

Data Protection Impact Assessment

Contents

Introduction	2
When and who should complete a DPIA?	2
Who do I send the completed DPIA to for review?	2
What if I need help?	2
Step 1 – What is the aim of the project being undertaken	3
Step 2: What type of data is being processed?	6
Step 3 – Data security	11
Step 4 – Data use and sharing	16
Step 5 – Processing by or with a supplier/third party	18
Step 6 – Consultation	19
Step 7 – Lawful basis	20
Stage 8 – Risk Template	22
Step 8 – Legal compliance	26
Step 9 - Assessment Summary	30
Step 10 - Recommendations for Action	32
Step 11 - Project signoff	33

Introduction

Data protection by design is about considering data protection and privacy issues upfront in everything you do. It can help you ensure that you comply with the UK General Data Protection Regulation's fundamental principles and requirements, and forms part of the focus on accountability.

A Data Protection Impact Assessment (DPIA) is a tool that we use to identify and reduce the data protection risks of our processing activities. They can also help us to design more efficient and effective processes for handling personal data.

The UK General Data Protection Regulation requires the Trust to put in place appropriate technical and organisational measures to implement the data protection principles effectively and safeguard individual rights. This is 'data protection by design and by default.'

In essence, this means we have to integrate or 'bake in' data protection into our processing activities and business practices, from the design stage right through the lifecycle. This concept is not new and **is now a legal requirement**.

When and who should complete a DPIA?

- 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. **No commitments to, or installation of systems, should take place before the DPIA has been signed off.**
- Information Assets Owners (IAO) and Information Assets Administrators (IAA) **must** complete the DPIA.
- Relevant stakeholders (internal and external suppliers) should be consulted throughout the DPIA process.

Who do I send the completed DPIA to for review?

- Information Governance Team sfh-tr.information.governance@nhs.net.

What if I need help?

- Please contact the Information Governance Team sfh-tr.information.governance@nhs.net or [SFHT Phonebook \(nnotts.nhs.uk\)](http://SFHT.Phonebook(nnotts.nhs.uk))

IMPORTANT – PLEASE COMPLETE ALL QUESTIONS. IF YOU THINK A QUESTION DOES NOT APPLY INSERT N/A AND EXPLAIN WHY.

Project title:	SnapComms
Reference number:	
Implementing organisation:	Sherwood Forest Hospitals NHS Foundation Trust
Key contacts involved in the DPIA (name and job title)	Richard Brown, Head of Communications Nicola McCormack, Project
Information Asset Owner (name and job title)	Richard Brown, Head of Communications
Information Asset Administrator (name and job title)	Communication Team

Step 1 – What is the aim of the project being undertaken

Q1	Project description: Describe in sufficient detail for the project to be understood	<p>SnapComms is a multi-channel communication tool to reach and engage with employees on Trust devices including desktop and mobile.</p> <p>SnapComms will support rapid communication with 100% visibility to targeted groups of employees in the event of serious incidents, or other time critical events.</p>
-----------	--	---

Q2	Why are we doing it? Summarise why there is a need for implementation or change and the benefits it will realise.	<p>Currently the Trust communicates with employees via email, intranet, and screen savers. None of these methods guarantee the recipient reads, takes notice or acts. They are also not immediate. The Trust needs to communicate relevant time critical information to key groups of employees. These channels also do not allow for an audit trail to evidence that messages have been received and read by recipients.</p> <p>Examples of how these pop-ups might be used include:</p> <ul style="list-style-type: none"> • Emergency pressures, and changes to
-----------	---	---

		<p>protocols as a result</p> <ul style="list-style-type: none"> • Escalation of current operation levels • Serious incidents <p>These communications are time critical, and relevant to key employees regardless of their location (on or off site), and their access to email or a Trust device. The ability to push communications direct to a Trust device ie desktop agent, mobile app, or via text will ensure that messages can be cascaded immediately, and appropriate action taken.</p>
--	--	--

Q3	<p>What is the nature of your relationship with the data subject (patient, employees) whose data will be used?</p> <p>For example, do you provide direct care to the data subjects, are they your patients?</p>	Employing organisation
-----------	--	------------------------

