack of bespoke protocols for communication and rushed deployment (Ghubaish et al., 2021)

Razdan, S. & Sharna S., 2021 covers suggested methods of implementing IoMT devices to produce a blockchain assisted patient-centric system. However, this implementation lacks scalability and is reliant on performance of AI.

Kim et al., 2022 surveys the efficiency and practicality of using IoMT devices for patient care, but is limited by the physical constraints of RF signals (superposition, material interruption etc.) and was only tested with a small number of patients.

Koutras et al., 2020 studies the protocols, application layer functionality, and general security of IoMT devices. However, it provides only a high-level overview of security measures which could be improved with further detail.

Ghubaish et al., 2021 proposes a comprehensive framework to meet the security requirements of IoMT devices. However, because of challenges with the framework, there is additional need for a system supporting remote initial setup and alternative access.

Risk Analysis of Named IoMT Devices

Standards and Policies

ISO/IEC 27001:2022
A document from the International Organization for Standardization that outlines the requirements for “establishing, maintaining and continually improving an information security management system” which can be used to assess an organization’s fulfillment of its information security requirements (ISO, 2022).

ISO/IEC 27005:2022
Another document from the International Organization for Standardization that outlines the theoretical guidelines for information security risk management in an organization, including PII management and computer misconfigurations (ISO, 2022).

ISO 31000:2018
Another document from the International Organization for Standardization that contains information on managing risks. It also includes a comprehensive guide to completing a risk assessment, which this document will follow (ISO, 2018).

Data Protection Act (2018)
UK law governing privacy and data protection. Prohibits processing of personal data including data concerning health (UK Government, 2018).

NCSC Cyber Essentials
A UK Government standard that ensures organisations are implementing the most important cyber security controls (NCSC, 2024).

Methodology

Scope

The scope for this risk analysis and assessment is limited to the given list of Internet of Medical Things (IoMT) devices. It is assumed that any devices that are able to connect to a network are connected to their expected networks (if for example, it is required for use e.g. Medtronic MyCareLink devices), or that it is connected to a network with further defences in use. It is also assumed that generalised risk (non-IT-related e.g. flooding, fire, natural disasters) have been assessed elsewhere. This assessment will also not take into account the number of affected users, risks to third-party suppliers, or insider threats, since this information is not available, or any consequences of attacks such as lawsuits.

Contextual Responsibilities

This table identifies the stakeholders (people who can affect, or be affected by, a decision or activity) within the organisation, and the responsibilities that they hold in ensuring that the organisation conforms to any information security policies, and to the Data Protection Act.

Type	**Stakeholder**	**Responsibilities**
Internal	Senior Management	● Defining risk appetite (acceptable risk) ● Making risk management decisions ● Setting organisational goals and policies ● Have business continuity plans for risks
Internal	Chief Information Security Officer	● Directing cyber security operations within the organization ● Overseeing and final say on risk assessment decisions
Internal	IT / Cyber Security departments	● Sitewide management of IT devices and security measures ● Develop risk control methods
Internal	Department Technology Specialist	● Ensuring correct and secure configuration of devices within their department ● Configuring devices to comply with the hospital's policies
Internal	Employees	● Handle data in accordance with hospital policies
External	Government organisations	● Create standards and policies for guidance for organisations including potentially bringing them into law
External	Technology Vendors	● Supplying technology to their customers ● Ensuring technology is sufficiently protected against attackers ● Update technology when required to fix vulnerabilities

Table 1: the contextual responsibilities of stakeholders

Contextual Goals

Although the organisation that runs the hospital is unknown in this situation, it is assumed that the basic goals of the hospital lie primarily in exceptional patient care and protecting confidential information.

Risk Assessment Components

Component	Description
Risk appetite	Defined by ISO/IEC 31000:2018 as “the amount and type of risk that an organisation is prepared to pursue, retain or take”. As a hospital, the risk appetite will be extremely low, and risk will need to be transferred or reduced accordingly.
Standards and Policies	Standards and baselines that are aimed to be met post-assessment, and the guidelines that will be followed in performing the risk assessment.
Risk Assessment Methodology	Involving many stages to identify assets, risks and threats, and then the relationships between them to identify issues.
Probability and Impact Scale	The probability and impact of the risk will be measured using an amended DREAD scale that does not consider the affected users since this is out of scope.

