Sherwood Forest Hospitals
NHS Foundation Trust

Data Protection Impact Assessment

Digital Communication via Letter using PKB portal and Synertec	**Ref number**

PAGE	1-16	1-17	1 - 17	1-19	1-19	1-20	1-21
ISSUE	V 0.3	V 0.4	V3.0	V4.0	V5.0	V5.1	V5.2
DATE	Sept 2015	Sept 2015	Dec 2015	June 2017	Nov 2017	June 2018	October 2018

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. Nottinghamshire Health Informatics Service, who are hosted by Sherwood Forest Hospitals NHS Foundation Trust, provides information Communication and Technology services. Nottinghamshire Health Informatics Service is responsible for implementation of Information Communication and Technology systems and provision of the network infrastructure.

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	✓	
Complete Project Details and check the Initial Screening Questions	✓	
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	✓	✓
Initial Screening Questions to be formally written up and Introductory Meeting to be formally recorded		✓

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

OR

If a Data Protection Impact Assessment **IS** required		
Activity	**Implementer**	**Governance**
Complete Stage 2 – Data Protection Impact Assessment (Full)	✓	✓
Complete Stage - 3 Work Flow Mapping	✓	✓
Complete Stage - 4 Identified Risks and Mitigating Action	✓	✓
Complete Stage – 5 Legal Compliance		✓
Complete Assessment Summary & Recommendations for Action		✓
Closure meeting for final agreement	✓	✓
Ensure Sign Off is completed	✓	
Assessment shared with customer if appropriate	✓	
Assessment to be kept with project documentation copy to Corporate Governance	✓	

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:	Digital Communication via Letter using PKB portal and Synertec

Project Description: Describe in sufficient detail for the proposal to be understood
Currently all written communications with patients are sent as hard copies either via the Royal Mail or through Synertec our mailing provider in the case of Medway appointment letters. The aim of this project is to enable patients to receive their written communications via a portal provided by Patients Know Best. The intention is for all letters to be directed to our mailing company, Synertec, who will then identify if the recipient has agreed to receive their communications digitally. If so the letters will be placed in the portal and the patient will receive a text message asking them to access their account. If the letters are not accessed within an agreed time period the letter will be posted. Those patients without a PKB account will continue to receive their letters by post Synertec currently process letters for Outpatient and Breast screening letters for the Trust. These letters are currently processed by Synertec's Prism software and sent via Synertec's Pay As You Mail service; Outpatient letters will also be uploaded to Patient Knows Best (PKB) in the near future. Patients will be able to access their letters digitally using Patient Knows Best.

Overview of the proposal: ***What the project aims to achieve***
To offer a digital solution to all patients in receiving communications from Sherwood Forest Hospitals NHS Trust. This will also result in some financial savings due to the reduced costs in comparison to mailing all letters. This will allow patients to access all of their appointment letters in one location and they will not need to worry about them being mislaid.

Implementing Organisation:	Sherwood Forest Hospitals NHS Foundation Trust

Staff involved in DPIA assessment (Include Email Address):	Ann Gray and Sarah Chinery

Key Stakeholders/Customers:	All SFH Staff

Project Sign Off

	Name	Job Title	Organisation	Date
Information Asset Owner	Elaine Torr	Divisional General Manager	Sherwood Forest Hospitals NHS Foundation Trust	**11th January 2021**
Information Governance	Gina Robinson	Information Security Officer	Sherwood Forest Hospitals NHS Foundation Trust	**5th October 2020**
Third Party Representative *(someone aware of project and appropriate level of responsibility)*	lucy.wiggan@synertec.co.uk		Synertec	**5th October 2020**
Caldicott Sign Off	Shirley Higginbotham	Director of Corporate Affairs	Sherwood Forest Hospitals NHS Foundation Trust	**11th February 2021**
Senior Information Risk Owner	Paul Robinson	Chief Financial Officer	Sherwood Forest Hospitals NHS Foundation Trust	**23rd April 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 no significant risks. No further action required.	☐

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

Summary:
The supplier assurance framework has identified very likely risks. The supplier assurance framework is designed to enable the Trust to gain a level of assurance from suppliers and service providers with regard to the security of assets throughout the lifetime of the contract and potentially beyond.