Q4	Individuals need to be told how their information is processed.	
	Have you consulted the data subject or their representative about using this data? If not, please explain why you have not consulted them?	No, this is not required
	Please provide details and an example of how this consent (if appropriate to rely on consent as a legal basis) to processing of their data was given? (Preferably embed document)	Not applicable
	What information will you give individuals informing them of what you are doing with their data? i.e. this is consent to the processing of their personal data, not consent to treatment	Communication team will issue notices in the weekly staff bulletin to inform all employees of the new system and how the messages will be used.
	Is this information covered by our existing fair processing information or	Not applicable


	<p>leaflet? If Yes, provide details. If No, please provide text to be added to our fair processing information.</p> <p><u>Patient</u>¹ <u>Staff</u>²</p>	
	<p>Explain why you believe they would consider the proposed new use of their data as being reasonable or expected?</p>	<p>If SnapComms was unavailable we would revert to business-as-usual processes ie. all user emails, staff bulletin and social media platforms.</p>

<p>Q5</p>	<p>Has an assessment been made that the information collected is the minimum required to meet the aim of the project?</p>	
	<p>Use of data should not be the first resort if the objective can be achieved without its use. You must justify why the use of all the data is necessary and proportionate. For example, do you need to use all the fields, can you not achieve the same objective with fewer data fields and/or a smaller data set?</p>	<p>Yes, User name Domain Name Full Name Job Title Base (SFH-KMH or NHIS) Last Device accessed name Last connected date Active groups Disabled groups Active Directory Groups Email Address</p> <p>The data that is captured is all present within the Trusts Active directory. This information is synchronised across to ensure that the correct and up to date data information is used.</p> <p>Without this sync the approach to identify who will receive the communication would be time consuming and add additional tasks to the onboarding and off-boarding process within the Trust.</p>
	<p>Has consideration been given to how the same objective or outcome may be achieved without using this data, using less data, or employing a different method - explain in full?</p>	<p>SnapComms is one communication tool that forms part of a tool kit. The pop-ups will introduce a new and instant source of information that an e-mail would not provide, unless the individual was accessing their e-mails at that exact time.</p>

¹ <https://www.sfh-tr.nhs.uk/for-patients-visitors/your-medical-record/>

² <https://www.sfh-tr.nhs.uk/work-for-us/your-employees-information/>

Step 2: What type of data is being processed?

Q6	Fully describe ALL the data that will be used and justify why it is needed.	
	Data item i.e. MRI images, patient, name, address, IP address, NHS/D number	Why is it necessary?
	User name Domain Name Full Name Job Title Base (SFH-KMH or NHIS) Last Device accessed name Last connected date Active groups Disabled groups Active Directory Groups Email address	The data is captured to be able to identify and target the correct active individual, based on Active directory groups. This is the basis of how the communication can be sent to a specific individual or group of users. <div style="text-align: center;">  RoE draft v3 (1).docx </div>

Q7	Will you use special categories of personal data?	
	political opinions	<input type="checkbox"/>
	racial or ethnic origin	<input type="checkbox"/>
	religious or philosophical beliefs	<input type="checkbox"/>
	trade-union membership	<input type="checkbox"/>
	genetic data	<input type="checkbox"/>
	biometric data for the purpose of uniquely identifying a natural person	<input type="checkbox"/>
	data concerning health	<input type="checkbox"/>
	data concerning a natural person's sex life or sexual orientation	<input type="checkbox"/>



Q8	Approximately how many individuals will be in the dataset?	
	<11 individuals	<input type="checkbox"/>
	11 – 50 individuals	<input type="checkbox"/>
	51 – 100 individuals	<input type="checkbox"/>
	101 – 300 individuals	<input type="checkbox"/>
	301 – 500 individuals	<input type="checkbox"/>
	501 - 1,000 individuals	<input type="checkbox"/>
	1,001 - 5,000 individuals	<input type="checkbox"/>
	5,001 - 10,000 individuals	x
	10,001 - 100,000 individuals	<input type="checkbox"/>
	100,001 or more individuals	<input type="checkbox"/>

Q9	How large and expansive are the records sets being used, what will it consist of?
	The data is held externally and due to the type of file we are unable to quantify the size.

Q10	What geographical area will the data be drawn from or cover? For example, Mansfield, Ashfield, Newark and Sherwood patients. Derbyshire patients ?
	All employees. Patient data is not being processed.

