Healthier Communities, Outstanding Care

NHS
Sherwood Forest Hospitals
NHS Foundation Trust

Data Protection Impact Assessment

Title	Ref number
Sapien Health X Sherwood Forest Service Evaluation Trial	

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:	Sapien Health X Sherwood Forest Service Evaluation Trial

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

Pilot study in conjunction with the Sherwood Forest perioperative team whereby Sapien Health will be used to support 100 patients before and after their surgery with a view to improving their surgical outcomes. For the initial cohort of patients, an SMS sent by Sapien will direct users to a tailored URL which will contain information about the Sapien service. This has shown to be a successful method of onboarding at NHS South Tees Hospital.

Sapien is a mobile app-based behavioural intervention for patients undergoing elective surgery. The Sapien Health model combines personalised digital guidance with 1-to-1 remote health coaching to help optimise patients preoperatively, and support their recovery during the postoperative phase.

A service evaluation protocol has been provided which provides full details on the proposed project.

PDF
Sherwood Forest
SE Protocolv4.pdf

Overview of the proposal: What the project aims to achieve

This service evaluation aims to assess the effectiveness of the Sherwood Forest Hospitals perioperative care pathway, where Sapien is used to support patients in addressing modifiable risk factors for surgery through lifestyle modification and improved self-management. The evaluation will also assess the impact of the intervention with respect to clinical and operational outcomes, and patient experience.

The primary outcome metric used to evaluate the success of the programme will be the Patient Activation Measure (PAM). Patient Activation Measure is a validated and licensed tool that measures people's knowledge, skills and confidence in managing their own wellbeing. Evidence shows that when people are supported to become more activated, they benefit from better health outcomes, improved experiences of care and fewer unplanned care admissions.

PDF
Sherwood Forest - Sapien Program.pdf

PDF
Sherwood Forest SE Protocolv4.pdf

PDF
Sherwood Forest - Sapien Postcard - A6.

Implementing Organisation:	Sapien Health Limited

Staff involved in DPIA assessment (Include Email Address):	Luke Eastwood (luke@sapienhealth.io) Rebecca Barker (rebecca.barker6@nhs.net) Robbie Huddleston (robbie@sapienhealth.io)

Project Sign Off

	Name	Job Title	Organisation	Date
Information Asset Owner	Steve Jenkins	Divisional General Manager	Sherwood Forest Hospitals NHS Foundation Trust	**27th August 2021**
Data Protection Officer	Jacquie Widdowson	Information Governance Manager	Sherwood Forest Hospitals NHS Foundation Trust	**16th August 2021**
Information Governance	Gina Robinson	Information Security Officer	Sherwood Forest Hospitals NHS Foundation Trust	**28th July 2021**
Senior Information Risk Owner	Paul Robinson	Chief Financial Officer	Sherwood Forest Hospitals NHS Foundation Trust	**23rd August 2021**
Caldicott Guardian	David Selwyn	Medical Director	Sherwood Forest Hospitals NHS Foundation Trust	**23rd August 2021**

Chief Clinical Information Officer	David Selwyn	Medical Director	Sherwood Forest Hospitals NHS Foundation Trust	**23rd 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: Data flows and information Asset Register to be documented in the Division **Summary of Risks**: UK GDPR compliance and Information Asset Management

Recommendations for Action

Summary of Identified Recommendations:		
Recommendations:	**Recommendation Owner:**	**Agreed Deadline for action:**
Ensure annual compliance with assurance from the Supplier that they are completing the Data Security and Protection Toolkit and the data processors remain ISO 27001 compliant	Information Asset Owner	Annually
Data flow maps for the use of Sapien to be documented	Information Asset Owner	31st August 2021
Sapien to be added to the Information Asset Register for the Division	Information Asset Owner	31st August 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	During the perioperative health coaching programme information will be shared with the individuals health coach as they are optimised before and after surgery
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?	Y	Limited personal details (name, contact details such as phone number and email if available) will be securely transferred from the care team at Sherwood to Sapien Health who will invite the patient to download the Sapien Health app using text message / email with a link to a landing page where they will be provided information on the processing and next steps if they wish to participate.
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	Yes – patients do not currently receive a health coach and digital programme in the lead up to surgery. It is hoped providing this will lead to increased PAM scores and positive behaviour change which will ultimately impact upon readmission, complication and LoS as detailed more fully in the service evaluation protocol.
5	Are there processes in place to ensure data is relevant, accurate and up-to-date?	Y	
6	Are there security arrangements in place while the information is held?	Y	From a Cyber perspective Sapien are low risk. Storage and Web is ISO 27001 compliant

