Healthier Communities, Outstanding Care

Sherwood Forest Hospitals NHS Foundation Trust

Data Protection Impact Assessment

Title	Ref number
Medtrum EasyView website and EasyTouch App	

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:	Medtrum EasyView Pro website (the Trust) and EasyTouch App (Patient)

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

Historically, all measured glucose values and insulin injection history were uploaded when the pump or personal diabetes manager was connected to the computer. The data was not shared in real-time.

The aim of this project is to enable the caregivers and healthcare professionals to remotely monitor the patients' real-time glucose data and insulin delivery data, view the statistics and create the reports on the EasyTouch App and EasyView Pro website.

Once the patients accept the request sent by the caregivers or the healthcare professionals, the patient data will be shared remotely and in real-time.

There are 3 different Apps for patients, depending on what they are using in terms of pump and/or continuous glucose monitor.

1. EasyTouch App is for patients using the pump standalone or the pump and continuous glucose monitor together. This App stores the data from the pump and continuous glucose monitor if being used together (via the Personal Diabetes Manager – controller)

2. EasySense App is for patients who are using the continuous glucose monitor standalone. This takes the readings directly from the continuous glucose monitor to the App.

3. EasyPatch App is for patients who have decided to control their pump (and continuous glucose monitor if using together) using their smart phone rather than the Personal Diabetes Manager. This takes the data straight from the pump and continuous glucose monitor if using together as a system.

All the data from the Apps is uploaded automatically to the secure Cloud, which is accessed by Healthcare Professionals via the web based EasyView Pro – permission is needed from the patient to allow their data to be seen.

There is also an App for parents/carers/loved ones which is called the EasyFollow App which allows them to see the data form the pump and/or continuous glucose monitor – permission is needed from the patient for this.

Overview of the proposal: What the project aims to achieve

The purpose of the EasyTouch App (patients) and EasyView Pro website (the Trust) is to provide a diabetes management service, which stores patient information, a personal email address and diabetes health data. The EasyTouch App can be used with the EasyView Pro website, displaying real time insulin pump and continuous glucose monitoring data in intuitive graphs and uploading the data to the Medtrum Cloud. Real-time glucose monitoring gives patients continuous 24-hour care, comprehensive statistics and intuitive graphs help patients evaluate and improve their glucose control and share glucose information with loved ones or healthcare professionals at their convenience.

Implementing Organisation:	Sherwood Forest Hospitals NHS Foundation Trust

Staff involved in DPIA assessment (Include Email Address):	Elaine Higgins, Diabetes Specialist Nurse Luj@medtrum.com

Project Sign Off

	Name	Job Title	Organisation	Date
Information Asset Owner	Siobhan Favier (Medicine) and Lisa Gowan (Women and Children's)	Divisional General Manager	Sherwood Forest Hospitals NHS Foundation Trust	**12th April 2022**
Information Governance	Gina Robinson	Information Security Officer	Sherwood Forest Hospitals NHS Foundation Trust	**11th March 2022**
Data Protection Officer	Jacquie Widdowson	Information Governance Manager	Sherwood Forest Hospitals NHS Foundation Trust	**11th April 2022**
Senior Information Risk Owner	Shirley Higginbotham	Director of Corporate Affairs	Sherwood Forest Hospitals	**11th April 2022**

			NHS Foundation Trust	
Caldicott Sign Off	David Selwyn	Medical Director	Sherwood Forest Hospitals NHS Foundation Trust	**23rd May 2022**
Chief Clinical Information Officer	David Selwyn	Medical Director	Sherwood Forest Hospitals NHS Foundation Trust	**23rd May 2022**

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: **Legislative Compliance:** Article 6(1)(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. Article 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)

Article 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

Summary of Risks:
Cyber security, loss of data, inappropriate access to data, inability to access data and Information Asset Management.