Table 2: components involved in the risk assessment

Asset Ranking

The given assets are ranked using a weighted-table approach, providing a comprehensive evaluation and ranking of the worst possible scenario given compromise of said device. This allows for several factors (derived from the aims of the hospital) to be taken into account when the assets and risks are used to determine the top vulnerabilities in the named devices.

	Critical (> 0.5)
	Major (0.41 - 0.5)
	Moderate (0.35 - 0.41)
	Minor (< 0.35)

Table 3: ratings of impact severity for asset compromise

Criteria	Impact on Patient Care	Critical Confidential Information	Financial Loss on Equipment and Operation	Weighted Total

Criteria Weight → Asset Name ↓	50%	35%	15%	
Thales Insulin Pump v SW RN 02.000	1.0	0.2	0	0.57
MiniMed Paradigm Veo 554/754 pumps	1.0	0.2	0	0.57
Smiths Medical Medfusion 4000 Wireless Syringe Infusion Pump	1.0	0.1	0.1	0.55
Dickinson and Company (BD) Alaris Plus medical syringe pumps	1.0	0.1	0.1	0.55
Axeda Agent (Access:7)	0	1.0	1.0	0.50
Various BD Pyxis Medstation devices	0.6	0.4	0.1	0.46
Medtronic MyCareLink Monitor version 24950	0.8	0.4	0.4	0.40
Medtronic MyCareLink (MCL) Smart Model 25000 patient reader	0.8	0.4	0.4	0.40
Innokas VC150 vital signs monitor	0.2	0.4	0.7	0.35
3.0T Signa HDx	0.2	0.3	0.8	0.33
Viper Medical Devices	0.2	0.2	0.5	0.25
Philips IntelliSpace Cardiovascular 5.1	0.2	0.3	0.3	0.25
Natus Xltek EEG device utilising Natus Xltek NeuroWorks	0.2	0.3	0.3	0.25

Table 4: weighted approach to asset ranking

Impact	**Device**	**Worst scenario given compromise**
	Thales Insulin Pump v SW RN	Could administer a malicious bolus of insulin

	02.000	causing a medical emergency involving a coma and/or death.
	MiniMed Paradigm Veo 554/754 pumps	Could administer a malicious bolus of insulin causing a medical emergency involving a coma and/or death.
	Smiths Medical Medfusion 4000 Wireless Syringe Infusion Pump	Could administer a malicious bolus of some medication to a patient which could cause severe harm/death.
	Dickinson and Company (BD) Alaris Plus medical syringe pumps	Could administer a malicious bolus of some medication to a patient which could cause severe harm/death.
	Axeda Agent (Access:7)	Complete control over devices via remote access which could control other devices.
	Various BD Pyxis Medstation devices	Could dispense incorrect doses or types of medication. However, a human must deliver to the patient - so it may be checked.
	Medtronic MyCareLink Monitor version 24950	Could fail to alert medical professionals about a cardiac emergency, or, alert them incorrectly.
	Medtronic MyCareLink (MCL) Smart Model 25000 patient reader	Could fail to alert medical professionals about a cardiac emergency, or, alert them incorrectly.
	Innokas VC150 vital signs monitor	Could fail to alert medical professionals about a cardiac emergency, or, alert them incorrectly.
	Viper Medical Devices	Could display incorrect information about a sample.
	Philips IntelliSpace Cardiovascular 5.1	Could display incorrect information about a scan.
	Natus Xltek EEG device utilising Natus Xltek NeuroWorks	Could display incorrect information about a scan.
	3.0T Signa HDx	Could display incorrect information about a scan.

Table 5: worst possible scenarios of compromised devices

Threat Identification

This section identifies threats that could happen to the hospital, or the devices inside of it, according to ISO/IEC 27005:2022. The threats are categorised into overarching threat

categories which identify the nature of the threat, and what caused it. The type of threat categories are as follows: Accidental (A), Deliberate (D), and Environmental (E).

