Healthier Communities, Outstanding Care

NHS
Sherwood Forest Hospitals
NHS Foundation Trust

Data Protection Impact Assessment

Title	Ref number
CareLink™ System	

Introduction

A Data Protection Impact Assessment enables Sherwood Forest Hospitals NHS Foundation Trust (SFHFT) to meet its legal/compliance obligations with the Data Protection Act 2018 and the General Data Protection Regulation 2016.

The Data Protection Impact Assessment (DPIA) ensures the confidentiality, integrity and availability of information by applying a risk management process and gives confidence to interested parties that risks are adequately managed, as required under ISO/IEC: 27001:2017. It is important that the DPIA is part of and integrated with the organisation's processes and overall management structure and that information security is considered in the design of processes, information systems, and controls. The process identifies and allows issues to be mitigated at an early stage of implementation/change thereby reducing associated costs and damage to reputation. Data Protection Impact Assessment are an integral part of the "privacy by design" approach as identified by the Information Commissioner's Office.

Document Completion

A DPIA must be completed wherever there is **a change to an existing process or service** or **if a new process or information asset is introduced** that is likely to involve a new use or significantly changes the way in which personal data, special categories of personal data or business critical information is processed.

This document, and the privacy risks, actions and recommendations identified within it, will be accepted in the Project Sign Off (page 3). The project will need to signed off by the Information Asset Owner, a representative from NHIS, Information Governance/Data Protection Officer and a customer representative (if applicable) and through the appropriate governance structure of the implementing organisation. Sign off and acceptance of the document does not close the privacy risks related to this project. It is important that the risks are revisited during the life of the project and any additional privacy risks identified are appropriately reviewed and mitigated.

PLEASE NOTE:
The Information Asset Owner (implementer) undertaking the Data Protection Impact Assessment has a responsibility to ensure that Patient Safety, Technical Security and Quality Impact Assessments are considered, in line with the Trust procedures.
Assessment Process Stages

Activity	IAO	Governance
Complete Title Bar and include Ref Number	x	
Complete Project Details and check the Initial Screening Questions	x	x

Complete Stage 1 – Introductory meeting and review Initial Screening Questions and follow up questions to determine if a Stage 2 – DPIA (Full) is to be undertaken	x	x
Initial Screening Questions to be formally written up and Introductory Meeting to be formally recorded	x	x

If a Data Protection Impact Assessment **IS NOT** required		
Activity	**IAO**	**Governance**
Complete Assessment Summary & Recommendations for Action	x	x
Assessment to be passed to Implementer		x
Ensure Sign Off is completed	x	x
Assessment shared with customer if appropriate	x	
Assessment to be kept with project documentation copy to Information Governance	x	

OR

If a Data Protection Impact Assessment **IS** required		
Activity	**IAO/IAA**	**Governance**
When a new system is being implemented and the supplier provides a completed DPIA on a suppliers template, the information will need to be transferred to the Trust's template to ensure there are no omissions	**x**	
Complete Stage 2 – Data Protection Impact Assessment (Full)	**x**	
Complete Stage - 3 Identified Risks and Mitigating Action	**x**	
Complete Stage – 4 Legal Compliance		x
Complete Assessment Summary & Recommendations for Action	x	
Account access management Standard Operating Procedure to be completed prior to the implementation of the project	x	
Closure meeting for final agreement	x	
Ensure Sign Off is completed		x
Assessment shared with customer if appropriate	x	
Assessment to be kept with project documentation copy to Information Governance	x	

This document is intended to be completed by the Trust and external organisations the *Governance* section will be completed by the IG Team with support from the relevant NHIS specialist teams as applicable.

Project Details

Project Title:	CareLink™ System

Project Description: Describe in sufficient detail for the proposal to be understood

CareLink™ System is a service provided by Medtronic to health care professionals to upload patient insulin pumps, continuous glucose monitor devices and compatible BG meters. This enables health care professionals to generate reports to assist with patient's diabetes management. health care professional's may create a patient profile in the system and upload a patients compatible device in clinic to see data from their device or request that the patient links their CareLink Personal™ with the clinic so that data patients upload at home can be viewed in CareLink™ System by the health care professional.

CareLink™ System is Medtronic's new version of CareLink for Healthcare Professionals which replaces CareLink Pro. It is compatible with the latest devices from Medtronic (including the MiniMed 670G) enabling the Trust to efficiently support patients by helping to optimise therapy by viewing reports on device usage.
Installation of the CareLink Uploader Applet will also be required within the hospital onto computers where the Trust wishes to upload compatible devices in clinic.

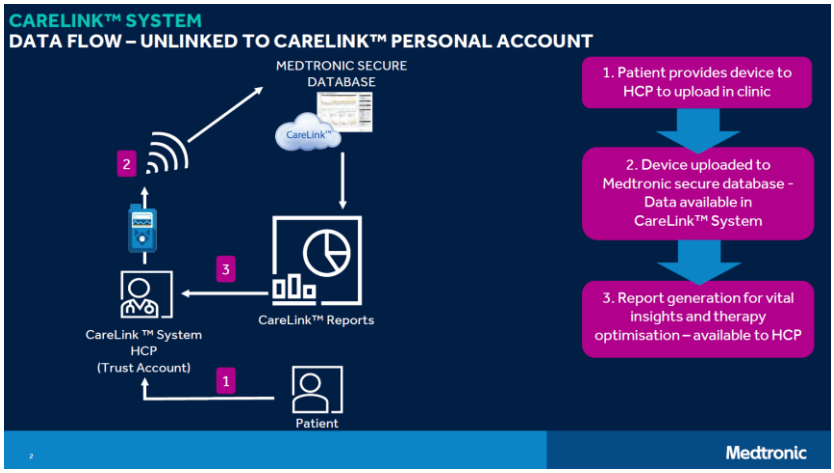
Overview of the proposal: What the project aims to achieve

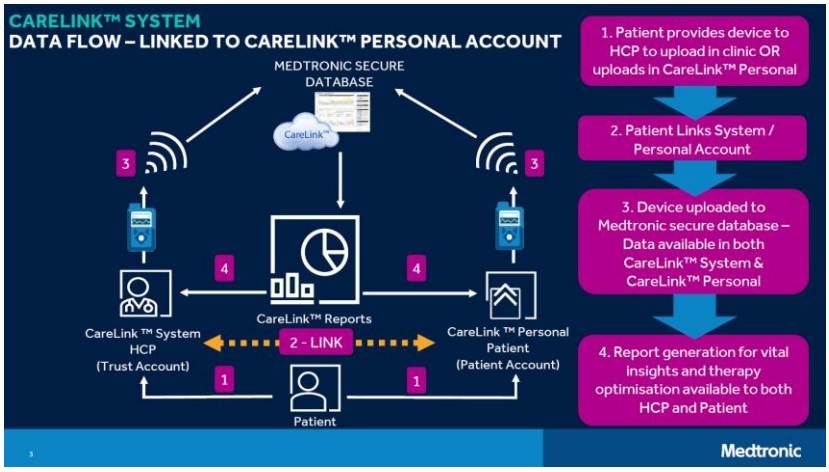
Direct Patient Care:

CareLink™ System assists in the provision of direct patient care by providing a visual representation of Medtronic Diabetes device data that is uploaded from a compatible Medtronic device. The system enables different CareLink reports to be generated that can be used by the clinical team to optimise patient therapy management and enhance collaboration on Diabetes management between clinical team and health care professional.

Research *(when system is linked to CareLink™ Personal + explicit consent is provided by the patient)*:
As per CareLink™ System contract the Trust is notified that due to the bi-directional natural of data flows between CareLink™ System and a LINKED account within CareLink™ Personal (a separate system which allows a patient to upload their Medtronic device at home – here the agreement is directly between patient and Medtronic) that if a patient profile in CareLink™ System is linked to a CareLink™ Personal account with the patient providing ***explicit*** consent to establish such a link, then any data uploaded to the patients profile in CareLink™ System will be available to the patient in CareLink Personal. Medtronic may use such data for research and development / analytics purposes provided that they have ***explicit*** consent directly from the patient in CareLink Personal. Note: Medtronic will only use data for research and development / analytics purposes in CareLink™ Personal AND if explicit consent is provided by the patient.

If no link is established between the patients profile in CareLink™ System and the patient CareLink™ Personal account, or the patient does not provide explicit consent to use data for extended purposes by Medtronic, no data will be used for research and development purposes.