Q	Screening question	Y/N	Justification for response
			Amazon Web Services (AWS) in a manner that is ISO 27001 (International Standard for Information Security Management) compliant. Data is encrypted All data is encrypted regardless of its classification and access control can be defined to the field level if required. Also using the correct levels of authentication and encryption and also using 2 Multi Factor Authentication. Communications are encrypted and authenticated using TLS1.2 (protocol), ECDHE_RSA with P-256 (key exchange), and AES-128-GCM (cipher) using 2048-bit keys.
7	Does the project involve using new technology to the organisation?	Y	Mobile App provided by the supplier
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	After liaising with the supplier directly we do not feel that this falls under the DCB0129 directive for clinical information systems as the data provided is to support the patient rather than to make clinical judgements and does not feed into the patient record. However the Sapein app has been designed and built in accordance with NHS Digital Clinical Safety standards (DCB 0129 and DCB 0160).

Q	Screening question	Y/N	Justification for response
10	Is a Quality Impact/Technical Security Review required?	Y	From a Cyber perspective Sapien are low risk. Storage and Web is ISO 27001 compliant Amazon Web Services (AWS) in a manner that is ISO 27001 (International Standard for Information Security Management) compliant. Data is encrypted All data is encrypted regardless of its classification and access control can be defined to the field level if required. Also using the correct levels of authentication and encryption and also using 2 Multi Factor Authentication. Communications are encrypted and authenticated using TLS1.2 (protocol), ECDHE_RSA with P-256 (key exchange), and AES-128-GCM (cipher) using 2048-bit keys.

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.		Pilot study in conjunction with the Sherwood Forest perioperative team whereby Sapien Health will be used to support 100 patients before and after their surgery with a view to improving their surgical outcomes. Sapien is a mobile app-based behavioural intervention for patients undergoing elective surgery. The Sapien Health model combines personalised digital guidance with 1-to-1 remote health coaching to help optimise patients preoperatively, and support their recovery during the postoperative phase. A service evaluation protocol has been provided which provides full details on the proposed project. Sherwood Forest SE Protocolv4.pdf			

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					□

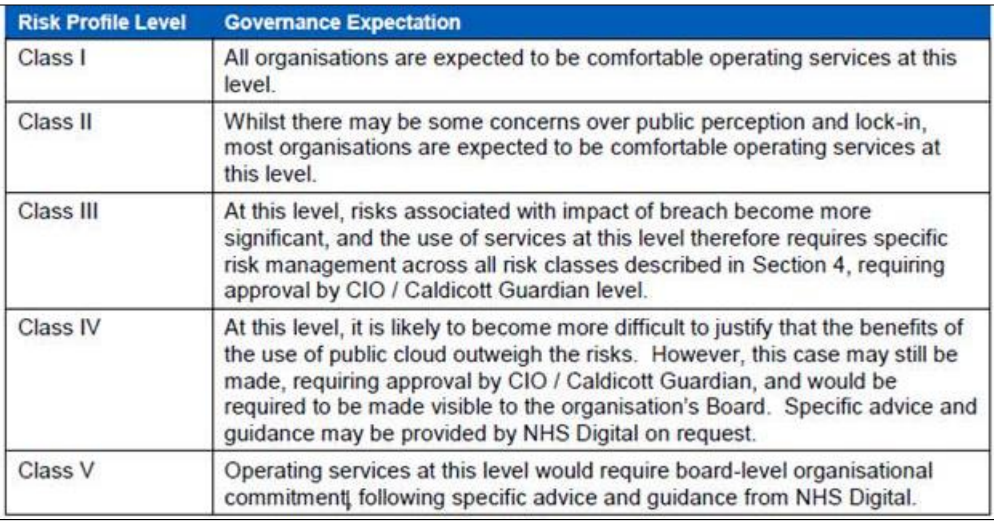
	Religious Belief	□
	Trade Union Membership	□
	Physical or mental health or condition	☒
	Sexual Health	□
	Criminal offence data	□
	Other data (please specify)	