Q11	What is the source of this data?	
	If the data is being taken from an existing system, identify what system that is and for what was the originally purpose that data was collected? How will this data be accessed?	The data items are being taken from Active Directory (AD). Microsoft Active Directory is a directory service, which can create groups to simplify the administration of user accounts or computers in different Active Directory domains by collating them and assigning ubiquitous access rights. Once part of an Active Directory group, a user can easily access all the resources and directory services common to the group without making multiple requests.
	If it is new data/system that is being collected, describe how this data collection will be done i.e. digital, paper, removeable media?	The data is captured when the SnapComms Client is installed onto the device and logged into by the individual. This will be updated when a new device is issued, and a new client is installed.

Q12	How will this data be used?	
	Will this data be used or combined with other data sets, if so what are these other data sets?	No
	What will this data show you that is relevant to the project aim and purpose?	Not applicable
	Describe the access controls in place. Will the supplier also have access to	SnapComms will be managed by the communications team and may be rolled

	the data?	out to other appropriate teams in the Trust. SnapComms will have access to the data in the portal.
	<p>Complete the Account Management and Access Standard Operating Procedure³</p>  <p>Account Management & Acce</p>	 <p>Account Management.docx</p>

Q13	Describe proportionality measures		
	Explain how the processing achieves your purpose?	Active Directory represents the most efficient and effective use of configuring this system to the Trust's requirements.	
	Is there another way to achieve the same outcome, give details of alternatives you have rejected and provide the reasons why?	No, current ways of working (email, social media) are not sufficient.	
	Please explain why a smaller amount of data cannot be used.	Not applicable	
	Does the <u>National Data Opt-Out apply</u> (allows patients to opt out of their confidential patient information being used for research and planning)?	Yes	No
<input type="checkbox"/>		<input checked="" type="checkbox"/>	

Q14	What is the duration of this processing? Is this one-off processing or will it continue for a specified period?
	1 year, option to renew

Q15	How long will the data be kept and how will it be deleted?	
	NHS data needs to be retained in	1 year. Upon termination of the contract

³ <https://www.sfh-tr.nhs.uk/about-us/policies-and-procedures/non-clinical-policies-procedures/information-governance/?id=13618>

	<p>accordance with the Records Management Code of Practice⁴. You can check the schedule here⁵.</p> <p>Has provision been made to ensure you are able to accommodate this?</p> <p>If No, describe how the data will be managed.</p>	<p>the Trust will instruct SnapComms to destroy all confidential information.</p>
	<p>If a third party is processing data, how will we ensure data is deleted when required? Appropriate evidence would be an embedded copy of the contract or agreement containing this detail</p>	<p>Contract in place between SnapComms and the Trust</p>
	<p>What will happen to the data at the end of the project/activity or end of contract with a third party? Will it be returned or deleted and how will this be done? Most contracts specify what happens to data at the end of contract. If this is not subject to contract, how will you ensure the data held by any third party is deleted? Embed extract of contract as necessary with highlighted sections.</p>	<p>SnapComms will be disconnected from Trust systems, with no personal data being transferred to external supplier at any point.</p> <p>NHIS to support with project management of the decommissioning of this project, if and when decision is taken to decommission.</p>

Q16	Have the personal/special categories of data been minimised?	
	<p>Please explain why a smaller amount of data cannot be used and explain why all the data fields are necessary to achieve the objective. You are required to minimise the amount and level detail of any data set. For example, dates of birth should not be used where age would provide sufficient information to achieve the project aim.</p>	<p>The data is captured to be able to identify and target the correct active individual, based on Active directory groups. This is the basis of how the communication can be sent to a specific individual or group of users.</p> <p>Without this sync the approach to identify who will receive the communication would be time consuming and add additional tasks to the onboarding and off-boarding process within the Trust.</p>





⁴ <https://www.sfh-tr.nhs.uk/about-us/policies-and-procedures/non-clinical-policies-procedures/information-governance/?id=8647>



⁵ <https://transform.england.nhs.uk/information-governance/guidance/records-management-code/records-management-code-of-practice-2021/#appendix-ii-retention-schedule>

	How will you prevent function creep?	SnapComms and the Trust have a contract in place. Data processing responsibilities have been included in the contract.
	How will you ensure high standards of data quality?	The SnapComms App will refresh the Active Directory information from Windows every 6 hours by default. The refresh will occur whenever the age of the cached directory information is at least 6 hours old. The refresh duration can be customized inside the Content Manager. Refresh will also occur the first time a particular user logs onto a desktop.