Risks

1. Loss of system access and or data - Full system back-up process in place
2. Leavers’ access not removed – Diabetes team to manage starters and leavers process in the team, which could lead to inappropriate access to data.
3. Business continuity plans in each area, users have business continuity plans for their areas/departments. Not having these could lead to access to data problems or service delivery problems.
4. Medtrum EasyView Pro will need to be added to both the Women and Children’s and Medicine’s divisional information asset registers and the data flows mapped and recorded as part of the annual IAO returns to the SIRO. Failure to add these may result in the system not being brought back online in response to a cyber attack

Recommendations for Action

Summary of Identified Recommendations:		
Recommendations:	**Recommendation Owner:**	**Agreed Deadline for action:**
Information Asset Administrators to ensure Medtrum EasyView Pro is added to the information asset register and data flows are mapped and recorded	IAA	31st March 2022
Ensure business continuity plans are in place	IAA	31st March 2022
Account management Standard Operating Procedure generated and implemented, routine audit to take place		30th September 2022

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	Yes. Data is collected from the insulin pump and glucose sensor. However, the patient themselves could decide whether to upload the data to the App or not. The patients information can only be shared with his/her consent. Any personnel/organisation without permission from the patient will not be able to access the data.
2	Will the project compel individuals to provide information about themselves?	N	
3	Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?	N	
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?	N	
5	Are there processes in place to ensure data is relevant, accurate and up-to-date?	Y	Yes. The data transmission between different Medtrum devices, and between a Medtrum device and a mobile App adopts the Bluetooth technology. CRC16 check algorithm is used to ensure data accuracy. The data transmission between the App and the server, and between the server and a website adopts the Transmission Control Protocol/Internet Protocol to ensure data accuracy. Medtrum only collects data needed for specified purposes.

Q	Screening question	Y/N	Justification for response
			If a Medtrum medical device or a Medtrum App does not receive information as expected, it will send an alert or reminder. Once a user uploads device data, the data will be updated to the server.
6	Are there security arrangements in place while the information is held?	Y	Yes. Different types of users have different access levels. The patient's own their health data, as they can upload, download, or delete their data. Once deleted by the patient the Trust will no longer have access to the data. Caregivers/healthcare professionals, once authorised by a patient, can view, and download the patient's data. Creating, access and download of data is logged including time/account/action. The logging record is kept for 2 years. The server and storage are installed with Security components. A firewall is sued to filter malicious access. Intrusion detection is used to detect system anomalies. Malicious code protection is used to perform security checks on all committed data. The website does not have multifactor authentication and allows passwords as low as 6 characters. Trust staff have been advised to use the 3 random words in creating their passwords in line with the Password Management Procedure https://www.sfh-tr.nhs.uk/media/13059/ig-013-password-management-procedure-version-1.pdf
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?	N	9th December 2021 - the Insulin isn't adjusted remotely as part of the project as it is not possible for the insulin dose to be

Q	Screening question	Y/N	Justification for response
			adjusted remotely by a third party, but that the data will be used to inform adjustment by the specialist team. A patient safety case has been conducted and signed off by the Trust.
10	Is a Quality Impact/Technical Security Review required?	Y	11th November 2021 - NHIS have reviewed the supplier assurance framework and Cloud risk assessment and have not identified any concerns or recommendations. Medtrum is ISO27001 certified.

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	☐
	Another unique identifier (please specify)		Height, weight, Diabetes type, email address			
	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					
	Data will be sent using HL7. SSL (Security Socket Layer) and HTTPS (Hypertext Transfer Protocol over Secure Socket Layer) are used in the encrypted transmission of data.					

2.3	Is the data required to perform the specified task?	
	Y/N	Please justify response **Yes or No**
	Y	Personal data will be used by the Trust to identify the patients and monitor the patient's sensor data and pump data via the website.
2.3.1	How will you collect, use, store and delete data?	
	Data is collected from the diabetes medical device. The patients can decide whether to upload and share the data or not. If the patients do not want to share the data, he or she can use the personal diabetes manager (Personal Diabetes Manager) to control the insulin pump and continuous glucose monitoring (continuous glucose monitor). In this case, the data would not be uploaded to the EasyView Pro website. Patient information can only be shared with his/her consent. Exceptions to the requirement for consent are limited to: • A legal reason to disclose information, e.g., by Acts of Parliament or court orders. • A public interest justification for breaching confidentiality such as a serious crime. A patient can decide what data is shared and who the data is shared to. Only data needed is stored and processed in the Cloud server in Germany. All data will be stored in the Cloud for 2 years and automatically deleted. The patient can delete their own data whenever they want.	
2.3.2	What is the source of the data? (i.e. from data subject, system or other third party)	
	The patient is the source of the data. The data is stored in Medtrum medical devices originally, such as the insulin pump and continuous glucose monitoring system, and the control system, such as personal diabetes manager and affiliated Mobile applications. The devices are held by the patient.	