2.2.2	Is the data?					
	Identifiable?	☒	Pseudonymised?	☒	Anonymised?	□
	Limited personal details (name, contact details such as phone number and email if available) will be securely transferred from the care team at Sherwood to Sapien Health who will invite the patient to download the Sapien Health app using text message / email with a link to a landing page where they will be provided information on the processing and next steps if they wish to participate. Appropriate patients who are suitable for the service download the Sapien app where they can input quantitative and qualitative data about their lifestyle and medical history. Health data is then shared with the Sapien Health coach who can interact with the patient to drive positive behaviour change and better optimisation. Outside of Sapien, confidential patient information is accessible only to patients, and to the clinicians/care team. There is no sharing of confidential patient information with third parties outside of infrastructure and software providers. Data is pseudonymised internally at Sapien and Sapien only retains confidential patient information while the project is active, all confidential patient information is deleted or anonymised so that it is impossible to re identify an individual when the patient is off boarded.					

2.3	Is the data required to perform the specified task?	
	Y/N	Please justify response **Yes or No**
	Y	Processing will involve collection and transmission of personal data & health data from the patient to their health coach at Sapien who will engage patients in their care and provide a personalised service in an effort to better optimise the patient for surgery (thereby achieving better surgical outcomes). Reports of activity and results will be emailed to the care team at Sherwood Forest Trust and the results will be filed in the patient's case notes by the anaesthetic patient pathway coordinators.

2.3.1	How will you collect, use, store and delete data?
	Personal data collected includes: - forename - surname - date of birth - age - biological sex - mobile telephone number - email address **Health data** The primary outcome metric used to evaluate the success of the programme will be the Patient Activation Measure (PAM). Patient Activation Measure is a validated and licensed tool that measures people's knowledge, skills and confidence in managing their own wellbeing. Evidence shows that when people are supported to become more activated, they benefit from better health outcomes, improved experiences of care and fewer unplanned care admissions. The following secondary outcome metrics will be collected at baseline and on completion of the programme: •Average length of stay •30 day readmission rate •Day of surgery cancellations •Quality of life (measured by EQ5D) •Knee or hip function/pain where applicable (measured by Oxford Knee/Hip Score) Additionally, patient experience will be measured upon completion of the programme using a numerical rating scale. Sapien only retains confidential patient information while the project is active, all confidential patient information is deleted or anonymised so that it is impossible to re identify an individual once the project ends.
2.3.2	What is the source of the data? (i.e. from data subject, system or other third party)
	Limited contact details will be provided by the care team at Sherwood forest to help Sapien on-board patients. These will be securely transferred from the care team at Sherwood to Sapien Health using NHSmail. The care team at Sherwood will write to the patient and invite them to use the service. Sapien Health will then invite the consenting patients to download the Sapien Health app using text message. Appropriate patients who are suitable for the service download the Sapien app where they can input quantitative and qualitative data relative to their treatment. Health data is then shared with the Sapien Health