Q17	Is the data anonymised or pseudonymised in any way?	Anonymised	Pseudonymised
		<input type="checkbox"/>	<input type="checkbox"/>
	If the data is pseudonymised please describe how this has been done and 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.	Not applicable	
	If the data is pseudonymised describe how the data will be transferred ie using HL7. ie 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.	Not applicable	
	Have you considered whether using anonymised/pseudonymised data is a suitable alternative, please explain how this has been considered and why it is not suitable?	Identifiable data is required, without this we would be unable to alert individuals.	
	What steps have been taken to minimise the risk of re-identification of anonymised or pseudonymised data?	Not applicable.	

Step 3 – Data security

Q18 Where will the data be stored?			
Will the data be stored on our servers or servers/cloud external to the Trust?			
Internal	External	Server	Cloud*
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
If external, where will it be stored, will this be the UK, EU/EEA or elsewhere? Provide the location/country ie London, England		The Trust's data will be processed in Azure Databases within the UK	
If the data is processed outside of the EU/EEA, what safeguards will be in place?		Not applicable.	
If a supplier is used they must complete the supplier assurance framework below  Supplier Assurance Framework TEMPLATE		 Copy of NHIS - Supplier Assurance Fr 15 th June 2023 - NHIS have reviewed and assessed as low risk.	
Will the storage be controlled by another party (not the supplier) such as a product/platform supplier ie AWS, Google, Microsoft? Provide details		Yes, the Trust's data is processed in Azure Databases within the UK	
If the data is stored on the cloud the following assessment must be completed by the supplier  Cloud Assessment.xlsx		 Cloud Assessment (Snapcomms).xlsx 15 th June 2023 – this has been identified as Class I, low risk.	

<p>If the data storage or processing is being done by a supplier, what certifications do they hold?</p> <p>When were they, and the proposed storage mechanism, subjected to an external penetration test and is a report available? (Please embed any documentary evidence)</p>			
	Certificate	External Penetration Test undertaken (date)	External Penetration Test Report
Cyber Essentials +/- Cyber Assessment Framework (CAF)			
ISO 15489 Records Management			
ISO 27001 Information Security Standards	 SnapComms (Everbridge) ISO 27001	4 th July 2022	 Secure Documentation.pdf
ISO/IEC 27701:2019 Ext to 27001/27002			
ISO 27017 Cloud Services			
ISO 27018 PII in public clouds			
Digital Technology Assessment Criteria for Health and Social Care (DTAC)			
ISO 9001 Quality Management Systems			
Other, please specify	SOC 2 Type II	31 st March 2023	
If a supplier is used are they registered with the ICO. Check the register ⁶ and provide the certificate number	Yes	No	
	<input type="checkbox"/>	x	
Registration reference: Organisations that do not decide how personal data is processed are exempt. SnapComms			

⁶ <https://ico.org.uk/ESDWebPages/Search>

		is a data processor and do not have to register with the ICO.		
	If a supplier is used, have they completed the Data Security and Protection Toolkit, search the register here ⁷	Yes	No	N/A
		<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	If yes, complete the following	Organisation code	Status	Date Published
		YGM1C	Standards Met	28 th June 2021

Q19	How will this data be secured during storage and when being moved?	
Will it be encrypted when stored and/or moved, if so what type of encryption will be employed?	<p>The data at rest is encrypted using Transparent Data Encryption (TDE) within Microsoft Azure datacenters.</p> <p>This encrypts the storage of an entire database by using a symmetric database encryption key (RSA 2048-bit).</p> <p>SnapComms uses HTTPS/TLS 1.2 for secure communication over the internet.</p>	
Will it be on a server protected by firewall and network intrusion detection?	<p>Yes, Microsoft Defender for Cloud to detect any unauthorised access to the system. This is Microsoft's cloud security posture management (CSPM) and cloud workload protection solution (antivirus/malware).</p>	
What technical controls are in place to prevent hacking of the data by unauthorised persons?	<p>SnapComms employees have strict role based access controls using privileged accounts, including quarterly access reviews and multi-factor authentication (MFA).</p>	
When being moved will it be secured through encrypted file transfer, secure transmission through SLL/TLS/SHS, please explain the specific technical standards that will apply?	<p>SnapComms' uses HTTPS/TLS 1.2 for secure communication over the internet.</p> <p>https://www.ssllabs.com/ssltest/analyze.html?d=svc.snapcomms.com</p>	