Implementing Organisation:	Sherwood Forest Hospitals NHS Foundation Trust

Staff involved in DPIA assessment (Include Email Address):	shermeen.mahmood@medtronic.com jack.c.cottle@medtronic.com elainehiggins@nhs.net ursula.ngwu@nhs.net

Project Sign Off

	Name	Job Title	Organisation	Date

Information Asset Owner	Rachael Briggs and Lisa Gowan	Divisional General Manager	Sherwood Forest Hospitals NHS Foundation Trust	**18th August 2021 /**
Data Protection Officer	Jacquie Widdowson	Information Governance Manager	Sherwood Forest Hospitals NHS Foundation Trust	**4th August 2021**
Information Governance	Gina Robinson	Information Security Officer	Sherwood Forest Hospitals NHS Foundation Trust	**13th July 2021**
Senior Information Risk Owner	Paul Robinson	Chief Financial Officer	Sherwood Forest Hospitals NHS Foundation Trust	**21st September 2021**
Caldicott Guardian	David Selwyn	Medical Director	Sherwood Forest Hospitals NHS Foundation Trust	**18th August 2021**
Chief Clinical Information Officer	David Selwyn	Medical Director	Sherwood Forest Hospitals NHS Foundation Trust	**18th August 2021**

Assessment Summary

To be completed by Information Governance

Outcome of Data Protection Impact Assessment:	
1. Project/Implementation is recommended **NOT** to proceed, as significant corporate/customer risks have been identified.	☐

2. Project/Implementation to proceed once identified risks have been mitigated as agreed.	☒
3. Project/Implementation has met required legislative compliance and poses not significant risks. No further action required.	☐

Summary of Data Protection Impact Assessment; including legislative compliance and identified risks:

Summary:

1. Medical devices will be plugged into Trust ports and will need to be added to the whitelist.
2. CareLink™ will need to be added to both the Women and Children's and Medicine's divisional information asset register and the data flows mapped and recorded as part of the annual IAO returns to the SIRO

Summary of Risks:

1. A call will need to be raised with the Cyber Security team (NHIS) for the medical devices to be added to the whitelist. The impact will be that if the devices are not whitelisted then data cannot be accessed by the Trust, unless the patient has linked their CareLink™ account and the data is flowing back to the Trust via the CareLink™ Portal
2. Information Asset Administrators to ensure CareLink™ is added to the information asset register and data flows are mapped and recorded

Recommendations for Action

Summary of Identified Recommendations:		
Recommendations: 1. A call will need to be raised with the Cyber Security team (NHIS) for the medical devices to be added to the whitelist	**Recommendation Owner:** IAO	**Agreed Deadline for action:** 31st August 2021
2. Information Asset Administrators to ensure CareLink™ is added to the information asset register and data flows are mapped and recorded	IAA	30th September 2021

Stage 1 – Initial Screening Questions

Answering "**Yes**" to a screening questions below represents a potential IG risk factor that may have to be further analysed to ensure those risks are identified, assessed and fully mitigated. The decision to undertake a full DPIA will be undertaken on a case-by-case basis by IG.

Q	Screening question	Y/ N	Justification for response
1	Will the project involve the collection of information about individuals?	Y	Medtronic Note - The following data is captured by CareLink™ System (*) denotes mandatory: First / Last Names* (Initials can be used) DOB* Device Serial Number* Diabetes type Email address Phone number Patient ID (This could be NHS number) Notes Device Health Data (including continuous glucose monitor data / insulin data etc. used for therapy management)*
2	Will the project compel individuals to provide information about themselves?	Y	This is required to link the patient to their account for on-going updates from the company and to ensure consumable supplies are provided effectively. CareLink™ System is the only compatible version of CareLink for healthcare professionals with Medtronic's new insulin pump and diabetes devices (such as the MinMed 670G System / MiniMed 780G System). CareLink™ System will enable the Diabetes department to view new reports that are exclusive to the Medtronic's latest insulin pump system helping to facilitate an improved patient care with greater glycemic control. The information on CareLink reports assists in reviewing and managing each individual patient's therapy programme. Access to CareLink reports is an essential part of helping to manage a patient's diabetes therapy programme.
3	Will information about individuals be	Y	Medtronic Comment - Data is processed by Medtronic with a service agreement needed between the Trust and Medtronic

Q	Screening question	Y/ N	Justification for response
	disclosed to organisations or people who have not previously had routine access to the information?		Limited (UK). Medtronic Limited uses the following Medtronic sub-processors to provide the CareLink Service. 1. Medtronic International Trading Sàrl ("Medtronic Europe") at Route du Molliau 31, CH - 1131 Tolochenaz. Europe, Middle East & Africa (EMEA) headquarters for Medtronic. Contains the regional functions for Marketing, Legal, and Operational support for the primary Medtronic businesses. 2. Medtronic B.V. with registered address at Industry Park Trilandis Earl Bakkenstraat 10, 6422 PJ, Netherlands. European Operations Centre for distribution and shared services. Provides support and dedicated staff to the Medtronic data centre at the Engie facility which houses the CareLink server for the collection and processing of patient and clinic CareLink data. 3. Medtronic Bakken Research Center B.V. ("BRC") with registered address at Endepolsdomein 5, 6229 GW Maastricht, Netherlands. Provides internal Medtronic EMEA regional support for regulatory filings/approvals, research studies and analysis, and global translations. 4. Medtronic MiniMed, Inc. ("Medtronic"), at 18000 Devonshire Street, Northridge, California, 91325. Global headquarters for the Medtronic Diabetes business unit. Supports the development and maintenance of diabetes products including insulin pumps, continuous glucose monitoring sensors, and software products including CareLink System. Supports tier 2 and 3 technical support. For all transfers of personal data to countries outside the EEA, Medtronic will transfer personal data only to countries outside the EEA on the basis of an adequacy decision of the European Commission or,

Q	Screening question	Y/ N	Justification for response
			where no adequacy decision is available, on the basis of standard data protection clauses adopted by the European Commission or any other legal ground explicitly allowed by the UK/EU GDPR. Medtronic Limited in the UK will put appropriate international transfer safeguards in place to ensure that personal data transfers to and from the UK can continue in compliance with applicable data protection laws. Specifically, for CareLink™ System (Diabetes) services, Medtronic Limited in the UK makes use of the services of Medtronic affiliates based in the EU.
4	Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?	Y	CareLink™ System supersedes the currently installed CareLink Pro software and is the only system available for the generation of reports from Medtronic diabetes devices (including the latest MiniMed 670G / MiniMed 780G insulin pump systems). CareLink™ System has been developed with Privacy by design ensuring full GDPR compliance. Medtronic Note - The data will be used to provide a variety of CareLink reports to the Diabetes service - this will enable the team to optimise patient therapy.
5	Are there processes in place to ensure data is relevant, accurate and up-to-date?	N	As data controller, the Trust administrator / user are able to update information of patients held within CareLink™ System (with the exception of device data which cannot be altered) in accordance with Trust policy. Device data uploaded to the system comes directly from the Medtronic device and as such cannot be altered / amended in any way. To ensure up to date device data is available the Trust will be able to upload a patient device to CareLink™ System via the web interface and using the CareLink Uploader (available at https://carelink.medtronic.eu/public/uploaderInstructions.html). Alternatively, the patient may provide explicit consent to link their CareLink™ Personal account with their

Q	Screening question	Y/ N	Justification for response
			profile in the Trust CareLink™ System account, thus providing access to data uploaded by the patient at home to the Trust.
6	Are there security arrangements in place while the information is held?	Y	Medtronic CareLink™ System is a Class I CE Marked Medical Device which stores data in an ISO 27001 certified datacentre within the Netherlands. Engie Services Zuid B.V. (formerly known as Cofely Zuid Nederland BV) with registered address at Amerikalaan 35, 6199 AE Maastricht-Airport, Netherlands, provides the physical facility where the Medtronic data processing electronic equipment (e.g., the CareLink servers) are housed. Engie provides the secure facility, the room to house the equipment, power, and temperature control to the room. Engie does not support the Medtronic electronic equipment or process CareLink data, and as such are not deemed sub-processors of information. Data is stored at rest with AES 256 Encryption Keys. CareLink™ System is a web based interface and uses a https:// secure internet connection (see https://carelink.medtronic.eu/media/faq_emea.pdf for compatible browsers and OS requirements) with data being uploaded via the CareLink Uploader (available for download at https://carelink.medtronic.eu/public/uploaderInstructions.html). All data in transit uses TLS 1.2 encryption standards. **Trust access** - There is a two-tier access for Trust users (administrator and user access) with the Trust able to determine which members of clinical or IT has access to the System. **Medtronic Access** - To support and provide appropriate Product support related to CareLink System, Medtronic may have access to data held within the platform. Please see obligations as stated within the CareLink™ System Services Agreement. Staff involved in processing patient data are appropriately trained and made aware of their

Q	Screening question	Y/ N	Justification for response
			confidentiality obligations. End user role-based access to data is restricted to authorised individuals. For further reassurance, Medtronic Limited have met standards outlined by NHS Digital (https://www.dsptoolkit.nhs.uk/OrganisationSearch/8HM01) and also hold ISO 9001 certification for Quality Management System (QMS) covering Medtronic's Policies, Systems and Processes (attached for reference)
7	Does the project involve using new technology to the organisation?	N	
8	Will the project result in you making decisions or taking action against individuals in ways which could have a significant impact on them?	N	
If you have answered "Yes" to any of the questions numbered 1-8 please proceed and complete stage 2.			
9	Is a Patient Safety Review required?	Y	Medtronic Patient Safety Case documentation sent to NHIS for review 12th July 2021. A patient safety case will be undertaken post go live given we can't physically test the pump in a test environment.
10	Is a Quality Impact/Technical Security Review required?	Y	9th June 2021 - NHIS have reviewed the supplier assurance framework and have not identified any concerns or recommendations

Please ensure that on completion this is returned to Information Governance lead to agree how to proceed.