	coach who can interact with the patient to drive positive behaviour change and better optimisation.
2.3.3	How much data will you be collecting and using?
	The data described above from 100 patients.
2.3.4	How often? (for example monthly, weekly)
	Patients will be asked to engage with the Sapien App regularly (perhaps daily) for the pre and post-operative period (3 months).
2.3.5	How long will you keep it?
	Identifiable data will only be retained whilst the patient is in their perioperative program. Upon completion of the perioperative program all identifiable data held by Sapien will be deleted or permanently anonymised so that no individual can be identified. Confidential patient information Sapien holds as a result of the project will be deleted or permanently anonymised so that no individual can be identified within 24 months of project completion. Sapien also welcomes using the Trusts’ standard data sharing agreement or contracts if preferable.
2.3.6	Where will the data be stored? i.e. Medway, Shared Drive, offsite storage
	Sapien stores the confidential patient information on cloud-based servers, located in the UK (AWS London, eu-west-2), for the duration of the deployment. (AWS in a manner that is ISO27001 compliant). As Sapien is a fully distributed company in terms of working location, a VPN is used to secure our internal systems. AWS’s Client VPN service is used to protect pre-production environments from the public Internet. health_and_social_care_data_risk_model_L Sapien have completed the Health and Social Care Data Risk Model for the usage of Cloud based servers and has scored as Class II.



Risk Profile Level	Governance Expectation
Class I	All organisations are expected to be comfortable operating services at this level.
Class II	Whilst there may be some concerns over public perception and lock-in, most organisations are expected to be comfortable operating services at this level.
Class III	At this level, risks associated with impact of breach become more significant, and the use of services at this level therefore requires specific risk management across all risk classes described in Section 4, requiring approval by CIO / Caldicott Guardian level.
Class IV	At this level, it is likely to become more difficult to justify that the benefits of the use of public cloud outweigh the risks. However, this case may still be made, requiring approval by CIO / Caldicott Guardian, and would be required to be made visible to the organisation's Board. Specific advice and guidance may be provided by NHS Digital on request.
Class V	Operating services at this level would require board-level organisational commitment, following specific advice and guidance from NHS Digital.

2.3.7	How many individuals are affected?
	100 individuals
2.3.8	What geographical area does it cover?
	The solution will be offered to patients currently on waiting lists to undergo knee or hip joint replacement surgery and elective, non-cancer, major gynaecological surgery.

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	Joint Data Controller/Processor
	Sapien Health Limited	Joint Data Controller/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**

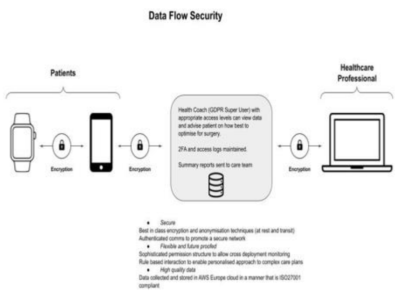
		to the completion of this proforma. An example of a completed assessment is also provided below NHIS - Supplier Assurance Framework Supplier Assurance Framework - Example
		Supplier Assessment has been provided and there are no concerns from NHIS
2.5.1		Please describe access and controls in place Account access management Standard Operating Procedure to be completed prior to the implementation of the project
		Sapien Health is ISO27001 Certified (March 2021) ISO27001 Certificate (2).pdf NHS Data Security Protection Toolkit (Standards Met) GCloud 12 Digital Marketplace (Approved Supplier) ICO Registration (Reg number : ZA779931) Cyber Essentials (IASME-CE-007281) Sapien Health CE.pdf Internally at Sapien Health a full DPIA has been conducted and an entry made on the Register of Processing Activities. **Security features** Data collected on the Sapien platform is hosted by Amazon Web Services (AWS) in a manner that is ISO 27001 (International Standard for Information Security Management) compliant. Communications are encrypted and authenticated using TLS1.2 (protocol), ECDHE_RSA with P-256 (key exchange), and AES-128-GCM (cipher) using 2048 bit keys. All data is encrypted regardless of its classification and access control can be defined to the field level if required. De Identification Used Internally; pseudonymisation practices are applied by allocating a random code to the patient's