⁷ <https://www.dsptoolkit.nhs.uk/OrganisationSearch>

	Do you have a business continuity plan for the information?	Yes, SnapComms have a Business Continuity Management Manual Policy. The Trust's communications team have a business continuity plan and is reviewed regularly.		
	What types of backups are undertaken i.e. full, differential or incremental?	Full	Differential	Incremental
		<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Q20	Who will have access to this data and how will this access be controlled?			
	Will the data be kept on a system that is password controlled, what is the password length and how often does it have to be changed? Who will administer these access controls?	SnapComms user password are a minimum of 8 complex characters and, due to enforced use of multi-factor authentication (MFA), changed every 180 days.		
	Is there an ability to audit access to the information? Can the supplier audit our data?	Yes, all access to the Trust's data is logged for auditing purposes.		
	What other security measures are in place, such as physical security, smartcard, Active Directory, multiple factor authentication?	<p>The Trust's data is processed in Microsoft Azure datacenters. Microsoft manages physical security.</p> <p>Logical access is controlled by Active Directory usernames/password and multi-factor authentication (MFA). All network access is assigned using role-based access controls.</p>		
	Is training available to employees for the new system?	Yes	No	
		<input checked="" type="checkbox"/>	<input type="checkbox"/>	

Q21	If you are using devices such as laptops to access data, how are these secured and managed?			
	SnapComms will only be used on Trust issued devices. Laptops are locked down with domain level security controls. Controls include disk encryption, remote wipe and malware protection. Encrypted VPN connections, authentication via username/password and multi-factor authentication (MFA). Session time out defaults to 15 minutes. Note that SnapComms do not have access to the Trust's data, except for a select few for-support purposes while helping your team with troubleshooting.			

Q22	Is this data an attractive target for criminals and hackers; does it contain			
------------	---	--	--	--

information that may be used for identity/financial fraud or reveal a person possibly being vulnerable to exploitation?	
<p>Yes</p> <p><input checked="" type="checkbox"/></p> <p>Rate its attractiveness from 0 to 10 below. https://nationalcrimeagency.gov.uk/what-we-do/crime-threats/cyber-crime</p> <p>8</p> <p>The following security has been reviewed and put in place to ensure that the application is locked as soon as possible:</p> <ul style="list-style-type: none"> • The application has been processed through the cyber security checks, in which it has passed. • Access to the content centre is managed internally and will only be created by the communications team. • Access from the supplier SnapComms to the content centre is restricted and will only be used when technical support is required. • If a cyber-attack were successful, the communications team would revert to other communication tools to ensure business continuity and the 3rd party supplier SnapComms that hosts the system would be contacted. <p>If this is a risk describe how you will manage it in stage 8.</p>	<p>No</p> <p><input type="checkbox"/></p>


Step 4 – Data use and sharing

Q23	Will this data be shared with anyone else?	
	If yes, explain who these other parties are and why the data is being shared?	SnapComms sub-processor are published at: https://www.snapcomms.com/dpa#annex4


Q24	Are other people processing this data?	
	If a third party such as a company is storing or otherwise managing or using our data, please explain what they doing and why they are doing it?	<p>Microsoft Azure - Hosting Infrastructure One Microsoft Way, Redmond, WA 98052, USA Microsoft Azure is an ever-expanding set of cloud services (IaaS & PaaS) used by SnapComms to deliver its SaaS offering. https://azure.microsoft.com/en-us/global-infrastructure/geographies/ Start Date: 2017, Registration number: UEN201906581Z</p> <p>Stack Path- Content Delivery 2021 McKinney Ave. Suite 1100, Dallas, TX 75201, USA StackPath is a secure Content Delivery Network service used by SnapComms to improve content delivery performance. https://www.stackpath.com/why-stackpath/network/ Start Date: 2019, Registration number: USTX0801564505</p> <p>Pendo- Analytics Provider 301 Hillsborough St Ste 1900, Raleigh, NC 27601, USA Pendo.io, Inc. ("Pendo") is a third-party analytics provider that SnapComms uses to capture how users interact with the Service. SnapComms uses this information to analyze and improve the services. https://www.pendo.io/data-privacy-security/ Registration number: 46-3519724</p> <p>Twilio, Inc.- Email 375 Beale Street, Suite 300, San Francisco, California 94105, USA SendGrid, Inc. ("SendGrid") is an email delivery service provider used within the SnapComms</p>