ID	Type of Threat Category	Threat Category	Threat	Description
1	A	Technical Failure	Device Failure	Stops working as intended
2	A/D		Violation of maintainability	Unable to update
3	D	Human Actions	Signal Interception	Read messages without authorisation
4	D		Remote Spying	Watching sensitive/private activities
5	D		Theft of Media/Documents	Stealing files from a compromised device
6	D		Theft of Equipment	
7	D		Theft of Credentials	
8	D		Theft of PII	Stealing Personally Identifiable Information
9	D		Theft of Health Data	
10	A/D		Data input from untrustworthy sources	
11	D		Tampering with hardware	
12	D		Tampering with software	
13	D		Replay attack/Man-in-the-middle	
14	D		Unauthorised use of Devices	
15	A/D		Damaging devices/media	
16	A/D		Corruption of data	

17	A/D		Sending or Distributing of Malware	
18	D		Position Detection	Determining where someone is or what they are doing based on metrics
19	D		Abuse of Medical Devices	Using devices for non-intended purposes
20	D		Network Connection Attempt	
21	A	Compromise of Function or Services	Error in Use	User making a mistake while using device for intended purpose
22	A/D		Abuse of Permissions	
23	D		Forging of Permissions	
24	D		Denial of Actions / Denial of Service	Stop users from performing legitimate actions
25	A/E	Organisational Threats	Lack of Staff	Lack of trained staff to performed trained actions
26	A/E		Lack of Resources	
27	A/E		Failure of Service Providers	E.g. of cloud infrastructure, i.e. MyCareLink system

Table 6: possible threats to the hospital as laid out in ISO/IEC 27005:2022

Vulnerability Identification

This section aims to provide a comprehensive list of known vulnerabilities in the identified assets, and their respective CVE numbers (vulnerability IDs from NIST, 2023). It also identifies the possible threats that would allow the vulnerabilities identified to be exploited. If the software of an identified asset was unknown, any vulnerabilities for that device have been listed. This is to ascertain that all devices are covered by this vulnerability identification.

Component	**Model**	**Version**	**Vulnerabilities**	**Threats**
Insulin Pump	Thales Insulin Pump	SW RN 02.000	Sending or Distributing of Malware (CVE-2020-15858)	Unauthorised Use of Device

			(U.S. Department of Health and Human Services, 2020)	
Insulin Pump	MiniMed Paradigm Veo 554/754 pumps	Software versions 2.6A	Improper Authorisation (CVE-2019-10964)	Replay attack / Man-in-the-middle
				Network Connection Attempt
Fluid Pump	Smiths Medical Medfusion 4000 Wireless Syringe Infusion Pump	Version 1.1, 1.5, and 1.6	Use of Hard-coded Credentials (CVE-2017-12726)	Network Connection Attempt
			Use of Hard-coded Credentials (CVE-2017-12725)	Network Connection Attempt
			Unauthenticated FTP file upload (CVE-2017-12724, CVE-2017-12720)	Network Connection Attempt
			Cleartext passwords (CVE-2017-12723)	Network Connection Attempt
			Communications module crash (CVE-2017-12722)	Device Failure
			Improper Certificate Validation (CVE-2017-12721)	Replay attack / Man-in-the-middle
			Buffer Overflow (CVE-2017-12718)	Network Connection Attempt
Fluid Pump	Dickinson and Company (BD) Alaris Plus medical syringe pumps	Version 2.3.6	Improper Authentication (CVE-2018-14786)	Unauthorised Use of Devices
Remote Access Software	Axeda Agent		Improper Check for Unusual or Exceptional Conditions	Network Connection Attempt

			(CVE-2022-25252)	
			Missing Authentication for Critical Function (CVE-2022-25251, CVE-2022-25250)	Network Connection Attempt
			Improper Limitation of a Pathname to a Restricted Directory (CVE-2022-25249)	Network Connection Attempt
			Exposure of Sensitive Information to an Unauthorized Actor (CVE-2022-25248)	Network Connection Attempt
			Use of Hard-coded Credentials (CVE-2022-25246)	Unauthorised Use of Devices
Medication Dispenser	Various BD Pyxis Medstation devices	Various, at least one using version 1.6	Restricted Desktop Environment Escape Mechanism (CVE-2020-10598)	Data input from untrustworthy sources
		MedStation ES, REF: 323	Application hang/freeze/crash (U.S. Department of Health and Human Services, 2024)	Device Failure
		MedStation 4000 System, REF: 303	Delicate electronics (U.S. Department of Health and Human Services, 2024)	Fluid Ingress
Pacemaker Monitor	Medtronic MyCareLink Monitor	Version 24950	Cleartext Transmission of Sensitive Information (CVE-2019-6540)	Signal Interception
			Missing Authentication for Critical Function (CVE-2019-6538)	Replay attack / Man-in-the-middle