Stage 2 – Data Protection Impact Assessment

2.1	What is the change					
	New purpose?	☒	Revised/changed?	☐	Other?	☐
	If Other please specify.					

2.2.1	What data will be processed?					
	Personal Data:					
	Forename	☒	Surname	☒	Age	☐
	DOB	☒	Gender	☐	Address	☒
	Post Code	☐	NHS No	☒	Hospital No	☐
	Other unique identifier (please specify)					
	Sensitive Personal Data (special categories):					
	Children					☒
	Vulnerable groups					☐
	Racial or ethnic origin					☐
	Political opinion					☐
	Religious Belief					☐
	Trade Union Membership					☐
	Physical or mental health or condition					☒
	Sexual Health					☐
	Criminal offence data					☐
	Other data (please specify)					

2.2.2	Is the data?					
	Identifiable?	☒	Pseudonymised?	☒	Anonymised?	☒
	If the data is pseudonymised please describe the technical controls in place ie pseudonymised data provided to a third party and the 'key' for re-identification to be retained by the Trust. Also describe how the data will be transferred ie using HL7					
	As data controller, the Trust will input data into the system to create a patient profile (including patient names and other personal information, although this can be limited to initials) Clinic application decryption keys are used to decrypt application data before it is sent to the client; these keys are owned by clinic. Keys must have a cryptographic strength commensurate the level of protection required for the information and be protected by a suitably secure passphrase. Keys and passphrases are only readable by the system root user, access to which is tightly controlled and monitored. Medtronic has documented acceptable cipher algorithms and methods. Data transfers to CareLink use TLS 1.2 and are encrypted via AES 256 Encryption Keys ▪ Data in CareLink System, including all health information, as far as possible, is de-identified or pseudonymised. Medtronic may have access to identifiable information in the course of supporting the service through Product Support requests ▪ Personal data may be de-identified (anonymised / aggregated) for the purpose of analytics and business operations.					

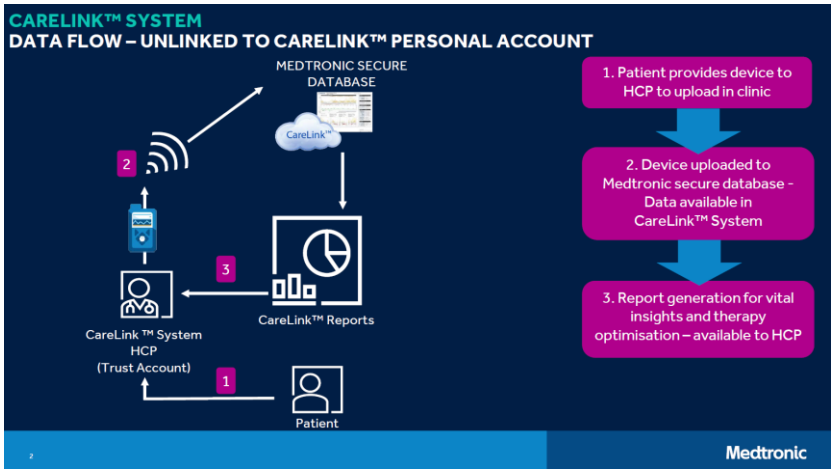
2.3	Is the data required to perform the specified task?	
	Y/N	Please justify response **Yes or No**
	Y	CareLink™ System assists in the provision of direct patient care by providing a visual representation of Medtronic Diabetes device data that is uploaded from a compatible Medtronic device. The system enables different CareLink reports to be generated that can be used by the clinical team to optimise patient therapy management and enhance collaboration on Diabetes management between the clinical team and health care professional.
2.3.1	How will you collect, use, store and delete data?	
	Direct Patient Care: CareLink™ System assists in the provision of direct patient care by providing a visual representation of Medtronic Diabetes device data that is uploaded from a compatible Medtronic device. The system enables different CareLink reports to be generated that can be used by the clinical team to optimise patient therapy	

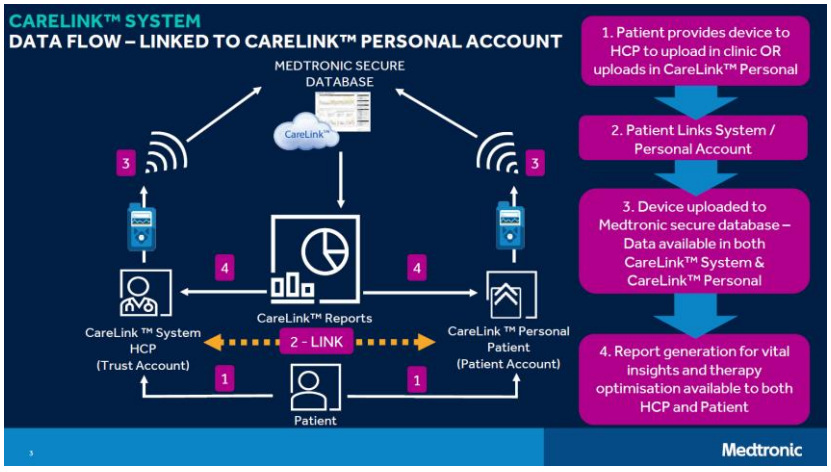
management and enhance collaboration on Diabetes management between the clinical team and health care professional.

Research (when system is linked to CareLink™ Personal + explicit consent is provided by the patient):

As per CareLink™ System contract the Trust is notified that due to the bi-directional natural of data flows between CareLink™ System and a LINKED account within CareLink™ Personal (a separate system which allows a patient to upload their Medtronic device at home – here the agreement is directly between patient and Medtronic) that if a patient profile in CareLink™ System is linked to a CareLink™ Personal account with the patient providing explicit consent to establish such a link, then any data uploaded to the patients profile in CareLink™ System will be available to the patient in CareLink Personal. Medtronic may use such data for research and development / analytics purposes provided that they have explicit consent directly from the patient in CareLink Personal.

Note: Medtronic will only use data for research and development / analytics purposes in CareLink™ Personal AND if explicit consent is provided by the patient. If no link is established between the patients profile in CareLink™ System and the patient CareLink™ Personal account, or the patient does not provide explicit consent to use data for extended purposes by Medtronic, no data will be used for research and development purposes.