2.3.3	How much data will you be collecting and using?
	The data will be collected from the diabetes medical device provided by Medtrum. It includes sensor glucose, meter blood glucose which are used to calibrate the sensor, for insulin delivery records, and the settings of the device.
2.3.4	How often? (for example, monthly, weekly)
	During usage the continuous glucose monitoring data is collected once every 2 minutes with EasySense App and EasyPatch, the pump data is collected once the user uploads the data with EasyTouch App and EasyPatch App.
2.3.5	How long will you keep it? https://www.nhsx.nhs.uk/information-governance/guidance/records-management-code/records-management-code-of-practice-2021/
	All data will be stored in the App for 90 days, and in the EasyView Cloud Server for 2 years.
2.3.6	Where will the data be stored? i.e., CareFlow EPR, Shared Drive, offsite storage
	Data is stored in a Cloud data center located in Frankfurt am Main, Germany.
2.3.7	How many individuals are affected?
	The number of affected individuals is around 400.
2.3.8	What geographical area does it cover?
	Mansfield, Ashfield, Newark, Sherwood Derbyshire, Lincolnshire and Bassetlaw patients.

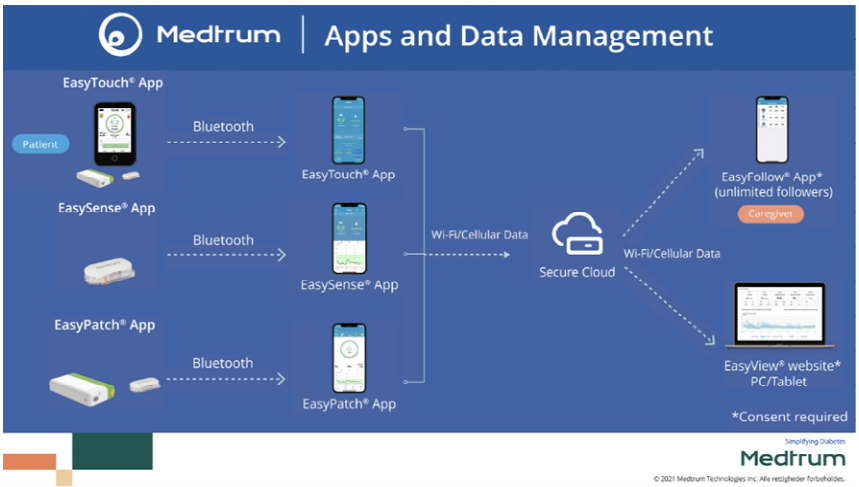
2.4	Who are the Organisations involved in processing (sharing) the data?	
	Organisations Name	Data Controller or Data Processor *The **Data Controller** is a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data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

	Patient	Data Controller
	Medtrum Ltd	Data Controller and Processor
	Sherwood Forest Hospitals NHS Foundation Trust	Data Controller and Processor

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
		 NHIS - Supplier Assurance Framework  Copy of Medtrum Cloud Assessment (0C NHIS have reviewed the attachments and assessed as low risk. In addition the systems used have accreditation with NHS Digital.
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 https://www.sfh-tr.nhs.uk/media/12007/ig-012-account-management-and-access-policy-2021.pdf  Account Management & Acces	
	Medtrum retain a secure record of the data in the Cloud and the data is only accessible to the individual and the organisations/individuals the patient wishes to share with. In order to ensure the confidentiality of patients' data, Medtrum have taken the following measures: 1. A verification code is required to register a Medtrum account. 2. Different types of users have different access levels.	

	Patients own their health data. They can upload, download or delete their data. Caregivers, once authorised by a patient, can view and download the patient data. Healthcare professionals, once authorised by a patient, can view and download the patients data. Each user needs a Medtrum account and password to access data. The password strength is high. The Trust will have administrators within the adult and paediatric team who will invite others to join and be able to monitor their access. SOP Medtrum Easyview Pro.docx			
2.5.2	Please provide a copy of the contract in place			
	Sherwood Forest MOA LPP Framew			
2.5.3	Have arrangements for retention and destruction been included in the contract when the service/contract expires?			
	No			
2.5.4	Is the supplier registered with the ICO? Please check the register		Yes	No
			ZA429918	
2.5.5	Has the supplier received ICO Enforcement? Please check the register		Yes	No
				No
2.5.6	Has the supplier received ICO Decision Notice? Please check the register		Yes	No
				No
2.5.7	Has the supplier received an ICO Audit? Please check the register		Yes	No
				No
2.5.8	Has the supplier completed a Data Security and Protection Toolkit, please	Completed: Yes/No	Date submitted	Standard Met/Not Met
		Yes	23rd November 2021	Standards exceeded