Risks to SFHFT:
Information and Communications Technology (ICT) Services, Business Process Outsourcing, Transport/Mail, and Storage/Archive most closely describe the services provided to SFHFT.
The services provided to SFHFT have access to, process and store any of SFHFT's assets (including data) in the delivery of service and has access to, process and store data in the delivery of service.
Personal data and Sensitive personal data as defined by the Data Protection Act are stored and processed in the delivery of service.
The volume of personal data processed is over 500,000.
Approximately more than 50 staff has access to assets.
Sub-contractors are used in the delivery of service.
Two sub-contractors have access to assets.
In relation to the ICT systems used to deliver service, remote working is permitted.
The organisation holds accreditations/certifications relating to ICT systems used in the delivery of service:

- ICT system/s are ISO27001:2013/2013 certified – No
- ICT system/s are compliant with ISO27001:2013/2013 – No
- System/s are compliant with a standard that is aligned to ISO27001:2013/2005 – Yes
- Cyber Essentials – No

The physical and environmental risk assessment did not cover manned guarding.
A forensic readiness policy documenting the approach to managing digital evidence relating to ICT security incidents is not in place.
The company does not provide guidance to staff on handling information with respect to the Official Secrets Act.
Right to audit is not detailed in contracts and is not exercised.

The need to meet recognised standards (such as ISO27001:2013) is not stipulated.

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	But this information is already collected within existing systems such as Medway
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	PKB and Synertec will receive patient name, address, verified NHS number's, District number's and when clinic letters are included date of birth will also be provided on the letters sent through. At this point detailed medical information will also be provided which may be sensitive
4	Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?	N	
5	Are there processes in place to ensure data is relevant, accurate and up-to-date?	Y	Outpatient SOP includes a requirement to check patient demographics each time they attend for an appointment. All appointment letters remind patient to inform us of any demographic changes
6	Are there security arrangements in place while the information is held?	Y	Demographic information is stored in Medway PAS and accessed via individual role based access. Patient case notes are stored securely on site.
7	Does the project involve using new technology to the organisation?	Y	PKB Portal. The Trust has been using Synertec since 2010
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	

Q	Screening question	Y/N	Justification for response
If you have answered "Yes" to any of the questions numbered 1-8 please proceed and complete stage 2.			
9	Is a Patient Safety Review required?	Y	The patient safety case identified no issues and was signed off 21 October 2020
10	Is a Quality Impact/Technical Security Review required?	Y	NHIS have reviewed the Supplier Assurance Framework and identified no security risks

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

Stage 2 – Data Protection Impact Assessment

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

2.2.1	What data will be processed?					
	Personal Data:					
	Forename	☒	Surname	☒	Age	☐
	DOB	☒	Gender	☐	Address	☒
	Post Code	☒	NHS No	☒	Hospital No	☒
	Other unique identifier (please specify)					
	Sensitive Persona 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?	☐

2.3	Is the data required to perform the specified task?	
	Y/N	Please justify response **Yes or No**
	Y	In order for the patient to be identified and communication to be sent to the correct individual and for the patient to receive the information they need regarding their healthcare/appointments
2.3.1	How will you collect, use, store and delete data?	
	Referrals are received from GPs via eRS and any updates to demographics from the patients themselves. Demographic information is stored in Medway PAS and accessed via individual role based access. Patient case notes are stored securely on site. Currently the Trust is not destroying paper or electronic patient records in line with the Records Management Code of Practice 2020	
2.3.2	What is the source of the data? (i.e. from data subject, system or other third party)	
	Initially Medway but may involve other systems such as CRIS, Winscribe etc.	
2.3.3	How much data will you be collecting and using?	
	No additional data to be collected other than patients request for an account	
2.3.4	How often? (for example monthly, weekly)	
	On-going as new patients are referred to the Trust	
2.3.5	How long will you keep it?	
	Currently the Trust is not destroying paper or electronic patient records in line with the Records Management Code of Practice 2020	
2.3.6	Where will the data be stored? i.e. Medway, Shared Drive, offsite storage	
	With PKB/Synertec and within Medway if patient requests to be exempt	
2.3.7	How many individuals are affected?	