			Insufficient Verification of Data Authenticity (CVE-2018-10626)	Data input from untrustworthy sources
			Insufficiently Protected Credentials (CVE-2018-10622)	Abuse of Medical Devices
			Use of Hard-coded Credentials (CVE-2018-8870)	Tampering with hardware
			Exposed Dangerous Method or Function (CVE-2018-8868)	Data input from untrustworthy sources
Pacemaker Monitor	Medtronic MyCareLink (MCL) Smart patient reader	Model 25000	Time-of-check Time-of-use (TOCTOU) Race Condition (CVE-2020-27252)	Tampering with software
			Heap-based Buffer Overflow (CVE-2020-25187)	Data input from untrustworthy sources
			Improper Authentication (CVE-2020-25183)	Network Connection Attempt
Vitals Monitor	Innokas VC150 vital signs monitor		Improper Neutralization of Input During Web Page Generation (CVE-2020-27262)	Sending or Distributing of Malware
			Improper Neutralization of Special Elements in Output Used by a Downstream Component (CVE-2020-27260)	Sending or Distributing of Malware
Molecular testing device	Viper Medical Devices		Use of Hard-coded Credentials (CVE-2022-22765)	Unauthorised Use of Devices

Scan management software	Philips IntelliSpace Cardiovascular	Version 5.1		
Scanning and scan management software	Natus Xltek EEG device utilising Natus Xltek NeuroWorks	Neuroworks version 8	Use of Hard-coded Credentials (CVE-2023-47800)	Unauthorised Use of Devices
			Out-of-bounds Read (CVE-2017-2860, CVE-2017-2852, CVE-2017-2861, CVE-2017-2858)	Network Connection Attempt
			Out-of-bounds Write (CVE-2017-2869, CVE-2017-2868, CVE-2017-2867, CVE-2017-2853)	Network Connection Attempt
MRI machine	3.0T Signa HDx	versions HD 16, HD23	Exposure of Sensitive Information to an Unauthorized Actor (CVE-2020-25175, CVE-2020-25179)	Replay attack / Man-in-the-middle

Table 7: Identified vulnerabilities with the assets from NIST, 2023 and CISA, 2023.

Risk Register

This section aims to provide an exhaustive list of risks to the identified assets. The threats that may exploit the vulnerabilities (identified by their CVE number in this table) are listed above. Risks are described and rated using an amended DREAD scale (numbers between 1 (low) and 3 (high), since relevant data about these risks is qualitative, summed together and divided by 4 to find the DRED Score). Since the scope only covers the devices themselves, and not the networks they may be connected to, it is assumed that all devices are easily discoverable. The DRED score is multiplied by the asset weight of the affected device to identify the total score of that risk to the hospital.

Device	**CVE-**	**Risk**	**D**	**R**	**E**	**D**	**DRED Score**	**Asset Weight**	**Total Score**
Thales Insulin Pump	2020-15858	Attacker gains system control	3	1	2	3	2.25	0.57	1.29
MiniMed Paradigm Veo	2019-10964	Attacker controls insulin delivery	3	2	2	3	2.5	0.57	1.43

554/754 pumps									
Smiths Medical Medfusion 4000 Wireless Syringe Infusion Pump	2017-12726	Remote code execution via Telnet	2	2	3	3	2.5	0.55	1.38
	2017-12724, 2017-12720	Attacker can upload files via FTP	1	2	3	3	2.25		1.24
	2017-12723	Attacker can steal passwords from configuration file	2	3	2	3	2.5		1.38
	2017-12722	Communications module crashes and device cannot communicate wirelessly	1	1	1	1	1.0		0.55
	2017-12721	Attacker gains unauthorised control of the pump	3	1	2	3	2.25		1.24
	2017-12718	Remote code execution	3	1	1	3	2.0		1.1
BD Alaris Plus medical syringe pumps	2018-14786	Attacker gains unauthorised control of the pump	3	1	1	3	2.0	0.55	1.1
Axeda Agent	2022-25252	Employees are unable to use the software due to DoS	2	2	3	3	2.5	0.50	1.25
	2022-25251	Configuration tampering of target device	2	2	2	3	2.25		1.13
	2022-25250	Employees are unable to use specific service as it has been shutdown	3	2	2	3	2.5		1.25
	2022-25249	Attacker could read and steal any	2	2	3	3	2.5		1.25