	Medtronic Limited in the UK will put appropriate international transfer safeguards in place to ensure that personal data transfers to and from the UK can continue in compliance with applicable data protection laws. Medtronic Limited in the UK makes use of the services of Medtronic affiliates based in the EU. Medtronic Limited do not anticipate any barriers to maintaining the flow of UK personal data by your hospital as data controller to and from Medtronic Limited's sub-processor(s). We continue to monitor the legal position. Should it prove necessary, we are prepared to take additional appropriate steps to avoid any interruption in our services.
2.3.2	What is the source of the data? (i.e. from data subject, system or other third party)
	Patients within the CareLink™ System and Trust staff Medtronic Comment - Trust - CareLink™ System will be made available to Administrators and Users within the Trust (usually the Diabetes team(s)) but this may also include IT for Administration purposes Patient - The patient may also have access to information uploaded by the clinic team if there is a link between the Trusts CareLink™ System account and patients CareLink™ Personal account Medtronic Limited - For the provision and support of CareLink services, including Medtronic sub-processors as identified within the CareLink Services Agreement 02A. Carelink System Services Contract (Dia
2.3.3	How much data will you be collecting and using?
	Answer in 2.3.1 within the data flows information
2.3.4	How often? (for example monthly, weekly)
	Daily
2.3.5	How long will you keep it? NHSX_Records_Management_Code_of_Prac
	Medtronic Comment - CareLink™ System collects insulin pump, continuous glucose monitor and BG meter data each time a health care professional uploads in clinic or in the case where the patients profile is linked with their CareLink™ personal account, data will

	also be available to the health care professional each time the patient chooses to upload their device at home. Each patient profile consists of the following data; name, physical address, gender, age category, diabetes type, email address, phone number and device serial number (where a Medtronic device) and device information (including continuous glucose monitor data / insulin data etc., used for therapy management). CareLink™ System also collects user details (username and email address) of account users you have been provided access to the system by the Trust administrator. CareLink™ System is a Class I CE marked Medical Device, with data uploaded to a secure data centre within the Netherlands (ICO 27001 certified).data is uploaded via a CareLink Uploader Applet installed on a local computer which uploads data from the compatible device to CareLink Servers. Data is transferred via TLS 1.2 encryption via a compatible https:// web connection.
2.3.6	Where will the data be stored? i.e. Medway, Shared Drive, offsite storage
	Medtronic CareLink™ System is a Class I CE Marked Medical Device which stores data in an ISO 27001 certified datacentre within the Netherlands. Engie Services Zuid B.V. (formerly known as Cofely Zuid Nederland BV) with registered address at Amerikalaan 35, 6199 AE Maastricht-Airport, Netherlands, provides the physical facility where the Medtronic data processing electronic equipment (e.g., the CareLink servers) are housed. Engie provides the secure facility, the room to house the equipment, power, and temperature control to the room.
2.3.7	How many individuals are affected?
	All patients who sign up to the Medtronic Diabetes CareLink system
2.3.8	What geographical area does it cover?
	Mansfield, Ashfield, Newark and Sherwood

2.4	Who are the Organisations involved in processing (sharing) the data?	
	Organisations Name	Data Controller or Data Processor *The **Data Controller** is a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.* *The **Data Processor**, in relation to personal data, means any person (other than an employee of the data*

		controller) who processes the data on behalf of the data controller.
	Sherwood Forest Hospitals NHS Foundation Trust	Data Controller
	Medtronic Limited	Data Processor - Medtronic will be a Data Processor for the data that they hold on behalf of the Trust in the CareLink system for clinicians. Medtronic will be a Data Controller for data collected through CareLink Personal. This data will in some cases be shared in a two way direction between the two Controllers if a patient chooses to link their CareLink Personal account to their CareLink system for clinicians.

2.5	If we have identified a supplier in 2.4, the following questions for 2.5 and 2.6 will need to be answered by the supplier and the Trust	
	Y/N	**If yes the third party will need to complete the following assessment. This will need to be provided in addition to the completion of this proforma. An example of a completed assessment is also provided below**  NHIS - Supplier Assurance Framework  Supplier Assurance Framework - Example
	Y	As per CareLink™ System Services Agreement Medtronic Limited act as a data processor for the services offered for CareLink System. Please note the following sub-processors / third parties engaged in the provision of the service are outlined in section 10 **1. Medtronic International Trading Sàrl ("Medtronic Europe") at Route du Molliau 31, CH - 1131 Tolochenaz.** Europe, Middle-East & Africa (EMEA) headquarters for Medtronic. Contains the regional functions for Marketing,

		Legal, and Operational support for the primary Medtronic businesses. **2. Medtronic B.V. with registered address at Industry Park Trilandis Earl Bakkenstraat 10, 6422 PJ, Netherlands.** European Operations Center for distribution and shared services. Provides support and dedicated staff to the Medtronic data centre at the Engie facility which houses the CareLink server for the collection and processing of patient and clinic CareLink data. **3. Medtronic Bakken Research Center B.V. ("BRC") with registered address at Endepolsdomein 5, 6229 GW Maastricht, Netherlands.** Provides internal Medtronic EMEA regional support for regulatory filings/approvals, research studies and analysis, and global translations. **4. Medtronic MiniMed, Inc. ("Medtronic"), at 18000 Devonshire Street, Northridge, California, 91325.** Global headquarters for the Medtronic Diabetes business unit. Supports the development and maintenance of diabetes products including insulin pumps, continuous glucose monitoring sensors, and software products including CareLink System. Supports tier 2 and 3 technical support. For all transfers of personal data to countries outside the EEA, Medtronic will transfer personal data only to countries outside the EEA on the basis of an adequacy decision of the European Commission or, where no adequacy decision is available, on the basis of standard data protection clauses adopted by the European Commission or any other legal ground explicitly allowed by the EU/UK GDPR. Copy of TASK1479370-Sherwo 9th June 2021 - This assessment provides for a suitable and sufficient assessment of risk and NHIS have no further observations or recommendations to make.

2.5.1	Please describe access and controls in place Account access management Standard Operating Procedure to be completed prior to the implementation of the project
	Medtronic CareLink™ System is a Class I CE Marked Medical Device which stores data in an ISO 27001 certified datacentre within the Netherlands. Engie Services Zuid B.V. (formerly known as Cofely Zuid Nederland BV) with registered address at Amerikalaan 35, 6199 AE Maastricht-Airport, Netherlands, provides the physical facility where the Medtronic data processing electronic equipment (e.g., the CareLink servers) are housed. Engie provides the secure facility, the room to house the equipment, power, and temperature control to the room. Engie does not support the Medtronic electronic equipment or process CareLink data, and as such are not deemed sub-processors of information. Data is stored at rest with AES 256 Encryption Keys. CareLink™ System is a web based interface and uses a https:// secure internet connection (see https://carelink.medtronic.eu/media/faq_emea.pdf for compatible browsers and OS requirements) with data being uploaded via the CareLink Uploader (available for download at https://carelink.medtronic.eu/public/uploaderInstructions.html). All data in transit uses TLS 1.2 encryption standards. **Trust access** - There is a two tier access for Trust users (administrator and user access) with the Trust able to determine which members of clinical or IT has access to the System. **Medtronic Access** - To support and provide appropriate Product support related to CareLink System, Medtronic may have access to data held within the platform. Please see obligations as stated within the CareLink™ System Services Agreement. Staff involved in processing patient data are appropriately trained and made aware of their confidentiality obligations. End user role-based access to data is restricted to authorised individuals. For further reassurance, Medtronic Limited have met standards outlined by NHS Digital (https://www.dsptoolkit.nhs.uk/OrganisationSearch/8HM01) and also hold ISO 9001 certification for Quality Management System (QMS) covering Medtronic's Policies, Systems and Processes (attached for reference)
2.5.2	Please provide a copy of the contract in place

	02A. Carelink System Services Contract (Dia Sherwood Forest NHS FT - CDA Signed		
2.5.3	Have arrangements for retention and destruction been included in the contract when the service/contract expires?		
	Medtronic Comment - As data controller, the Trust has the ability to request Medtronic permanently delete data subject information from CareLink Servers. Medtronic will action any such request so long as no legal or regulatory obligation prevents it from doing so. Any such request will mean data is erased at database level. Please note that Medtronic's data retention period is 10 years. Please also note CareLink reports (graphical representation of device data / patient produced by CareLink System) may be exported from the system in PDF format to be included into patient records as deemed appropriate by the Trust. Destruction of exported notes will need to be in line with Trust policies. Destruction of data upon end of contract with Medtronic. Medtronic's corporate data retention policy is 10 years. This will apply only to data held within CareLink Personal for which Medtronic is data controller. As data controller the Hospital may act upon data subject rights under GDPR. Where required and through a Product Support ticket request Medtronic can assist with erasure of data unless a legal or regulatory requirement prevents it from doing so. Data shall be kept for the life of the contact and upon termination / end of the contract all user-created data stored in CareLink System shall be exported as a standard gzipped tar archive (.tar.gz) to the Hospital, unless a legal or regulatory requirement prevents Medtronic from doing so.		
2.5.4	Is the supplier registered with the ICO? Please check the register	Yes	No
		x	
2.5.5	Has the supplier received ICO Enforcement? Please check the register	Yes	No
			x
2.5.6	Has the supplier received ICO Decision Notice? Please check the register	Yes	No
			x