	Any patient who signs up for a PKB account. All patients will be asked if this is required. All patients within the geographical location of Nottinghamshire and will include out of area patients who attend the Trust
2.3.8	What geographical area does it cover?
	Anywhere in the UK

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

2.5	Does a third party have access to existing network or systems (remote or onsite)?	
	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**
		NHIS have undertaken with no security risks identified synertec - Supplier Assurance Framework
2.5.1	Please describe access and controls in place	
	Data is submitted by the Trust to Synertec; Synertec does not unilaterally collect data from the Trust or their systems. As such, the data is limited to that submitted by the Trust. The Trust can control	

	who may submit data to Synertec's systems. Synertec Employees Data is stored on servers, which are located in locked server rooms at each of our company premises. Physical access to the server rooms and remote access to the servers is restricted to those who require access to perform their duties. Data stored on the Synertec network is also segregated between different network drives and shared folders. Employees are only given access to the resources they need to do their job; Active Directory User Accounts and Security Groups are utilised for this purpose. Synertec operates its PAYM service from three sites. No other locations are involved in data storage or data handling, or host service desks, data hosting or disaster recovery facilities. Head Office is based in Wellington (Somerset) which is the main administration and support centre for the business and is involved in data storage, data handling, and host service desks. Production sites are based in Bristol and Warrington and they primarily produce the documents for our customers and are involved in data storage and data handling. Our ISMS is in place to control and mandate employee behaviour with regards customer data; for example: AES-256-bit encryption standard is adhered to for all data transfers up to the point of printing and mailing: • During upload from customer network to Synertec's PAYM system (Pay As You Mail) • During communication between Synertec's Head Office and other Synertec sites • When stored on removable media Customer data is never: • Shared with organisations to which the data does not belong • Sent by email without first encrypting it • Communicated via the same mechanism as associated passwords In addition, Synertec:

	• Operates a policed Clear Desk and Clear Screen policy • Regularly enforces employee questionnaires to test understanding of how customer data must be handled • Maintains specific controls and procedures for Remote Workers, e.g. encryption of laptop hard drives • Backs up data daily, with backups encrypted to AES-256-bit standard in order to prevent unauthorised access. The backups are only handled by members of the I.T. Department • Does not host data on any cloud-based solution within the U.K nor outside • Ensures no data is exposed to the Internet/web-sites Remote Access Some Synertec employees are able to gain access to computers belonging to Synertec customers as part of Synertec's 'remote support' facility. Whilst it is acknowledged that the Trust has responsibility for keeping their systems secure, it is prohibited for this facility to be used to access, or attempt to access, any customer systems or locations without explicit permission from the Trust. Trust Access Users are able to use our desktop software, Prism Client, in order to access their data. To retrieve documents submitted to the Prism software at the Trust site, employees must be granted access within Prism Client by one or more nominated "administrative users". A simple group-based security model is employed. Prism Client software communicates with the Prism Server application on the Prism Unit. The Prism server will accept documents submitted from the Trust LAN, and enable LAN users to access the documents. The Prism Server checks credentials of those attempting to access archive documents. All such access is logged, whether successful or not.
2.5.2	Please provide a copy of the contract in place
	PDF 2019_10_01_Sherwood Forest Hospitals NH