	check the register and provide the following details			
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		No	
	ISO 15489 Records Management		No	
	ISO 27001 Information Security Standards	Yes		
	ISO 9001 Quality Management Systems		No	
2.5.10	Is the data held outside of the UK ie Europe, USA, Ireland? If yes please include the country			
	Yes		No	
	Yes, Germany			
	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			
	The data will continue to flow from Germany			
2.6	Will this information be shared outside the organisations listed above?			
	Y/N	if answered **Yes** please describe organisation/s and geographic location		

	N					
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	Sherwood Forest MOA LPP Framew				
2.8	Has a data flow mapping exercise been undertaken?					
	Y/N	If **Yes**, please provide a copy here. If No, please explain why				
	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					
	Y	Data is collected from the diabetes medical device. The data is insulin delivery history and glucose data, which cannot be changed. The Trust will need to map the flow of data for this service. Added as a risk to the DPIA. 				
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	All diabetes health data such as glucose value and insulin pump delivery are only accessible to the customer/user/account owner.

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?
	Accuracy: The data transmission between different Medtrum devices, and between a Medtrum device and a mobile app adopts the Bluetooth technology. CRC16 check algorithm is used to ensure data accuracy. The data transmission between an app and the server, and between the server and a website adopts the Transmission Control Protocol/Internet Protocol to ensure data accuracy. Up to date: If a Medtrum medical device or a Medtrum app does not receive information as expected, it will send an alert or reminder. Once a user uploads device data, the data will be updated in the server. Data minimisation: We only collect and keep patients' insulin pump history (bolus, basal, alarms), continuous glucose monitoring (continuous glucose monitor) history (readings, calibrations, alerts) and entered events for the patients and clinicians to review.
2.13	Who will have access to the information? (list individuals or staff groups)
	A patient is informed why we are collecting their information, what we are going to do with it and who we may share it with through the Privacy Policy (http://www.medtrum.com/privacy-policy) in our website and apps. Once permitted, the caregivers and Healthcare providers can use the EasyFollow App to download the data from the cloud server and monitor the patient's Patch Pump and continuous glucose monitoring (continuous glucose monitor) system data. The Patients, caregivers and Healthcare providers can also view the data and print the reports on EasyView website using their own accounts.

	These reports will be stored in the patient's medical records at the Trust.			
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)	☐		
2.14.2	What physical security measures have been implemented to secure access? ie swipe cards, digilock			
	Physical access to the server rooms and remote access to the servers is restricted to those who require access to perform their duties.			
2.15	Will the data be stored on Trust servers			
	Yes	No		
		x		
2.16	Please state by which method the information will be transferred?			
	Email (not NHS.net)	☐	NHS.net	☐
	Web site Access (internet or intranet)	☒	Wireless Network (Wi-Fi)	☐

	Secure Courier	☐	Staff delivered by hand	☐
	Post (internal)	☐	Post (external)	☐
	Telephone	☐	SMS	☐
	Other	☒	please specify below	☒
	SSL (Security Socket Layer) and HTTPS (Hypertext Transfer Protocol over Secure Socket Layer) are used in the encrypted transmission of data. In order to ensure that data are accessed as expected, we have taken the following measures: 1. A firewall is used to filter malicious access. 2. Intrusion detection is used to detect system anomalies. 3. Malicious Code Protection is used to perform security checks on all committed data.			

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.**
	Yes	Medtrum - Full back up. 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.