2.5.7	Has the supplier received an ICO Audit? Please check the register		Yes	No
				x

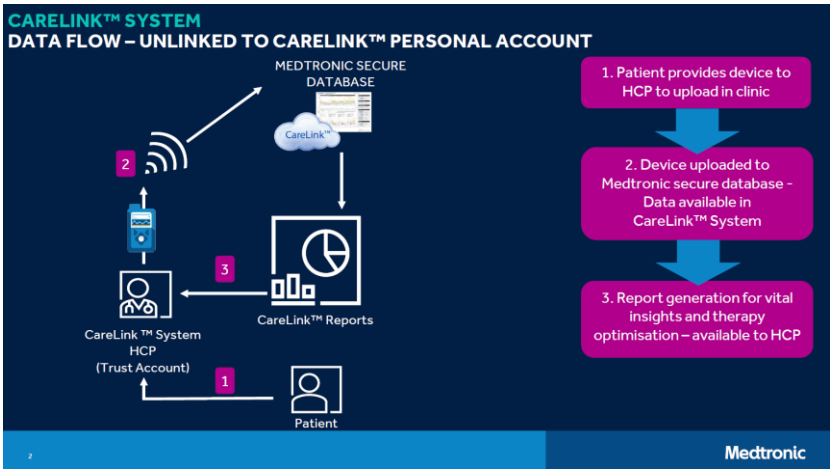
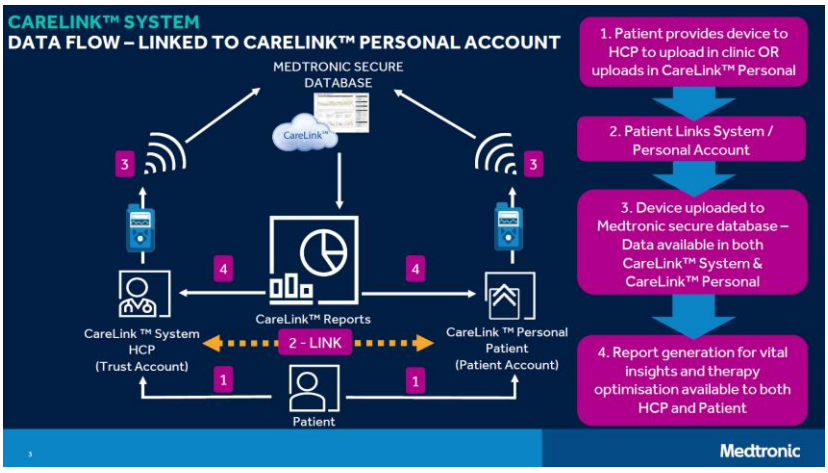
2.5.8	Has the supplier completed a Data Security and Protection Toolkit, please check the register and provide the following details	Completed: Yes/No	Date submitted	Standard Met/Not Met
		Yes	19/05/2021	Met

2.5.9	Can the supplier demonstrate compliance with any of the following standards? If YES please provide further information e.g. date achieved and a copy of the certificates		
		Yes	No
	Cyber Essentials Plus		x
	ISO 15489 Records Management		x
	ISO 27001 Information Security Standards	Note: CareLink™ System software is built to ISO standards. In addition see data centre ISO certification Global Security Office Customer Sta 07. ENGIE Services Smart Digital Operat	
	ISO 9001 Quality Management Systems	Yes	

		 2090418 (EN ISO 13485+9001) + ADD E	
2.5.10	Is the data held outside of the UK ie Europe, USA, Ireland? If yes please include the country		
	Yes	No	
	Netherlands		
	If yes we need to seek assurance that the data will continue to flow post Brexit 31.12.2020, provide further detail below from the supplier		
	Medtronic Limited in the UK will put appropriate international transfer safeguards in place to ensure that personal data transfers to and from the UK can continue in compliance with applicable data protection laws. Specifically, for CareLink™ System (Diabetes) Medtronic Limited in the UK makes use of the services of Medtronic affiliates based in the EU. We do not anticipate that there will be any barriers to maintaining the flow of UK personal data by your hospital as data controller to and from Medtronic Limited's sub-processor(s). We continue to monitor the legal position. Should it prove necessary, we are prepared to take additional appropriate steps to avoid any interruption in our services.		
2.6	Will this information be shared outside the organisations listed above?		
	Y/N	if answered **Yes** please describe organisation/s and geographic location	
	Y	Please note the following sub-processors / third parties engaged in the provision of the CareLink™ System service: **Sub-Processors:** **1. Medtronic International Trading Sàrl ("Medtronic Europe") at Route du Molliau 31, CH - 1131 Tolochenaz.** Europe, Middle-East & Africa (EMEA) headquarters for Medtronic. Contains the regional functions for Marketing, Legal, and Operational support for the primary Medtronic businesses.	

		2. Medtronic B.V. with registered address at Industry Park Trilandis Earl Bakkenstraat 10, 6422 PJ, Netherlands. European Operations Center for distribution and shared services. Provides support and dedicated staff to the Medtronic data centre at the Engie facility which houses the CareLink server for the collection and processing of patient and clinic CareLink data. **3. Medtronic Bakken Research Center B.V. ("BRC") with registered address at Endepolsdomein 5, 6229 GW Maastricht, Netherlands.** Provides internal Medtronic EMEA regional support for regulatory filings/approvals, research studies and analysis, and global translations. **4. Medtronic MiniMed, Inc. ("Medtronic"), at 18000 Devonshire Street, Northridge, California, 91325**. Global headquarters for the Medtronic Diabetes business unit. Supports the development and maintenance of diabetes products including insulin pumps, continuous glucose monitoring sensors, and software products including CareLink System. Supports tier 2 and 3 technical support. For all transfers of personal data to countries outside the EEA, Medtronic will transfer personal data only to countries outside the EEA on the basis of an adequacy decision of the European Commission or, where no adequacy decision is available, on the basis of standard data protection clauses adopted by the European Commission or any other legal ground explicitly allowed by the GDPR. Medtronic Limited has in place a standard contractual clause with its Medtronic USA counterpart to ensure sufficient data protection under EU/UK GDPR. Medtronic Limited in the UK will put appropriate international transfer safeguards in place to ensure that personal data transfers to and from the UK can continue in compliance with applicable data protection laws. Specifically for CareLink™ System (Diabetes), Medtronic Limited in the UK makes use of the services of Medtronic affiliates based in the EU. Based the current legal position as we understand it, we do not anticipate that there will be any barriers to maintaining the flow of UK personal data by your hospital as data controller to and from Medtronic Limited's sub-processor(s). We continue to monitor the legal position. Should it prove necessary, we are prepared to take

		additional appropriate steps to avoid any interruption in our services. **Third Parties (not deemed sub-processors):** ▪ **Engie Services Zuid B.V. (formerly known as Cofely Zuid Nederland BV) with registered address at Amerikalaan 35, 6199 AE Maastricht-Airport, Netherlands**. Provides the physical facility where the Medtronic data processing electronic equipment (e.g., the CareLink servers) are housed. Engie provides the secure facility, the room to house the equipment, power, and temperature control to the room. Engie does not support the Medtronic electronic equipment or process CareLink data. **Eurofibre Holding B.V. with its head office at Safariweg 25-31, 3605 MA Maarssen, Netherlands**. Provides telecommunications access for the Medtronic data processing electronic equipment (e.g., the CareLink servers). Eurofibre does not support the Medtronic electronic equipment or process CareLink data.
2.7	Does the work involve employing contractors external to the Organisation?	
	Y/N	If **Yes**, provide a copy of the confidentiality agreement or contract?
	Y	**1. Medtronic International Trading Sàrl ("Medtronic Europe") at Route du Molliau 31, CH - 1131 Tolochenaz.** Europe, Middle-East & Africa (EMEA) headquarters for Medtronic. Contains the regional functions for Marketing, Legal, and Operational support for the primary Medtronic businesses. **2. Medtronic B.V. with registered address at Industry Park Trilandis Earl Bakkenstraat 10, 6422 PJ, Netherlands.** European Operations Center for distribution and shared services. Provides support and dedicated staff to the Medtronic data centre at the Engie facility which houses the CareLink server for the collection and processing of patient and clinic CareLink data. **3. Medtronic Bakken Research Center B.V. ("BRC") with registered address at Endepolsdomein 5, 6229 GW Maastricht, Netherlands.** Provides internal Medtronic EMEA regional support for regulatory filings/approvals, research studies and analysis, and global translations.

		4. Medtronic MiniMed, Inc. ("Medtronic"), at 18000 Devonshire Street, Northridge, California, 91325. Global headquarters for the Medtronic Diabetes business unit. Supports the development and maintenance of diabetes products including insulin pumps, continuous glucose monitoring sensors, and software products including CareLink System. Supports tier 2 and 3 technical support. For all transfers of personal data to countries outside the EEA, Medtronic will transfer personal data only to countries outside the EEA on the basis of an adequacy decision of the European Commission or, where no adequacy decision is available, on the basis of standard data protection clauses adopted by the European Commission or any other legal ground explicitly allowed by the GDPR.
2.8	Has a data flow mapping exercise been undertaken?	
	Y/N	If **Yes**, please provide a copy here. If No, please explain why
	Y	 

	Have the information flows and assets that are identified within this DPIA been added to your departmental information flow map and asset register? If No, please explain why					
	N	Identified and recorded as a risk				
2.9	What format is the data?					
	Electronic	☒	Paper	☐	Other (Please describe)	Click here to enter text.