		files on the device							
	2022-25248	Attacker can read the event log of a specific service	1	2	3	3	2.25		1.13
	2022-25246	Attacker gains full control of host OS that is running this software	3	2	2	3	2.5		1.25
BD Pyxis Medstation devices	2020-10598	Attacker can steal health data	3	1	2	3	2.25	0.46	1.04
	Hang/freeze/ crash	Delays to medication access and potential data loss	2	2	1	1	1.5		0.69
	Delicate electronics	Smoke, system downtime, and/or fire	3	2	1	1	1.75		0.81
Medtronic MyCareLink Monitor	2019-6540	Attacker can listen to pacemaker information	2	1	1	3	1.75	0.40	0.7
	2019-6538	Attacker can edit memory values in implanted pacemaker	3	1	2	3	2.25		0.9
	2018-10626	Attacker may upload invalid data to the MCL network	1	2	2	3	2.0		0.8
	2018-10622	Attacker uses stolen credentials for network authentication	3	2	3	3	2.75		1.1
	2018-8870	Attacker gains full control over the system	2	2	1	3	2.0		0.8
	2018-8868	Attacker can read and write arbitrary memory values to pacemaker	3	1	2	3	2.25		0.9

Medtronic MyCareLink (MCL) Smart patient reader	2020-27252	Attacker can upload custom firmware and gain complete system control	3	1	1	3	2.0	0.40	0.8
	2020-25187	Attacker can gain full system control through remote code execution	3	1	2	3	2.25		0.9
	2020-25183	Attacker can steal medical data from the reader	1	1	2	3	1.75		0.7
Innokas VC150 vital signs monitor	2020-27262	Arbitrary web script/HTML present on multiple endpoints of administrative web interface	1	2	2	3	2.0	0.35	0.7
	2020-27260	Multiple endpoints may contain injected HL7 v2.x segments in messages	2	1	1	3	1.75		0.62
Viper Medical Devices	2022-22765	Attacker can read and write confidential information	3	2	1	3	2.25	0.33	0.74
Natus Xltek EEG device utilising Natus Xltek NeuroWorks	2023-47800	Attacker gets complete control over SQL server including remote code execution	3	1	3	3	2.5	0.25	0.63
	2017-2860 2017-2852 2017-2861 2017-2858	System is unable to be used due to DoS attack	1	2	2	3	2.0		0.5
	2017-2869 2017-2868 2017-2867 2017-2853	Remote code execution on the target device	3	2	2	3	2.5		0.63
3.0T Signa HDx	2020-25175 2020-25179	Attacker collects credentials and is	2	1	2	3	2.0	0.33	0.66

		able to access the system							

Table 8: Risk register of the assets

Risk Evaluation

As a hospital, it is very important that the risk appetite is extremely low - we do not want any residual risk if it can be avoided, since that risk may impact the ability to care for patients. Therefore, it is crucial that we work to reduce or transfer the risk so that the residual risk falls below that of the risk appetite.

Risk Control

This section suggests mitigations that can be undertaken in order to help fix or protect the named vulnerabilities, and thus reduce the risk. Since assets with unknown software versions have all CVEs included, it is up to the team(s) implementing these mitigations to decide whether the mitigation is necessary based on the software running on the device.

Device	**Risk**	**Mitigation Strategy**
Thales Insulin Pump	Attacker gains system control	Patch the insulin pump with the update released in February 2020.
MiniMed Paradigm Veo 554/754 pumps	Attacker controls insulin delivery	Discontinue use of the device in favour of newer model insulin pumps, but if not, ensure physical control of pump at all times and keep a close eye on its operation.
Smiths Medical Medfusion 4000 Wireless Syringe Infusion Pump	Remote code execution via Telnet	Update the device to version 1.6.1 which is patched for all listed vulnerabilities to this device.
	Attacker can upload files via FTP	
	Attacker can steal passwords from configuration file	
	Communications module crashes and device cannot communicate wirelessly	
	Attacker gains unauthorised control of the pump	
	Remote code execution	
BD Alaris Plus	Attacker gains unauthorised	Only operate the device in a