		<p>application to send notification and password reset email messages. https://sendgrid.com/files/SendGrid-FAQ.pdf Start Date: Dec 2017, Registration number: USDE4518652</p> <p>Elasticsearch - Search Engine 800 W El Camino Real, Suite 350, Mountain View, CA 94040, USA Elasticsearch is a full-text search and analytics engine that SnapComms uses to store, search, and analyze log data quickly and in near real time. https://www.elastic.co/guide/en/cloud/current/ec-reference-regions.html Start Date: 2020, Registration number: USTX0801802463</p>
	<p>If we are using a third-party product that requires maintenance where they access our networks, explain how this will be managed (will they remotely connect, how will this access be managed).</p>	<p>Third-party suppliers do not require access to SnapComms or the Trust's networks. SnapComms send the minimum data via Secured API.</p>
	<p>Is there a process in place to remove personal data if data subject refuses/removes consent? ie The right to restrict processing/the right to object - People can request the use of their data to be restricted in certain circumstances. These will be considered on a case-by-case basis.</p>	<p>Yes, there is a process in place in the Trust and SnapComms.</p>
	<p>Are arrangements in place for recognising and responding to requests for access to personal data?</p>	<p>The Trust has a policy and procedure for responding to subject access requests. Further information for employees on how to access their records is here: https://www.sfh-tr.nhs.uk/work-for-us/your-employees-information/.</p>

<p>Q25</p>	<p>Describe the data flows</p>	
	<p>Please complete the data flow template below to detail how the data is collected, moved and used?</p>	<p>Data flows to be completed as part of the annual data flow mapping exercise undertaken by the communications team.</p>

 New Flow Map UPDATED.xlsm	
<p>Are there security or data protection concerns in any of the data flow stages you identify? If so, please indicate where and what steps you are taking to reduce these risk?</p>	<p>Data flows to be completed as part of the annual data flow mapping exercise undertaken by the communications team. A review will be undertaken by Information Governance following the completion of the exercise.</p>

Step 5 – Processing by or with a supplier/third party

Q26	<p>If you are using a supplier or organisation to process, store or otherwise interact with this data, if not answer N/A</p>	
	<p>What is the arrangement between the Trust and the supplier/third party concerned?</p>	<p>All master agreements with sub-processors obligate the sub-processor to process the data solely for the purposes stated in such master, including any data protection addendums thereto.</p> <div style="text-align: center;">  <small>snapcomms-uk-eme a-hyperlink-master-s</small> </div>
	<p>What activities will the supplier/third party conduct i.e. storage, transport, processing of data on their platform</p>	<p>SnapComms will host the data in a secure cloud environment.</p>
Q27	<p>What steps or measures will you put in place to manage these risks? What measures will you take to ensure processors comply? PLEASE ATTACH COPIES/ RELEVANT SECTIONS OF ANY CONTRACT/ AGREEMENT.</p>	<p>Technical and administrative data privacy controls are in place via our Third-Party Service Provider Qualification policy and contractual agreements.</p> <p>SnapComms’ conducts an annual review of all critical sub-processors, aligned with our “Third-Party Service Provider Qualification Policy”</p> <p>Contract agreements with our sub-processors are internal document only and cannot be shared.</p>

Step 6 – Consultation

Q28	Consider how to consult with those who have an interest in this project	
	Describe when and how you will seek individuals' views or justify why it is not appropriate to do so. i.e. do we need wider public engagement.	The DPIA was reviewed at the Information Governance Working Group for wider stakeholder engagement.
	Who else do you need to involve within the Trust? i.e. Digital Innovations Approval Group (DIAG).	<p>NHIS, Communications and Operation teams leading the project</p> <p>Digital Innovations Approval Group (DIAG) already appraised and have approved the project to continue, subject to clinical oversight for its usage (now approved).</p> <p>All Trust communications to be sent, forewarning users of the pop-ups appearing ahead of planning Trust-wide go-live date of week commencing 26th June 2023.</p>
	Do you need to ask the data processors (supplier) to assist?	No
	Do you plan to consult information security experts, or any other experts?	No