	records. Only certain team members have access to confidential patient information for distinct purposes. Other features utilised to prevent a breach include: - Database and network protection from Cyber Attack - Backup and recovery procedures in place to protect the data -Security in place to physically protect the data -Access controls and Authentication methods - Sapien passed stage 2 audit for ISO27001 Certification on 19th March 2021.		
2.5.2	Please provide a copy of the contract in place		
	A signed partnership Agreement governing the pilot phase has been provided; a template data sharing agreement (unsigned) has been provided and can be used to support the partnership agreement Data protection requirements. 300720_Sherwood_Partneship__Signed_Cc Please_sign_-_DSA.pdf		
2.5.3	Have arrangements for retention and destruction been included in the contract when the service/contract expires?		
	DSA_20.04.21.pdf Confidential patient information Sapien holds as a result of the project will be deleted or permanently anonymised so that no individual can be identified within 24 months of project completion.		
2.5.4	Is the supplier registered with the ICO? Please check the register	**Yes**	**No**
		Yes ZA779931	
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 check the register and provide the following details	Completed: Yes/No	Date submitted	Standard Met/Not Met
		Yes 8KN81	25/10/2020	Standards Met, Category 3

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		CE IASME-CE-007281 Sapien Health CE.pdf
	ISO 15489 Records Management		No however relevant controls related to annex A of iso27001 have been applied to records management
	ISO 27001 Information Security Standards	Yes ISO27001 Certificate (2).pdf	
	ISO 9001 Quality Management Systems		No – considerable overlap w ISO27001 however.

2.5.10	Is the data held outside of the UK ie Europe, USA, Ireland? If yes please include the country	
	Yes	No
		No – all data kept in UK
	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	
	Not applicable	
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?
	N	No contractors are utilised
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	
	N, recorded as a risk.	 Data Flow Security Patients Healthcare Professional Encryption Encryption Encryption Health Coach (GDPR Super User) with appropriate access levels can view data and advise patient on how best to optimise for surgery. 2FA and access logs maintained. Summary reports sent to care team • *Secure* Best in class encryption and anonymisation techniques (at rest and transit) Authenticated comms to promote a secure network • *Flexible and future proofed* Sophisticated permission structure to allow cross deployment monitoring Rule based interaction to enable personalised approach to complex care plans • *High quality data* Data collected and stored in AWS Europe cloud in a manner that is ISO27001 compliant
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	Events are logged using CloudWatch. It collects monitoring and operational data in the form of logs, metrics, and events, providing a unified view of AWS resources, applications and services. CloudWatch is used to set high resolution alarms, visualize logs and metrics side by side, take automated actions, troubleshoot issues, and discover insights to optimize applications, and ensure they are running smoothly.https://aws.amazon.com/cloudwatch/ The logging facilities and information are protected from tampering and unauthorized access. System administrators (in addition to operators or normal users) are prohibited from disabling logging activity; disabling audit logs or tampering with audit log information is treated as a serious offence in the disciplinary policy and may result in immediate dismissal.

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?
	Data will be checked for accuracy by the designated Sapien Health coach, who is a trained clinical safety officer, caldicott guardian and GDPR super user (having received relevant training for all these roles). Only the minimal possible data will be collected to achieve the project goals.
2.13	Who will have access to the information? (list individuals or staff groups)
	Designated health coach will have access to the information. Only a very limited number of trained GDPR super-users can gain access and this is a necessity for continuation of services and the requirements of GDPR (e.g. the right-to-be-forgotten)

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)	☒
	Organisational Security Sapien is ISO 27001 certified. Every employee of Sapien Health receives Information Security training when they join and must pass a test demonstrating understanding of IS. This is repeated annually. System administrators are responsible for managing access to systems, the processes for which are documented and implemented as part of Sapien Health's Information Security Management System. **Infrastructure description** Sapien Health employs a server less infrastructure hosted on AWS who manage all physical servers, resources and networking hardware to enable all business logic and higher level services. The robust security services provided by AWS can be augmented by multiple, additional layers of security and other services. It also facilitates automatic, seamless and extensive backups, allowing for quick and simple recovery in case of data loss or other errors, and also enables Disaster Recovery solutions.	