2.5.3	Have arrangements for retention and destruction been included in the contract when the service/contract expires?
	Data at the Trust Synertec’s Prism software is installed on the Trust’s server on their network. Document data is accepted by the Prism software and it is assumed that the Trust will secure this server in such a way as to only allow authorised access. All configuration, processing, routing and storage of document data, occurs on the Trust’s server. All documents accepted and processed by the Prism software are maintained in an archive ‘Trust side’ to allow for the review and retrieval of those documents at a later date if required. The documents in this archive are stored in an encrypted form at all times. Data retention periods are defined according to Trust requirements and can be varied, if required, by document type. Documents despatched via our PAYM (Pay As You Mail) service are transferred to Synertec’s servers for processing. Document data uploaded from customer sites to Synertec is encrypted to AES-256 bit standard and utilises SFTP (Secure FTP). Synertec-side Segregation of customer data is fundamental to all of Synertec’s services for our customers. Synertec’s bespoke systems segregate all data by owner (i.e. customer A’s data will be kept separate from customer B’s data) throughout the process of moving data into Production. Synertec archives customer document data for a period of 90 days as standard on its servers. These servers are secured in such a way as to only allow authorised access, and the documents in this Synertec-side archive are stored in an encrypted form at all times. Archived data will be present on Synertec’s encrypted backups for a maximum of 12 weeks beyond this retention period. Backups are only accessible to system administrators. This archiving allows full traceability of documents for a reasonable period following despatch. Customers can request that Synertec varies the retention period for a specific reason, if appropriate. After the standard 90 day retention period deletion of the document data is then completed, without manual involvement, using a secure deletion algorithm that complies

	with DoD 5220.22-M media sanitisation standards. Synertec do not operate an outsourced data centre. Customer data is never stored outside of the U.K, and all Synertec offices, as well as our printing and mailing facilities, are located inside the U.K.	
2.6	Will this information be shared outside the organisations listed above?	
	Y/N	if answered **Yes** please describe organisation/s and geographic location
	Y	Patient Knows Best, Registered Office: Patients Know Best St John's Innovation Centre, Cowley Road Milton, Cambridge, CB4 0WS Phone: 01223 790708
2.7	Does the work involve employing contractors external to the Organisation?	
	Y/N	If **Yes**, provide a copy of the confidentiality agreement or contract?
	Y	PKB and Synertec Nottinghamshire_Connect___Patients_Know
2.8	Has a data flow mapping exercise been undertaken?	
	Y/N	If **Yes**, please provide a copy here. 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 complete – Section 3
	Y	Please see attached ‘Synertec Data Encryption Path’ and ‘Synertec Production Timeline’ relating to documents despatched via Pay As You Mail. Please also see ‘PKB Prism Data Flow’ which shows the data flow for data for upload to PKB.

		Synertec Data Encryption (Data Path) PKB Prism Data Flow.pdf				
2.9	What format is the data?					
	Electronic	☒	Paper	☒	Other (Please describe)	Data is submitted electronically to Synertec’s Prism software. Following processing, the data may be despatched as traditional letters, emails, SMS, or it may be uploaded to a 3rd party portal (PKB).

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	Trust users are able to use our desktop software, Prism Client, in order to access their data. To retrieve documents submitted to the Prism software at the Trust site, employees must be granted access within Prism Client by one or more nominated “administrative users”. A simple group-based security model is employed. The Trust has 1 individual set up as an administrator. Prism Client software communicates with the Prism Server application on the Prism Unit. The Prism server will accept documents submitted from the Trust LAN, and enable LAN users to access the documents. The Prism Server checks credentials of those attempting to access archive documents. All such access is logged, whether successful or not. Synertec cannot guarantee that every access to data by a Synertec employee can be linked to an individual user or system: • Trust data being sent via the PAYM service takes the form of data files. Although these are restricted to those requiring access as part of their job role, it is not possible to attribute every access to an individual person. However: • User network activities (including logon/off times,