2.10	Is there an ability to audit access to the information?	
	Y/N	Please describe if answered **Yes.** If **NO** what contingencies are in place to prevent misuse?
	Y	02. CareLink System - Audit Log Example.pdf

2.11	Does the system involve new links with personal data held in other systems or have existing links been significantly changed?	
	Y/N	Please describe if answered **Yes**
	N	

2.12	How will the information be kept up to date and checked for accuracy and completeness? (data quality) How will you ensure data minimisation?
	Medtronic Comment - The following fields are present in CareLink™ System. * denotes mandatory field. This enables flexibility to meet minimisation techniques that the Trust may want to employ: Trust Administrator / Users: - Username* - Email Address* - Password* Patient Profile: - First / Last Name (Initials could be used if required)* - Date of Birth* - Device Serial Number* - Device Data (Insulin Pump data / continuous glucose monitor data) - Health data*

	- Diabetes Type - Email - Patient ID (could be NHS Number or other patient identifier) - Gender - Mobile / telephone Number - Notes (field to add notes at Trust discretion) The Trust will follow the procedures set out in the Data Quality Strategy
2.13	Who will have access to the information? (list individuals or staff groups)
	- Members of the Adult and Paediatric Diabetes team with a direct care relationship with the patient that is participating in the delivery of the insulin pump service. - Patient (If linked account) Medtronic Limited and its sub-processors for the provision of CareLink™ System service

2.14.1	What security measures have been implemented to secure access?	
	Active Directory (Window's username and password)	☐
	Username and password	☒
	Smartcard	☐
	Key locked filing cabinet/room	☐
	Hard/soft Token (VPN) Access	☐
	Restricted Access to Network Files (shared drive)	☐
	Has information been anonymised?	☐
	Has information been pseudonymised?	☐
	Is information fully identifiable?	☐
	Other (provide detail below)	☒

	Upon completion of a CareLink Contract – the Trust will be provided with a registration key to create a CareLink™ System Account. The initial user provided with a registration key will create the Trust account and then be able to create other users within the system. Each user will receive a link via email which they will need to confirm to gain access. Trust administrators will be able to tailor security settings (including password reuse, length, etc as well as two factor authentication) within the security section of their account.			
2.14.2	What physical security measures have been implemented to secure access? ie swipe cards, digilock			
	Access to CareLink will be via a username and password. Appropriate staff will be given access to the system. Trust devices will be locked when not in use			
2.15	Will the data be stored on Trust servers			
	Yes	No		
		X Note, the system can create PDF CareLink reports to visualise device data / usage which can be exported for storage on records in the Trust's records management system		
2.16	Please state by which method the information will be transferred?			
	Email (not NHS.net)	☐	NHS.net	☐
	Website Access (internet or intranet)	☒	Wireless Network (Wi-Fi)	☐
	Secure Courier	☐	Staff delivered by hand	☐
	Post (internal)	☐	Post (external)	☐
	Telephone	☐	SMS	☐

	Other	☐	please specify below	☐
	Data transferred via TLS 1.2 encryption (in transit)			

2.17	Are disaster recovery and business contingency plans in place for the information? What types of backups are undertaken i.e. full, differential or incremental?	
	Y/N	Please describe if answered **Yes.** Please state why not if response is **No.**
	Y	CareLink System: Database is backed up nightly for as part of Medtronic's BCP. ▪ **DC1 - Engie Services Zuid B.V. (formerly known as Cofely Zuid Nederland BV) with registered address at Amerikalaan 35, 6199 AE Maastricht-Airport, Netherlands.** Active CareLink Data Centre for CareLink™ SystemServices ▪ **DC2 - Medtronic. B.V., Eurofiber, Koningin Wilhelminaweg 471 Groenekan, Netherlands 3737 BE** Back up DC for tapeless back up (nightly) as part of Medtronic's Business Continuity Planning / Disaster Recovery Plan Service offered 98% availability (outside of maintenance periods, data centre down times, and natural disasters). In the Trust we have a business continuity plan if the service was unavailable. The department would default back to the current practice and access the information manually on the pump or over the phone with the patient reading out the information to us.

2.18	Has staff training been proposed or undertaken and did this include confidentiality and security topics areas?	
	Y/N	Please describe if answered **Yes**

	Y	**Medtronic Access** - To support and provide appropriate Product support related to CareLink System, Medtronic may have access to data held within the platform. Please see obligations as stated within the CareLink™ System Services Agreement. Staff involved in processing patient data are appropriately trained and made aware of their confidentiality obligations. End user role-based access to data is restricted to authorised individuals. For further reassurance, Medtronic Limited have met standards outlined by NHS Digital (https://www.dsptoolkit.nhs.uk/OrganisationSearch/8HM01) and also hold ISO 9001 certification for Quality Management System (QMS) covering Medtronic's Policies, Systems and Processes (attached for reference) Medtronic will provide training to Trust staff on the use of the system

2.19	Will reports be produced?	
	To assist in the provision of direct care for patients using Medtronic insulin devices, CareLink™ System is able to generate a variety of reports to help visualise information and is an important tool used by the clinical team in optimisation of therapy. Medtronic has the following certifications: - CareLink™ System is a CE Marked Class I Medical Device - Built to ISO 27001 Standards (resides in a certified ISO 27001 data centre, hosted within the EEA) - Medtronic Limited meets standards as set out in the NHS DPS Toolkit - https://www.dsptoolkit.nhs.uk/OrganisationSearch/8HM01) Medtronic Limited is ISO 9001 certification for Quality Management System (QMS) covering Medtronic's Policies, Systems and Processes (attached for reference)	
	Will reports contain personal/sensitive personal or business confidential information?	CareLink™ System is designed to produce a variety of reports to aid health care professionals in therapy management. Reports contain

		patient health information, patient device usage information as well as glycaemic control information.
	Who will be able to run reports?	Trust employees who have been granted access to CareLink™ System by the Trust CareLink™ System administrator
	Who will receive the reports and will they be published?	Reports to be used by Diabetes clinical team / patient to optimise therapy management

2.20	If this new/revised function should stop, are there plans in place for how the information will be **retained / archived/ transferred or disposed of?**	
	Y/N	Please describe if answered **Yes.** Please state why not if response is **No.**
	Y	CareLink System: Database is backed up nightly for as part of Medtronic's BCP. ▪ **DC1 - Engie Services Zuid B.V. (formerly known as Cofely Zuid Nederland BV) with registered address at Amerikalaan 35, 6199 AE Maastricht-Airport, Netherlands.** Active CareLink Data Centre for CareLink™ SystemServices

		▪ **DC2 - Medtronic. B.V., Eurofiber, Koningin Wilhelminaweg 471 Groenekan, Netherlands 3737 BE** Back up DC for tapeless back up (nightly) as part of Medtronic's Business Continuity Planning / Disaster Recovery Plan Service offered 98% availability (outside of maintenance periods, data centre down times, and natural disasters). In the Trust we have a business continuity plan if the service was unavailable. The department would default back to the current practice and access the information manually on the pump or over the phone with the patient reading out the information to us.
2.21	Is consent required for processing of personal data?	
	Y/N	Please describe if answered **Yes**
		As data controller, the Trust administrator / user are able to update information of patients held within CareLink™ System (with the exception of device data which cannot be altered) in accordance with Trust policy. Device data uploaded to the system comes directly from the Medtronic device and as such cannot be altered / amended in any way. To ensure up to date device data is available the Trust will be able to upload a patient device to CareLink™ System via the web interface and using the CareLink Uploader (available at https://carelink.medtronic.eu/public/uploaderInstructions.html). Alternatively, the patient may provide explicit consent to link their CareLink™ Personal account with their profile in the Trust CareLink™ System account, thus providing access to data uploaded by the patient at home to the Trust.
		If **No**, list the reason for not gaining consent e.g. relying on an existing agreement, consent is implied, the project has s251 approval or other legal basis?