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	Medtrum employees have received UK GDPR training. Trust employees will receive training on how to use the website. The following guide has been produced to support

		this training and there is also a guide for patients on how to use the App.  D-UG889000GB-003 Medtrum EasyView W  D-IM889001WW Eas yTouch App Quick Sta	
2.19	Will reports be produced?		
	Will reports contain personal/sensitive personal or business confidential information?		The reports won't contain personal/sensitive personal or business confidential information
	Who will be able to run reports?		Medtrum
	Who will receive the reports, and will they be published?		Trust contact.
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	The report is being filed in the patient's case notes and will follow the Trusts retention and destruction arrangements. The patient has the ability to delete all data in the App. The APP of the EasyView System stores data of 90 days. If the HCP choose to upload the data stored in the EasyView APP to the Medtrum server, the data will be stored in the server for 2 years.	
2.21	Is consent required for processing of personal data?		
	Y/N	Please describe if answered **Yes**	
	N		

		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 another legal basis?
		The Trust - Part of our statutory duties under GDPR 6(1)(e) public interest or public duty, and Article 9(2)(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services. Medtrum – EasyView App under GDPR Article 6(1)(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes; and Article 9(2)(a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes.
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.**
	Y	The information cannot be shared if the patient doesn't approve the request. http://www.medtrum.com/privacy-policy. The Trust's privacy notice is here https://www.sfh-tr.nhs.uk/for-patients-visitors/your-medical-record/
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	The patient can withdraw the consent at any time and delete the followers (the Trust).
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.**

	Y	The patient can choose to upload the data via App or remain the data on their own device by using Personal Diabetes Manager. Patients have the right to not upload device data to the Medtrum server, in which case we cannot access their data, and caregivers and healthcare professionals cannot access patients' data remotely. Without data upload, no one can see a patient's device data without checking the device itself. The EasyView APP of the EasyView System stores data of 90 days. Patients have the option to upload device data to the Medtrum server. One's data is protected by a username (email address or mobile number) and a strong password. Patients can see their own information anytime from a Medtrum website. No data will be shared without the patient's consent. Exceptions to the requirement for consent are limited to: • A legal reason to disclose information, e.g., by Acts of Parliament or court orders. • A public interest justification for breaching confidentiality such as a serious crime.
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.**
	Y	The patients will get a message that caregiver or HCP want to follow them. 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	Siobhan Favier and Lisa Gowan
	IAA	Elaine Higgins and Ursula Ngwu

	System Administrators	Elaine Higgins and Ursula Ngwu
2.27	How is the data secured in transit and at rest? Eg encryption, port control number	
	In order to maintain data integrity and security, we use SSL (Secure Socket Layer) server certificate to secure its diabetes management portal: to provide encryption for the data being transferred between the server, the patient and clinician. This helps to prevent eavesdropping attacks on the data and third-party accessing to the data.	
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.
	N	A patient safety case is not required as the insulin is not adjusted remotely. No security issues have been 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?	
	The purpose of data processor's processing is to give the Data Controller access to the EasyView system, which is an internet-based program with a web-based solution that allows the Data Controller to upload and/or browse patient data stored on the patient's Medtrum supported equipment, including specific health information and information regarding the patient's diabetes related activities and behaviours in the form of reports that can be used by the Data Controller for the management and treatment of the specific patient.	
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?	

	Patient representative will feedback the comments. Elaine Higgins 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).
	The Trust's lawful basis for processing personal and special categories of personal data are:

	1. Article 6(1)(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. 2. Article 9(2)(g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject 3. Article 9(2)(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services. Supplier 1. Article 6(1)(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.Article 9(2)(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services
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)
	A patient is informed why we are collecting their information, what we are going to do with it and who we may share it with through the Privacy Policy (https://www.medtrum.co.uk/privacy_policy.html) in our website and apps. This DPIA will be published once finalised. 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?
	All data will be stored in the App for 90 days, in the EasyView cloud for 2 years. Only data needed for our service is required. If the user deletes the data by mistake, the data can be retrieved from backup within 1 month. After one month, the data is deleted on both main server and backup storage.

2.35	How will you prevent function creep? Manage lifecycle of system/process
	The function creep will be prevented by the security measures in the cloud server/App and the security measures in medical devices (our products). 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: 15th February 2022

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)**	
Loss of system access and or data	Software and hardware protection system. Full system back-up process in place. Medtrum are ISO27001 compliant	2	2	4	System back-up not present	2	2	4	Manual input, business continuity plan to be used
Leavers' access not removed	Diabetes team will manage starters and leavers within the team	3	1	3	The starters and leavers process not followed	3	1	3	Account management SOP generated and implemented, routine audit to take place
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	2	2	4	Medtrum will need to be added to the divisional information asset register and the data flows mapped and recorded as part of the annual IAO returns to the SIRO	2	1	**2**	Medtrum will need to be added to the divisional information asset register and the data flows mapped and recorded as part of the annual IAO returns to the SIRO

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)**	
	patient reading out the information to us.								

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.