Step 7 – Lawful basis

Q29	What is your lawful basis for processing personal data? Select all that apply	
	a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes. Please note, do not use this if it is for direct care, (e) maybe more appropriate	<input type="checkbox"/>
	b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract	<input checked="" type="checkbox"/>
	c) processing is necessary for compliance with a legal obligation to which the controller is subject	<input type="checkbox"/>
	d) processing is necessary in order to protect the vital interests of the data subject or of another natural person	<input type="checkbox"/>
	e) processing is necessary for the performance of a task conducted in the public interest or in the exercise of official authority vested in the controller	<input checked="" type="checkbox"/>

Q30	What is your lawful basis for processing special categories of personal data? Select all that apply	
	a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes. Please note, do not use this if it is for direct care, (h) and/or (i) maybe more appropriate	<input type="checkbox"/>
	b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment	<input type="checkbox"/>
	c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent	<input type="checkbox"/>
	e) processing relates to personal data which are manifestly made public by the data subject	<input type="checkbox"/>
	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	<input type="checkbox"/>
	i) processing is necessary for reasons of substantial public interest, i.e.	<input type="checkbox"/>

	public health, such as protecting against serious cross-border threats to health	
	j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purpose	<input type="checkbox"/>

Stage 8 – Risk Template

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

Completed by: Gina Robinson

Role: Information Security Officer

Date completed: 12th June 2023

Guidance notes:

Confidentiality - Are there any risks to the confidentiality of personal data? Do employees have a legitimate relationship in order to process personal data? Is personal data disclosed to people who do not require it?

Integrity - Systems must be designed so that the input and management of information is not prone to human error and that the flow of information does not result in loss or alteration. Data should be complete and accurate and not tampered with during or after submission. Ensuring that during the process of transmission data integrity is maintained.

Availability - System design must include appropriate access controls and checks, so that the information in the system has consistency, accuracy, can be trusted as correct and can be relied on when providing healthcare. Data is available and delivered to the right person, at the time when it is needed and that there is accessibility to systems at all times. Having safeguards in place for power outages, natural disasters, hardware failures and systems upgrades.

Examples of risks that are common in projects is included below. Please amend/delete, as necessary.

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)	

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 due to connection failure or server failure either via NHIS or 3 rd party supplier. This could result in the service being disrupted or unavailable. The consequences of this could be enforcement action and reputational damage to the Trust	Full system back-up processes and ISO 27001 accreditation in place Business continuity plan in place Regular updates from supplier to advise users of any planned updates and a process is in place to contact all main users for support during any unplanned downtime	1	2	2		1	2	2	
Loss of system data due to connection failure or server failure by third party supplier.	Full system back-up processes and ISO 27001, accreditations in place Business continuity plan in place	1	2	2		1	2	2	

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)	
<p>This could result in the service being disrupted or unavailable.</p> <p>The consequences of this could be enforcement action and reputational damage to the Trust.</p>									
<p>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</p>	<p>In the Trust we have a business continuity plan if the service was unavailable. The department would default back to the current practice and contact employees via all user emails, social media, updating the website/intranet</p>	2	2	4		2	1	2	<p>SnapComms 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</p>

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)	
Data is accessed inappropriately due to lack of access controls. Movers and leavers access not removed. Data is inappropriately processed and/or disclosed	Username and password controls in place. Access is managed within the communications team. Account Management and access procedure to be audited on a regular basis. Appropriate access according to role. IG Training in place	2	2	4		2	2	4	



Risk Scoring Matrix.pdf

Step 8 – Legal compliance

To be amended by Information Governance from the responses provided in the previous stages.

UK General Data Protection Regulation 2018	Compliance
<p>Principle 1 – Personal data shall be processed fairly and lawfully and, in a transparent manner</p>	<p>Lawfulness</p> <ul style="list-style-type: none"> • 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 do not do anything generally unlawful with personal data. <p>Fairness</p> <ul style="list-style-type: none"> • 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. <p>Transparency</p> <ul style="list-style-type: none"> • We are open and honest and comply with the transparency obligations of the right to be informed.
<p>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</p>	<ul style="list-style-type: none"> • 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

	<p>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.</p>
<p>Principle 3 – Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed</p>	<ul style="list-style-type: none"> • We only collect personal data we actually need for our specified purposes. • We have sufficient personal data to properly fulfil those purposes. • We periodically review the data we hold and delete anything we do not need.
<p>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</p>	<ul style="list-style-type: none"> • 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
<p>Principle 5 – Kept no longer than is necessary.</p>	<ul style="list-style-type: none"> • 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. • We clearly identify any personal data that we need to keep for public interest archiving, scientific or historical research, or statistical purposes.
<p>Principle 6 – Appropriate security, including protection against unauthorised or unlawful processing and against accidental</p>	<ul style="list-style-type: none"> • 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.