	N	To provide direct care to the patient as part of our statutory functions
2.22	Will individuals be informed about the proposed uses and share of their personal data?	
	Y/N	Please describe if answered **Yes.** Please state why not if response is **No.**
		As data controller it is the responsibility of the Trust to ensure that any additional consent that is required falls in line with Trust policy. It could be considered that additional consent is not required as use of CareLink™ System falls under direct care of the patient (Article 9, h of GDPR legislation). If the Trust feels that additional consent is required from the patient, they may wish to use their own consent form (however Medtronic is able to provide a model consent form for adoption by the Trust should this be required) - CareLink information is available to patients at https://www.medtronic-diabetes.co.uk/carelink - To link the patients account with the CareLink™ System patient profile the patient is required to provide explicit consent to establish the link by entering their username and password to acknowledge the confirmation. The following statement appears: - ***Link CareLink™ Personal to your hospital's CareLink™ System record*** By pushing the Link button, you provide your explicit consent that your medical provider can access and process the device data that you upload in CareLink™ Personal. You can withdraw your consent by going to CareLink™ Personal and removing your link with the hospital; this will stop any further sharing of your future CareLink™ Personal data with the CareLink™ System. For more information with regards to the processing of your CareLink™ Personal data in the CareLink™ System by your health care provider, please consult with your medical provider as to how your medical data will be processed.

		By linking CareLink™ Personal to your hospital's CareLink™ System record, you will also be able to access in CareLink™ Personal your device data uploaded by your health care provider in hospital's CareLink™ System record. Please take into account that, when you provide or have provided consent to Medtronic to further use your CareLink™ Personal data for Medtronic's scientific research, product improvement and/or analytical purposes, after linking, Medtronic's use will include your device data uploaded by your health care provider in hospital's CareLink™ System record provided that your hospital has agreed for Medtronic to use such CareLink™ System data. - Links to CareLink™ Personal Terms & Condition / Privacy Links can be found here: ▪ https://carelink.minimed.eu/help/en/privacyPolicy.pdf ▪ https://carelink.minimed.eu/help/en/termsOfUse.pdf - Links to CareLink™ System Terms & Condition / Privacy Links can be found here: ▪ https://carelink.medtronic.eu/public/privacyPolicy.html ▪ https://carelink.medtronic.eu/public/termsOfUse.html The Trust's privacy notice has been updated with the following information: **CareLink™ System** CareLink™ System is a service provided by Medtronic to health care professionals to upload patient insulin pumps, continuous glucose monitor devices and compatible BG meters. This enables health care professionals to generate reports to assist with patient's diabetes management. health care professional's may create a patient profile in the system and upload a patients compatible device in clinic to see data from their device or request that the patient links their CareLink Personal™ with the clinic so that data patients

		upload at home can be viewed in CareLink™ System by the health care professional. Further information is available here.
2.23	Is there a process in place to remove personal data if data subject refuses/removes consent	
	Y/N	Please describe if answered **Yes.** Please state why not if response is **No.**
	Y	MEDTRONIC NOTE: As data controller it is for the Trust to manage additional consent and opt out / objection as per Trust policy. As per Medtronic's Obligations detailed in Exhibit III Article 3.3 of the CareLink™ System Services Agreement -. Medtronic shall assist the Hospital promptly with all Data Subject rights request (including in relation to subject access, rectification, erasure, restriction, data portability and other data protection related requests, or inquiries and complaints which may be received from Data Subjects and/or from data protection authorities, and to notify the Hospital promptly if Medtronic receives any such request, inquiry or complaint in relation to Personal Data obtained via the Hospital. For any Data Subject right requests, inquiries and complaints, the Hospital can contact Medtronic through the regular channels.
2.24	How much control will they have? Would they expect you to use their data in this way?	
	Y/N	Please describe if answered **Yes.** Please state why not if response is **No.**
		MEDTRONIC NOTE: As data controller it is for the Trust to determine which consent (if required) they wish to rely on. Please note, it could be considered as part of a patients direct care (Article 9 h GDPR) as they are using a Medtronic insulin pump. If explicit consent is required by the Trust policy as per CareLink™ System Service agreement Medtronic request that this consent is recorded appropriately.

2.25	Are arrangements in place for recognising and responding to requests for access to personal data?	
	Y/N	Please describe if answered **Yes.** Please state why not if response is **No.**
		MEDTRONIC NOTE: As data controller it is for the Trust to manage additional consent and opt out / objection as per Trust policy. As per Medtronic's Obligations detailed in Exhibit III Article 3.3 of the CareLink™ System Services Agreement -. Medtronic shall assist the Hospital promptly with all Data Subject rights request (including in relation to subject access, rectification, erasure, restriction, data portability and other data protection related requests, or inquiries and complaints which may be received from Data Subjects and/or from data protection authorities, and to notify the Hospital promptly if Medtronic receives any such request, inquiry or complaint in relation to Personal Data obtained via the Hospital. For any Data Subject right requests, inquiries and complaints, the Hospital can contact Medtronic through the regular channels. In addition, clinic administrator's ad users can rectify Personally identifiable data under patient profiles within CareLink™ System (with the exception of downloaded device data which cannot be altered). **A) Right to be Informed** - As data controller, it is up to the Trust to policy to confirm is data subject consent is required or whether use of CareLink™ System by the Trust constitutes part of patients Direct Care and falling within GDPR Article 9 (h) **B) Right of Access** - Staff involved in processing patient data are appropriately trained and made aware of their confidentiality obligations. End user role-based access to data is restricted to authorized individuals. A hospital appointed employee is designated as the initial clinic administrator, who has the privileges to provision, deactivate, grant admin rights or manage other user accounts. At the request to Medtronic Product Support, all user-created data stored in

		CareLink™ System can be exported as a standard gzipped tar archive (.tar.gz). **C) Right of Rectification** - Medtronic design our solutions in a way that enables product owners (clinic users / administrators) to see, change, or delete relevant personal data as prescribed by law **D) Right of Erasure -** To the extent possible, data can be erased upon the request of the account owner (clinic user / admin). Permanent deletion at database level can be requested to Medtronic via a support ticket, so long as there is no legal obligation preventing Medtronic from doing so **E) Restriction of Processing Data** - will only be processed to the extent where it is necessary to provide the intended services and functionality for the product, and to deliver services that the account owner has provided their explicit and voluntary consent. **F) The Right to Object –** As data controller, the Trust is responsible for handling a patient's right to objection in line with its policy. As a note, if a patient does link their CareLink™ Personal account with their profile in the Trusts CareLink™ System account they can subsequently object and revoke the linking in CareLink Personal **G) The right to data portability** at the request to Medtronic Product Support, all user-created data stored in CareLink™ System can be exported as a standard gzipped tar archive (.tar.gz). The Trust has a policy and procedure for responding to subject access requests. Further information for patients on how to access their records is here: Sherwood Forest Hospitals (sfh-tr.nhs.uk)
2.26	Who are the Information Asset Owner(s) and Administrator(s)?	
	IAO	Rachel Briggs and Lisa Gowan

	IAA	Elaine Higgins and Dr Ursula Ngwu
	System Administrators	Elaine Higgins and Dr Ursula Ngwu

2.27	How is the data secured in transit and at rest? Eg encryption, port control number	
	Data transfers to CareLink use TLS 1.2 and are encrypted via AES 256 Encryption Keys	
2.28	Has the impact to other NHIS systems/processes been considered and appropriate SBU's consulted and in particular technical security?	
	Y/N	Please describe if answered **Yes.** Please state what checks were undertaken if response is answered **No.**
	Y	A patient safety case and supplier assurance framework have both been reviewed by NHIS. No risks or recommendations identified.
2.29	Are there any current issues of public concern that you should factor in?	
	Y/N	Please describe if answered **Yes.**
	N	
2.30	What do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for you, and more broadly?	
	To improve the management of patients with diabetes	
2.31	Consider how to consult with relevant stakeholders: • Describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. • Who else do you need to involve within your organisation? • Do you need to ask your processors to assist?	
	Medtronic will support the Trust by providing the necessary feedback on CareLink™ System technical and GDPR aspects. Medtronic presented this document to the Information Governance working group for consultation.	