		failed login attempts etc...) are automatically logged for security purposes • Logon hours are restricted in order to balance security whilst allowing normal working activity for employees • Repeated failed login attempts cause account lockout and the generation of an alert, which is investigated by I.T. employees as a possible attempt to breach security • Synertec's ISMS policy states that employees must not attempt to log on to any Synertec system using credentials other than those provided to them
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**
	Y	There are no changes to the demographics held in Medway but the transfer of demographic information via the PKB Portal is new
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?	
	There will be a daily update from SFH from Medway to PKB/Synertec with up to date details required to send details to patients Data is submitted to Synertec's Prism software by the Trust. The quality and accuracy of this data is the responsibility of the Trust. The data received will be processed and retained in agreement with the Trust. It will not be amended, used, or retained by Synertec outside of the purposes of the agreed processing. The data will be 'single use' in that it comprises individual documents, which do not require keeping up to date. As this relates to patients demographics, we check with patients each time they attend if these details are correct, we also include advice in all communications for patients to advise us if their details have changed and need amending e.g. appointment and admission letters.	
2.13	Who will have access to the information? (list individuals or staff groups)	
	Synertec employees are given access only to data and resources they require to perform their job role, with limited users possessing	

	local administrative rights. System administrators perform their routine day-to-day tasks when logged in under a user account without system administrative privileges. Access is controlled by methods consistent with our ISMS policies. Only Synertec employees have access to customer data. Data is segregated between different network drives and folders. Applications for access to secured areas must be made in writing via the Asset Request procedure. Applications require approval from the IT Director or Data Protection Officer.	
2.14	What security measures have been implemented to secure access?	
	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)	☒
	Other - Patient receive a text to alert them to access their account within the portal. The above measures relate to the data when at a Synertec site.	
2.15	Will any information be sent offsite? – i.e. outside of the organisation and its computer network	
	Y/N	Please describe if answered **Yes**
	Y	Letters will be sent electronically to Synertec/PKB either to be onward posted or placed within the portal for patients to access. Yes – If ‘the organisation’ refers to the Trust: Synertec

		operates its PAYM (‘Pay As You Mail’) service from three sites, all based in the UK. No other locations are involved in data storage or data handling, or host service desks, data hosting or disaster recovery facilities. Head Office is based in Wellington in Somerset which is the main administration and support centre for the business and is involved in data storage, data handling, and host service desks. Production sites are based in Bristol and Warrington and they primarily produce the documents for our customers and are involved in data storage and data handling. Both production sites provide disaster recovery provisions for each other as our system is designed to allow immediate redirection of work to any production site. The Bristol site also provides the disaster recovery provision for our Head Office. When uploading Outpatient letter data to Patient Knows Best (PKB), the data will also be uploaded from Synertec to PKB for processing. For information regarding their data security measures, please contact Patient Knows Best directly.		
	Are you transferring personal data to a country or territory outside of the EEA?			
	Y/N	Please identify data sets and destinations if answered **Yes**		
	N			
2.16	Please state by which method the information will be transferred?			
	Email (not NHS.net)	☐	NHS.net	☐
	Website Access (internet or intranet)	☐	Wireless Network (Wi-Fi)	☐
	Secure Courier	☐	Staff delivered by hand	☐
	Post (internal)	☐	Post (external)	☐
	Telephone	☐	SMS	☐
	Fax	☐	Other (please specify below)	☒

	Data is transferred from the Trust to Synertec's infrastructure over an encrypted connection over the HSCN. Pay As You Mail data: Once data is uploaded to Synertec's PAYM Service it passes to the production centres over Synertec's secure VPN structure. At no point is data accessible to third parties.	
2.17	Are disaster recovery and business contingency plans in place for the information? What types of backups are undertaken i.e. full, differential or incremental?	
	Y/N	Please describe if answered **Yes.** Please state why not if response is **No.**
	Y	If access to the portal is unavailable letters will be posted by Synertec to the patient. If Synertec are unable to process letters either electronically or via hard copy for postage they can be printed, enveloped and posted at SFH. Whilst Synertec will provide as much assistance as possible in the event of data loss, Prism is not supplied with any inbuilt backup functionality. As such, the backup of Prism files is the responsibility of the Trust. We strongly recommend that this backup is incorporated into your existing backup methods to ensure there is no loss of critical files. The following locations must be incorporated into your daily backup routine: • C:\ Sher_Fore_Hosp_NHSFT\Acquired\ (recursive) • C:\ Sher_Fore_Hosp_NHSFT\Lookup\ • C:\Prism\Programs\Prism.mdb The contents of these folders can be used to completely restore the data and user settings for your Prism system in the event of a 'disaster'. When notified that a 'disaster recovery' situation has been invoked, Synertec will prioritise the restoration of the Trust's Prism system, with all timescales being dependent upon the