medical syringe pumps	control of the pump	segmented network or without network connection. Only connect to Alaris Gateway Workstation docking stations.
Axeda Agent	Employees are unable to use the software due to DoS	Update Axeda Agent to version 6.9.2 build 1049 or 6.9.3 build 1051. Configure the device to only listen on the local host interface 127.0.0.1 if possible. Refrain from using the ERemoteServer utility, and delete it from devices. Remove the installation file. Configure Axeda Agent to include authentication information required to log in.
	Configuration tampering of target device	
	Employees are unable to use specific service as it has been shutdown	
	Attacker could read and steal any files on the device	
	Attacker can read the event log of a specific service	
	Attacker gains full control of host OS that is running this software	
BD Pyxis Medstation devices	Attacker can steal health data	Update the devices to version 1.6.1.
	Delays to medication access and potential data loss	Monitor and investigate system reboots. Limit physical access to the devices to authorised users.
	Smoke, system downtime, and/or fire	
Medtronic MyCareLink Monitor	Attacker can listen to pacemaker information	Ensure that the monitor is receiving updates. Maintain good physical control over the monitor. Do not connect or use any devices that were not obtained directly from your healthcare provider.
	Attacker can edit memory values in implanted pacemaker	
	Attacker may upload invalid data to the MCL network	
	Attacker uses stolen credentials for network authentication	
	Attacker gains full control over the system	

	Attacker can read and write arbitrary memory values to pacemaker	
Medtronic MyCareLink (MCL) Smart patient reader	Attacker can upload custom firmware and gain complete system control	Ensure the MyCareLink app has been updated to version 5.2. Maintain good physical control over monitors. Only use devices obtained directly from a healthcare provider.
	Attacker can gain full system control through remote code execution	
	Attacker can steal medical data from the reader	
Innokas VC150 vital signs monitor	Arbitrary web script/HTML present on multiple endpoints of administrative web interface	Update the software to version 1.7.15b or later. Ensure device is used in a segmented network, and that physical access to it is restricted.
	Multiple endpoints may contain injected HL7 v2.x segments in messages	
Viper Medical Devices	Attacker can read and write confidential information	Update the software version to 4.80. Ensure only authorised users have access to the system, and remove network access if possible.
Natus Xltek EEG device utilising Natus Xltek NeuroWorks	Attacker gets complete control over SQL server including remote code execution	Update software to version 8.5 GMA 3, which has been patched. Minimise network exposure of the device. Ensure the device is not accessible from the Internet.
	System is unable to be used due to DoS attack	
	Remote code execution on the target device	
3.0T Signa HDx	Attacker collects credentials and is able to access the system	Update to the latest firmware.

Table 9: Suggested mitigations per risk

Critical Evaluation of the Most Severe Risks

Of the listed risks, these three are the highest rated: the most severe in terms of impact on hospital goals.

Attacker controls insulin delivery to patients

This risk involves a malicious party exploiting the vulnerability in the MiniMed Paradigm Veo 554/754 pumps by sending packets containing blood glucose data, which the pump then acts upon. The pumps do not verify the authenticity of these packets, or the authorisation with which they are sent.
However, it should be noted that this requires an RF (radio frequency) connection to the insulin pump itself. Any malicious party would require close proximity, less than 11m, to the user in order to be able to realise this risk.
Secondly, it is unlikely that a user will not notice the extra insulin being administered, or their symptoms of a pending hypoglycemic attack. Insulin pumps usually notify the user before administering a correction, and once the correction has been delivered, by beeping or vibrating.

Hard-coded Credentials for Telnet

The Smiths Medical Medfusion 4000 Wireless Syringe Infusion Pump has many risks associated with it, but one of the most severe ones is the hard-coded credentials (credentials that are written into the code itself, and cannot be changed) used for Telnet. If the pump is configured to accept external connections, which we can assume is a reasonable percentage, given that the pumps need to communicate with the PharmGuard server, then the Telnet protocol can be utilised.
Telnet is an insecure protocol that allows users to remotely access and control a device.