<p>loss, destruction or damage.</p>	<ul style="list-style-type: none"> • When deciding what measures to implement, we take account of the state of the art and costs of implementation. • We have an information security policy and take steps to make sure the policy is implemented. • When deciding what measures to implement, we take account of the state of the art and costs of implementation. • We make sure that we regularly review our information security policies and measures and, where necessary, improve them. • We have assessed what we need to do by considering the security outcomes we want to achieve. • We have put in place technical controls such as those specified by established frameworks like Cyber Essentials. • We understand that we may also need to put other technical measures in place depending on our circumstances and the type of personal data we process. • We use encryption and/or pseudonymisation where it is appropriate to do so. • 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. • Where appropriate, 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.
<p>Principle 7 – Accountability principle</p>	<ul style="list-style-type: none"> • We take responsibility for complying with the UK GDPR, at the highest management level and throughout our organisation. • We keep evidence of the steps we take to comply with the UK GDPR. • We put in place appropriate technical and organisational measures,

such as:

- adopting and implementing data protection policies (where proportionate);
- taking a 'data protection by design and default' approach - putting appropriate data protection measures in place throughout the entire lifecycle of our processing operations;
- putting written contracts in place with organisations that process personal data on our behalf;
- maintaining documentation of our processing activities;
- implementing appropriate security measures;
- recording and, where necessary, reporting personal data breaches;
- carrying out data protection impact assessments for uses of personal data that are likely to result in high risk to individuals' interests;
- appointed a data protection officer; and
- adhering to relevant codes of conduct and signing up to certification schemes (where possible).
- We review and update our accountability measures at appropriate intervals.

Step 9 - Assessment Summary

To be completed by Information Governance.

Outcome of Data Protection Impact Assessment	
Project is not recommended to proceed, as significant risks have been identified.	
Project to proceed once identified risks have been mitigated as agreed.	X
Project has met required legislative compliance and poses no significant risks. No further action required.	

Summary of Data Protection Impact Assessment; including legislative compliance and identified risks	
Legislative Compliance:	<p>Suggested text, remove, amend, as necessary.</p> <p>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.</p> <p>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)</p> <p>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</p>
Summary of Risks	<p>Suggested text, remove, amend, as necessary.</p> <p>Cyber security, loss of data, inappropriate access to data, inability to access data and Information Asset Management.</p>
Identified risks	
The risk	Mitigation
Loss of system access	Full system back-up process in place

Loss of system data	Full system back-up process in place
Data is accessed inappropriately	Individual usernames and passwords are provided

Step 10 - Recommendations for Action

Summary of recommendations (amend/delete as necessary)		
Recommendations	Recommendations	Agreed deadline for action
Information Asset Administrators to ensure SnapComms is added to the information asset register and data flows are mapped and recorded	IAO/IAA	30 th June 2023
Ensure business continuity plans are in place	IAO/IAA	30th June 2023
Account management Standard Operating Procedure generated and implemented, routine audit to take place	IAO/IAA	30 th September 2023

Step 11 - Project signoff

	Name	Job Title	Date
Information Asset Owner*	Richard Brown	Head of Communications	20th June 2023
Data Protection Officer	Jacque Widdowson	Information Governance Manager	19 th June 2023
Senior Information Risk Owner	Sally Brook Shanahan	Director of Corporate Affairs	27th June 2023
Caldicott Guardian	Dr David Selwyn	Medical Director	23rd June 2023
Chief Digital Information Officer	Richard Walker	Chief Digital Information Officer	22nd June 2023
Patient safety⁸	Not applicable		

The Data Protection Impact Assessment must be reviewed and approved by the Information Asset Owner, Data Protection Officer, Senior Information Risk Owner and Caldicott Guardian. Approval does not close the data protection risks related to this project.

*It is important that the risks and the original scope of the project are reviewed on a regular basis to ensure any new confidentiality, integrity or availability risks are identified, documented, and mitigated wherever possible. All amendments must be approved following the approvals process.

⁸ [DCB0129: Clinical Risk Management: its Application in the Manufacture of Health IT Systems - NHS Digital](#)