2.32	What is your lawful basis for processing? (please see Appendix 10 Information Sharing Protocol for further information). **Consent is usually the last basis to rely on** **Legal basis: patients** **Personal data i.e. name, address** 6(1)(a) the patient has given consent 6(1)(c) necessary for legal obligations 6(1)(e) public interest or public duty 6(3) the above supported by Member State law (UK legislation as applicable to circumstances) **Sensitive personal data (special category)** 9(2)(a) the patient has given explicit consent 9(2)(c) processing for 'vital interests' (safety, safeguarding, public safety, etc.) 9(2)(h) allows processing for the provision of healthcare (direct care) or the management of healthcare systems (invoice validation, commissioner reporting, quality audits – essentially, mandated activity). 9(2)(i) allows processing for "ensuring high standards of quality and safety of health care." – which would cover research, audit, service improvement and addressing public health/inequalities. 9(2)(j) (together with Article 89 and relevant recitals) relates to archiving, statistical analysis and research. **Legal basis: staff** – please review Appendix 10 Information Sharing Protocol for further information).
	Trust 6(1)(e) public interest or public duty 9(2)(h) allows processing for the provision of healthcare (direct care) or the management of healthcare systems (invoice validation, commissioner reporting, quality audits – essentially, mandated activity). **Medtronic**

	6(1)(e) public interest or public duty 9(2)(h) allows processing for the provision of healthcare (direct care) or the management of healthcare systems (invoice validation, commissioner reporting, quality audits – essentially, mandated activity).
2.33	What information will you give individuals about the processing? (This information will be added to the Trust's Patient Privacy Notice and Staff Privacy Notice by the Information Governance Team)
	As data controller it is the responsibility of the Trust to ensure that any additional consent that is required falls in line with Trust policy. It could be considered that additional consent is not required as use of CareLink™ System falls under direct care of the patient (Article 9, h of GDPR legislation). If the Trust feels that additional consent is required from the patient, they may wish to use their own consent form (however Medtronic is able to provide a model consent form for adoption by the Trust should this be required) - CareLink information is available to patients at https://www.medtronic-diabetes.co.uk/carelink - To link the patients account with the CareLink™ System patient profile the patient is required to provide explicit consent to establish the link by entering their username and password to acknowledge the confirmation. The following statement appears: - **Link CareLink™ Personal to your hospital's CareLink™ System record** By pushing the Link button, you provide your explicit consent that your medical provider can access and process the device data that you upload in CareLink™ Personal. You can withdraw your consent by going to CareLink™ Personal and removing your link with the hospital; this will stop any further sharing of your future CareLink™ Personal data with the CareLink™ System. For more information with regards to the processing of your CareLink™ Personal data in the CareLink™ System by your health care provider, please consult with your medical provider as to how your medical data will be processed. By linking CareLink™ Personal to your hospital's CareLink™ System record, you will also be able to access in CareLink™ Personal your device data uploaded by your health care provider in hospital's CareLink™ System record. Please take into account that, when you provide or have provided consent to Medtronic to further use your CareLink™ Personal data for Medtronic's scientific research, product improvement and/or analytical purposes, after linking, Medtronic's use will include your device data uploaded by your health care provider in hospital's CareLink™

	System record provided that your hospital has agreed for Medtronic to use such CareLink™ System data. - Links to CareLink™ Personal Terms & Condition / Privacy Links can be found here: ▪ https://carelink.minimed.eu/help/en/privacyPolicy.pdf ▪ https://carelink.minimed.eu/help/en/termsOfUse.pdf - Links to CareLink™ System Terms & Condition / Privacy Links can be found here: ▪ https://carelink.medtronic.eu/public/privacyPolicy.html ▪ https://carelink.medtronic.eu/public/termsOfUse.html The Trust's privacy notice has been updated. Patients are informed during a consultation with clinicians and the devices being given to them.

2.34	What measures do you take to ensure processors comply?
	Medtronic will support the Trust by providing the necessary feedback on CareLink™ System technical and GDPR aspects. Annual assurance will need to be obtained from Medtronic via the Information Asset Owner in relation to the certification of ISO:27001
2.35	How will you prevent function creep? Manage lifecycle of system/process
	In order to prevent function creep, processing activity will be carried out on behalf of the Trust by Medtronic that is agreed to. The CareLink™ System Service Agreement provides explicit information on processing activity provided by Medtronic as part of offering the CareLink™ System service. CareLink™ System is set up with the view to provide health care professionals within the Trust information on patients using Medtronic Insulin pumps and continuous glucose monitor devices. As such, there is limited scope to utilise the platform for other functions within the Trust. As data controller, the Trust has full responsibility for ensuring health care professionals accessing the system utilise it appropriately.

Stage - 3 Risk Template

For advice on completing this Risk Template please contact the Risk & Assurance Manager on x6326

Completed by Gina Robinson	Role: Information Security Officer	Date completed: 13th July 2021

Risk description What event could happen which would impact on the activity? What would cause it to happen? What would the consequence be?	**Primary controls** What is in place now to prevent the risk from occurring or to act as a contingency if it does occur?	**Current risk**			**Gaps in control** If the risk is not controlled to an acceptable level, what are the issues that need to be addressed?	**Acceptable risk**			**Mitigating actions required** What needs to be done to reduce the risk to an acceptable level?
		Consequence	**Likelihood**	**Rating (C x L)**		**Consequence**	**Likelihood**	**Rating (C x L)**	
Medical devices will be plugged into Trust ports and will need to be added to the whitelist	Cyber Security Programme Board and NHIS whitelisting procedure	2	2	4	A call will need to be raised with the Cyber Security team (NHIS) for the medical devices to be added to the whitelist	2	1	**2**	A call will need to be raised with the Cyber Security team (NHIS) for the medical devices to be added to the whitelist
If the system is not recorded on the information asset register, the system may not be brought back online in response to a cyber attack	In the Trust we have a business continuity plan if the service was unavailable. The department would default back to the current practice and access the information manually on the pump or over the phone with the patient reading out the information to us.	2	2	4	CareLink will need to be added to both the Women and Children's and Medicine's divisional information asset register and the data flows mapped and recorded as part of the annual IAO returns to the SIRO	2	1	**2**	CareLink will need to be added to both the Women and Children's and Medicine's divisional information asset register and the data flows mapped and recorded as part of the annual IAO returns to the SIRO

Risk Scoring Matrix.pdf

Stage – 4 Legal Compliance

Compliance to be determined by IG team from the responses provided in the previous stages, delete as appropriate:

Data Protection Act 2018	Compliance and Comment
Principle 1 – Personal data shall be processed fairly and lawfully and, in a transparent manner	Lawfulness • We have identified an appropriate lawful basis (or bases) for our processing. • We are processing special category data and have identified a condition for processing this type of data. • We don't do anything generally unlawful with personal data. Fairness • We have considered how the processing may affect the individuals concerned and can justify any adverse impact. • We only handle people's data in ways they would reasonably expect, or we can explain why any unexpected processing is justified. • We do not deceive or mislead people when we collect their personal data. Transparency • We are open and honest, and comply with the transparency obligations of the right to be informed.
Principle 2 – Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes	• We have clearly identified our purpose or purposes for processing. • We have documented those purposes. • We include details of our purposes in our privacy information for individuals. • We regularly review our processing and, where necessary, update our documentation and our privacy information for individuals. • If we plan to use personal data for a new purpose other than a legal obligation or function set out in law, we check that this is compatible with

	our original purpose or we get specific consent for the new purpose.
Principle 3 – Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed	• We only collect personal data we actually need for our specified purposes. • We have sufficient personal data to properly fulfil those purposes.
Principle 4 – Personal data shall be Accurate and, where necessary, kept up to date, having regard to the purposes for which they are processed, are erased or rectified without delay	• We ensure the accuracy of any personal data we create. • We have appropriate processes in place to check the accuracy of the data we collect, and we record the source of that data. • We have a process in place to identify when we need to keep the data updated to properly fulfil our purpose, and we update it as necessary. • If we need to keep a record of a mistake, we clearly identify it as a mistake. • Our records clearly identify any matters of opinion, and where appropriate whose opinion it is and any relevant changes to the underlying facts. • We comply with the individual's right to rectification and carefully consider any challenges to the accuracy of the personal data. • As a matter of good practice, we keep a note of any challenges to the accuracy of the personal data
Principle 5 – Kept no longer than is necessary	• We know what personal data we hold and why we need it. • We carefully consider and can justify how long we keep personal data. • We have a policy with standard retention periods, however due to the Goddard Inquiry no destruction or deletion of patient records is to take place until further notice.
Principle 6 – Appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage	• We undertake an analysis of the risks presented by our processing, and use this to assess the appropriate level of security we need to put in place.

	• We have an information security policy (or equivalent) and take steps to make sure the policy is implemented. We have put in place technical controls such as those specified by established frameworks like Cyber Essentials. • We use encryption. • We understand the requirements of confidentiality, integrity and availability for the personal data we process. • We make sure that we can restore access to personal data in the event of any incidents, such as by establishing an appropriate backup process. • We conduct regular testing and reviews of our measures to ensure they remain effective, and act on the results of those tests where they highlight areas for improvement. • We implement measures that adhere to an approved code of conduct or certification mechanism. • We ensure that any data processor we use also implements appropriate technical and organisational measures.