		Trust’s ability to provide critical items. Appropriate hardware or a virtual machine must be provided, onto which the Prism software can be installed, along with a backup of the Trust’s Prism system to allow the restoration of customer data and Prism user settings. Alternatively, the Prism software can be easily installed on another machine (physical or virtual) and the data restored over time (to minimised downtime). In such instances, Synertec can help implement a “hot spare” backup Prism system for customers wishing to further minimise any downtime. **Synertec disaster recovery (a full business continuity statement is available upon request):** A ‘disaster’ has never been declared, however Synertec has robust disaster recovery procedures in place to ensure that in the event of a ‘disaster’ there is minimal impact upon our business continuity. At Synertec we print our customers’ documents in real-time across multiple production sites. If one of these production sites cannot print, insert, or despatch documents to meet our production service levels; we are able to remotely divert documents to another of the production sites to be processed (utilising real-time mirroring). Our production sites are located across a wide geographical area and it is therefore unlikely that a disaster will affect all of these locations concurrently. The plan allows for recovery of PAYM (Pay As You Mail) services to customers within 48 hours of a disaster being declared. We also have facilities in place, in the form of a ‘cold’ site, should a ‘disaster’ occur at our Head Office based in Wellington. These include a furnished and networked office environment which can operate as a fully functional Head Office facility within 0-48 hours (dependent upon the nature of the ‘disaster’). In the Trust if Sysertec is unavailable we have a process in place where we print the letters, envelope them and frank them and send out to the patients. We check each day that the letters have left Medway and transferred across to

		Synertec. If they haven't then there is dialogue between them and us and we assess how long we can leave this before deciding to implement the business continuity process. There have also been occasions when Synertec have advised us that they have not received the letters from us and then the same actions are taken.
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	Confidentiality is covered with all employees as part of their Contract of Employment. All employees are bound by the conditions laid out in the Synertec Staff Handbook and the ISMS policy; mandatory compliance with all rules and regulations within this are agreed upon when signing the Contract of Employment. On commencement of employment, all company employees are issued with our ISMS policy, which details our security / data privacy policies. Induction training and testing is also carried out at this time. Additional training is also provided for all employees on the subjects of social engineering, information governance, and security incidents. All employees are required to be familiar with the ISMS and regular emails are sent out on the subject to all employees to keep data security issues in the spot-light. Regular employee questioning is completed, with mandatory re-testing for those failing to score adequately. We also have security awareness posters and screen savers that constantly remind employees of Data Security issues. Bulletins are sent out by the Data Protection Officer where awareness of a new situation (e.g. an increase in volume of phishing emails, or a Security Incident) could itself provide some mitigation against another Incident.
2.19	Will reports be produced?	
	Will reports contain personal/sensitive personal or	Synertec provide a comprehensive set of audit

	business confidential information?	reports to ensure our customers: • Can confirm all of their documents have successfully reached Prism • Have visibility of the document process, with each stage of this being transparent and easy to reconcile Once your documents have reached Prism, Synertec will ensure that the documents are processed as anticipated and despatched in expected timescales. However, we must stress that it is your responsibility to ensure that the correct number of documents have reached Prism, to isolate any issues as soon as possible. It is therefore essential that you arrange for these reports to be viewed when received and any discrepancies highlighted as soon as possible to Synertec, so they can be investigated and addressed accordingly. It is highly recommended that more than one person receives the reports and that each report is received by an appropriate set of recipients to ensure document numbers are easily reconciled. **Frequently Asked Questions** What happens if I don’t receive a report or it appears to be incorrect?