However, Smiths Medical asserts that it isn't possible to upload files via Telnet to the device which makes it much harder to run complicated scripts/malware.
Secondly, they also assert that any impact from exploiting this vulnerability is limited to the communications module. This is a separate module to the therapeutic module, which is the module responsible for administering the medication contained in the syringe.

Attacker can steal passwords from configuration file

Another risk originating from the Smiths Medical Medfusion 4000 Wireless Syringe Infusion Pump is the potential for passwords stored in cleartext from the configuration file to be stolen. It is unknown what passwords can be stolen from the configuration file, but due to the wireless nature of the device, it may contain user passwords or credentials to access the network. This may allow malicious parties to compromise user accounts and connect to the network. This gives them a far larger attack surface, especially if using a compromised account.

However, there is no evidence of the type of passwords stored in the file, and assuming it grants malicious parties account credentials and network access is simply the worst possible scenario.

Secondly, in order to access these passwords, the pump must be configured to allow external communications. As mentioned above, this is likely, but it is not a given.
Finally, the pump only stores “some” passwords in the configuration file, not all.

Critical Evaluation of the Top Vulnerabilities

Of the listed vulnerabilities, the CVSS score, as determined by NIST and ICS-CERT, has been used to determine the top three.

Code Execution Vulnerability in NeuroWorks Version 8

CVE-2017-2853 (CVSS 9.8), CVE-2017-2868 (CVSS 10.0)

There are several vulnerabilities in Neuroworks version 8 that allow for writing data out-of-bounds by using a specially crafted network packet to achieve a stack buffer overflow. These vulnerabilities are relatively easy to exploit, since it is very likely that the machine running the Neuroworks software is connected to the Internet, because this allows for the full synchronisation of data, which is one of their features.
For CVE-2017-2853, the software requests a path to open an EEG file from the client, but the construction of the path variable contains the buffer overflow.
The other vulnerability is a buffer overflow in the parsing of a list of lists data structure, using keys. A sufficiently long enough key string can result in a buffer overflow.

However, it is not guaranteed that these devices would be connected to the Internet, and may instead be connected in a network that connects them together, but not to the Internet. This would make exploitation very difficult, and an attacker would require physical access to the machines.

Exposure of Sensitive Information from Signa HDx

CVE-2020-25175 (CVSS 9.8), CVE-2020-25179 (CVSS 9.8)

These vulnerabilities involve the transmission of credentials in cleartext over a network. This device connects to a network in order to transmit the MRI scan data to another device. However, anyone connected to this network could access the plaintext credentials also transmitted. These are therefore very easy vulnerabilities to exploit, since they only require an attacker to sniff packets on the network and wait for the device to send the credentials.

However, it requires the MRI machine and target device to be on a network that is publicly accessible or has weak security features.

Missing Authentication in Axeda Agent

CVE-2022-25251 (CVSS 9.8)

This vulnerability allows remote attackers to send XML messages to specific ports without authentication, which can edit the configuration of the target device.

However, it requires an attacker to be able to connect to the Axeda Agent software, so it must be accessible over the Internet, which is possible, but neither likely nor unlikely, or the attacker must have physical access to a device connected to another running this software.
Even then, a specific port must be accessed which may have been configured to an arbitrary number up to 65,535 which is therefore unlikely to be guessed or bruteforced in a reasonable length of time.

Recommendations

Type	Recommendation	Explanation	Stakeholder
Regular	Ensure routine software updates to all devices	A lot of the vulnerabilities discovered in this assessment already have updates and patches released for them, which would mitigate the vulnerability. However, the lack of regular software updates to these devices has caused these vulnerabilities to remain. Consider testing the software update on a singular device first, to ensure it does not impact operation, then roll out the update to every device of that type.	Technology Vendors, IT / Cyber Security departments, Department Technology Specialist
Regular	Ensure regular IT audits	Ensure that risk assessments/audits are completed on a regular basis in order to ensure that mitigations are being implemented, and in order to catch any new risks that might be introduced. It is recommended to have at least one every year, so no risk is prevalent for too long. It is also considerably cheaper to the hospital to perform these than pay compensation and fines for breaching the Data Protection Act.	Chief Information Security Officer, Senior Management
Quick fix	Install and configure network security devices to limit remote access to devices	A lot of these risks involve a remote attacker. Implementing and correctly configuring network security devices such as firewalls will make it much more difficult for an attacker to access any device on the network, thus reducing its discoverability, and therefore its risk rating.	IT / Cyber Security departments
Long-term	Educate staff about device usage	Ensure staff are using devices correctly and securely by providing sufficient training opportunities.	Chief Information Security Officer
Long-term	Meet NCSC Cyber Essentials	Ensure that devices and systems meet the requirements laid out by the NCSC to be the baseline for protection for cyber security threats.	Chief Information Security Officer
Quick fix	Invest in more modern technology with better security controls	More modern devices have more robust security controls, and have less of a risk associated with them because major vulnerabilities may not have been disclosed to the public, making them less discoverable.	Senior Management, Chief Information Security Officer