	System access and the associated security are tightly controlled by taking full advantage of the AWS Identity and Access Management solution (https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies.html). Multi Factor Authentication is used by all users with access to the infrastructure. Only trained GDPR super-users have access to health data that is not anonymised. This is typically only for the purpose of responding to subject access requests. **Technical Security** Data collected on the Sapien Health platform is hosted by Amazon Web Services (AWS) in a manner that is ISO 27001 (International Standard for Information Security Management) compliant. Communications are encrypted and authenticated using TLS1.2 (protocol), ECDHE_RSA with P-256 (key exchange), and AES-128-GCM (cipher) using 2048 bit keys. Public Sapien Health sites, such as those potentially accessed from hospital systems that may be running old versions of Windows that do not support TLS 1.2, accept TLS 1 and TLS 1.1. All data is encrypted regardless of its classification and access control can be defined to the field level if required. DynamoDB encryption at rest provides enhanced security by encrypting all data at rest using encryption keys stored in AWS Key Management Service (AWS KMS). This functionality helps reduce the operational burden and complexity involved in protecting sensitive data.	
2.14.2	What physical security measures have been implemented to secure access? ie swipe cards, digilock	
	System access is controlled remotely and the cloud is utilised to ensure complete security of information assets and prevention of unauthorised access. AWS Identity and Access Management solution has been implemented with Multi Factor Authentication used by all users with access to the infrastructure. Only trained GDPR super-users have access to health data that is not anonymised. This is typically only for the purpose of responding to subject access requests. Sapien Health passed stage 2 audit for ISO27001 in March 2021, is cyber essentials plus certified and has met the standards for the NHS Digital Data Security and Protection Toolkit.	
2.15	Will the data be stored on Trust servers	
	Yes	No
		No – however reports from Sapien Health may be stored on Trust servers
2.16	Please state by which method the information will be transferred?	

	Email (not NHS.net) robert.huddleston@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	☐
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	Yes ; Sapien has implemented - Capacity management policy and corresponding plan - Business continuity management policy - Change management policy - Back up policy (Full Backups) All controls relating to these requirements in Annex A of ISO27001 have been implemented and Sapien was externally certified as having these controls in place in March 2021. In the event that the data is unavailable to the Trust, a copy of the information will be provided as soon as possible		

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	All staff must pass an external test on IS to gain access to any Sapien health information systems. This test is repeated annually. All staff receive training on key IS policies and procedures.
2.19	Will reports be produced?	
	Will reports contain personal/sensitive personal or business confidential information?	Yes – reports on the study will be provided to the care team at Sherwood.
	Who will be able to run reports?	Sapien Health will provide regular reports on usage and outcomes to Sherwood and will be forwarded to Dr Barker via NHSmail
	Who will receive the reports and will they be published?	Dr Rebecca Barker, and anonymised publication to be confirmed
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	On Sapien side all confidential patient information can be deleted upon project completion. The reports sent to Sherwood can be retained / deleted as the trust sees appropriate.

2.21	Is consent required for processing of personal data?	
	Y/N	Please describe if answered **Yes**
	Y	Yes (For Sapien) the trust may rely on a different legal basis for their processing
		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	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). 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.
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.**
	Yes	Sapien Health has been added to the Trust’s patient privacy policy. Patients will be informed of the service by the Trust. The Sapien Health App includes a privacy notice to inform patients of their rights.
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	Process in place for individuals to exercise all individual rights.
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 will be informed what data is being collected, why and how it will be processed. The language is simple and clear, thereby encouraging the patient to read the entire consent form. Patients review how their data will be used, and consent to sharing their data with their Sapien coach and healthcare professional, for the purpose of enhancing adherence to therapies as agreed with the clinician. Patients can access and/or rectify relevant data that has been entered into the app at any time. They are informed of their right to withdraw and their right to have their personal information deleted. Patients are informed that Sapien can be contacted by sending an email to privacy@sapienhealth.io, in order to exercise these rights or lodge a complaint.
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 Trust has an established process for responding to subject access requests Sherwood Forest Hospitals (sfh-tr.nhs.uk)
2.26	Who are the Information Asset Owner(s) and Administrator(s)?	
	IAO	Steven Jenkins
	IAA	Dr Rebecca Barker
	System Administrators	Dr Rebecca Barker
2.27	How is the data secured in transit and at rest? Eg encryption, port control number	
	Data collected on the Sapien platform is hosted by Amazon Web Services (AWS) in a manner that is ISO 27001 (International Standard for Information Security Management) compliant. Communications are	