		If you have not received a report, or you are concerned that the figures on it appear to be incorrect, you should raise this with Synertec immediately by contacting your Customer Service Advisor. I don’t want these reports. Can they be suppressed? Once set up, requests to suppress one or more reports must be made in writing by an authorised contact point within your organisation. If I receive an Invalid Address Report, will the affected documents still be posted? Yes, however the documents will be sent via the Royal Mail 2nd Class tariff, rather than the discounted Business Class tariff that is applied to documents that have a valid address. How do I check the validity of addresses? To check the validity of an address, use the Royal Mail Postcode finder: 1. Go to www.royalmail.com/postcode-finder 2. Enter the address details in the spaces provided and click the ‘Find…’ button 3. You will then be provided with details of whether or

		not the address is valid **Sensitive information:** Some bespoke reports may contain Patient Identifiable Data, but these will only have been set up at the Trust's specific request, and following agreement with the Trust.
	Who will be able to run reports?	Synertec will provide the Prism audit reports on a regular and agreed schedule. They are also accessible within Prism Client, which the Trust's users have access to.
	Who will receive the reports and will they be published?	The Prism audit reports will be received by contacts nominated by the Trust. They will not be published beyond this by Synertec.
2.20	If this new/revised function should stop, are there plans in place for how the information will be **retained / archived/ transferred or disposed of?**	
	Y/N	Please describe if answered **Yes.** Please state why not if response is **No.**
	Y	The team would liaise directly with Procurement and the current contract is on a standard NHS contract with terms and conditions included for termination
2.21	Is consent required for processing of personal data?	
	Y/N	Please describe if answered **Yes**
	Y N	For letters to be added to the portal the patient has to request a PKB account Letters sent by post will be automatically processed by Synertec on behalf of the Trust as part of our statutory duties under GDPR 6(1)(e) public interest or public duty

		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?
2.22	Will individuals be informed about the proposed uses and share of their personal data?	
	Y/N	Please describe if answered **Yes.** Please state why not if response is **No.**
	Y	The information letter asking patients to sign up for an account will provide this information.
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.**
	N/A	Letters sent by post will be automatically processed by Synertec on behalf of the Trust as part of our statutory duties under GDPR 6(1)(e) public interest or public duty
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	Having a PKB account is a patient choice. Patients can still receive hard copy letters if this is preferred SFH PKB Support 1.1.xlsx
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 a well-established FOI/Access to Health Records process in place.

2.26	Who are the Information Asset Owner(s) and Administrator(s)?	
	IAO	Elaine Torr
	IAA	Ann Gray
2.27	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.**
		SAF sent to NHIS for review. Synertec contract has been in place for over 10 years. No security issues identified by NHIS
2.28	Are there any current issues of public concern that you should factor in?	
	Y/N	Please describe if answered **Yes.**
		None known
2.29	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?	
	Allows patients to receive communications swiftly and by digital means. This will also have an advantageous financial impact to the Trust.	
2.30	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?	
	There is a patient representative on the Project Board and any communications have been approved by the Trusts Public Involvement Forum	

2.31	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).
2.32	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)
	Patient privacy notice on the website and includes a link to PKB information. DPIA

	will also be published once finalised

2.33	What measures do you take to ensure processors comply?
	Synertec is not aware of any sub processors involved in this project, for which it is responsible for ensuring compliance.
2.34	How will you prevent function creep?
	Synertec will only ever process the Trust's data as per explicit agreement with the Trust.

Stage 3 - Risk Assessment Form

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

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 transmission of daily data update	Regular upkeep of servers and process of checking transfer has taken place	2	1	2		2	1	**2**	
Loss of power either at the Trust or Synertec	Backup generator available at the Trust	2	1	2		2	1	**2**	

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.