Table 10: Recommendations for further action to improve the cyber security of the hospital.

References

1. Darin Mansor Mathkor, Noof Mathkor, Zaid Bassfar, Farkad Bantun, Petr Slama, Faraz Ahmad, Shafiul Haque, Multirole of the internet of medical things (IoMT) in biomedical systems for managing smart healthcare systems: An overview of current and future innovative trends, Journal of Infection and Public Health, Volume 17, Issue 4, 2024, Pages 559-572, ISSN 1876-0341, https://doi.org/10.1016/j.jiph.2024.01.013. (https://www.sciencedirect.com/science/article/pii/S1876034124000194)
2. A. Ghubaish, T. Salman, M. Zolanvari, D. Unal, A. Al-Ali and R. Jain, "Recent Advances in the Internet-of-Medical-Things (IoMT) Systems Security," in *IEEE Internet of Things Journal*, vol. 8, no. 11, pp. 8707-8718, 1 June, 2021, doi: 10.1109/JIOT.2020.3045653.
3. Razdan, S., & Sharma, S. (2021). Internet of Medical Things (IoMT): Overview, Emerging Technologies, and Case Studies. *IETE Technical Review*, *39*(4), 775–788. https://doi.org/10.1080/02564602.2021.1927863
4. Kim, B., Kim, S., Lee, M., Chang, H., Park, E., & Han, T. (2022). Application of an Internet of Medical Things (IoMT) to Communications in a Hospital Environment. *Applied Sciences*, *12*(23), 12042. https://doi.org/10.3390/app122312042
5. Koutras, D., Stergiopoulos, G., Dasaklis, T., Kotzanikolaou, P., Glynos, D., & Douligeris, C. (2020). Security in IoMT Communications: A Survey. *Sensors*, *20*(17), 4828. https://doi.org/10.3390/s20174828
6. International Organization for Standardization. (2022). *Information security, cybersecurity and privacy protection — Information security management systems — Requirements* (ISO Standard No. 27001:2022). https://www.iso.org/standard/27001
7. International Organization for Standardization. (2022). *Information security, cybersecurity and privacy protection — Guidance on managing information security risks* (ISO Standard No. 27005:2022). https://www.iso.org/standard/80585.html
8. International Organization for Standardization. (2018). *Risk management — Guidelines* (ISO Standard No. 31000:2018). https://www.iso.org/standard/65694.html
9. UK Government. (2018). *Data Protection Act 2018* https://www.legislation.gov.uk/ukpga/2018/12/introduction/enacted
10. NCSC. (2024). *Cyber Essentials - NCSC*. https://www.ncsc.gov.uk/cyberessentials/overview
11. U.S. Department of Health and Human Services. (2020). *Health Sector Cybersecurity Coordination Center (HC3) Analyst Note* (Report: 202008190742). https://www.hhs.gov/sites/default/files/thales-modules-vulnerability-affecting-devices-in-the-hph-sector.pdf
12. Cybersecurity & Infrastructure Security Agency. (2023). *America's Cyber Defense Agency* https://www.cisa.gov/
13. U.S. Department of Health and Human Services. (2024). *Class 2 Device Recall BD Pyxis" MedStation" ES; BD Pyxis" MedStation" ES Tower; BD Pyxis" Anesthesia Station ES*. https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfres/res.cfm?id=205949

14. U.S. Department of Health and Human Services. (2024). *Class 2 Device Recall BD Pyxis MedStation ES*. https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfres/res.cfm?id=207439
15. NIST. (2023). *National Vulnerability Database.* https://nvd.nist.gov/vuln