	encrypted and authenticated using TLS1.2 (protocol), ECDHE_RSA with P-256 (key exchange), and AES-128-GCM (cipher) using 2048 bit keys. All data is encrypted regardless of its classification and access controls can be defined to the field level if required.	
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	Full DPIA and Register of processing entry completed by Sapien Health, supplier assurance framework completed and submitted to the Trust.
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?	
	This service evaluation aims to assess the effectiveness of the Sherwood Forest Hospitals perioperative care pathway, where Sapien is used to support patients in addressing modifiable risk factors for surgery through lifestyle modification and improved self-management. The evaluation will also assess the impact of the intervention with respect to clinical and operational outcomes, and patient experience. The primary outcome metric used to evaluate the success of the programme will be the Patient Activation Measure (PAM). Patient Activation Measure is a validated and licensed tool that measures people’s knowledge, skills and confidence in managing their own wellbeing. Evidence shows that when people are supported to become more activated, they benefit from better health outcomes, improved experiences of care and fewer unplanned care admissions. A full protocol has been written and agreed which details the aims and objectives of both parties in more detail.	
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?
	Sapien is happy and encourages liaising with individual hospitals regulatory teams. Projects that are different to those previously completed go through Management Review board and ensure the views of relevant clinical, legal and regulatory team members are gathered. Views of legal and information security professionals have been obtained to ensure the proposed processing complies with the 6 principles of UK GDPR and other applicable privacy legislation.

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).
	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). 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.
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)
	Landing page following email / text with information on processing Privacy Notice In app information This DPIA will be published once finalised.
2.34	What measures do you take to ensure processors comply?
	All suppliers subject to strict supplier assessments conducted in line with ISO27002 controls. Appropriate contracts are put in place with software providers. Sapien is not aware of any sub processors involved in this project, for which it is responsible for ensuring compliance. The Trust and Sapien have a contract in place and this will be reviewed on a regular basis.
2.35	How will you prevent function creep? Manage lifecycle of system/process
	Function creep is prevented as Sapien projects are time limited to surgical periods. The App will only perform in accordance with its specifications during this period. Any further use of the Sapien app after project expiry requires a new agreement. Sapien will only ever process the Trust’s data as per explicit agreement with the Trust. The Trust and Sapien have a contract and data sharing agreement in place where roles and responsibilities are defined.

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: 28th 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)**	
Software failure due to a Cyber-attack and/or power loss. Availability of patient information would be impacted	Sapien is ISO27001 certified, meets the standards for the NHS DSPT and has cyber essentials, we are a GCloud 12 approved supplier. **Security features** Data collected on the Sapien platform is hosted by Amazon Web Services (AWS) in a manner that is ISO 27001 (International Standard for Information Security Management) compliant. Communications are encrypted and authenticated using TLS1.2 (protocol), ECDHE_RSA with P-256 (key exchange), and AES-128-GCM (cipher) using 2048 bit keys. All data is encrypted regardless of its classification and access control can be defined to the field level if required. **De Identification Used Internally**	2	1	2	Data flows for the use of Sapien will need to be documented and the Information Asset Register for the division updated	2	1	**2**	Data flows for the use of Sapien will need to be documented and the Information Asset Register for the division updated

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)**	
	Internally, pseudonymisation practices are applied by allocating a random code to the patient's records. Only certain team members have access to confidential patient information for distinct purposes. Other features utilised to prevent a breach include: - Database and network protection from Cyber Attack • Backup and recovery procedures in place to protect the data • Security in place to physically protect the data • Access controls and Authentication methods Supplier (Processor) Management All suppliers subject to strict supplier assessments conducted in line with ISO27002 controls. Sapien received ISO27001 Certification on 19th March 2021. Annual programme of work with the Information Asset Owners to document and review data flow maps and populate the Information Asset Register. Business continuity plans in place at Sapien and the Trust			🟩				🟩	

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.