Nottinghamshire Health Informatics Service
Transforming care through technology

NHS
Sherwood Forest Hospitals
NHS Foundation Trust

Privacy & Security Impact Assessment

Title	Ref number
Electronic Prescribing & Medicines Administration (EPMA)	EPMA 0000100

PAGE	1 - 19	1 - 21	1-21	1-23	1-23	1-23	1-23	1-24
ISSUE	V 0.1	V0.2	V0.2.1	V0.3	V0.3.1	V0.4	V0.5	0.6
DATE	April 2020	June 2020	June 2020	July 2020	July 2020	July 2020	Aug 2020	Aug 2020

Introduction

A Privacy & Security Impact Assessment enables Sherwood Forest Hospitals NHS Foundation Trust (SFHT) 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 the 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.

Privacy & Security Impact Assessments 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 organisations.

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 Privacy & Security Impact Assessment has a responsibility to ensure that Patient Safety, Technical Security and Quality Impact Assessments are considered, in line with NHIS and the Trust procedure.

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 Privacy & Security Impact Assessment (Full) **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 Privacy & Security Impact Assessment (Full) **IS** required Activity	Implementer	Governance
Complete Stage 2 – Privacy & Security 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 used by both NHIS and SFHFT jointly to complete the Privacy Impact Assessment (PIA) process. The *Governance* section will be completed by SFHFT IG Team with support from the relevant NHIS specialist teams as applicable.

Project Details

Project Title:	Electronic Prescribing & Medicines Administration (EPMA)

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

The Nervecentre EPMA solution will support Sherwood Forest Hospitals FT in standardising processes which will improve patient safety and efficiency by adding choice, prescribing, administering and supply of medicines. Although still in development, the implementation has the potential to achieve significant local and Integrated Care System (ICS) level strategic benefits beyond EPMA with the same supplier.

The Nervecentre EPMA solution offers the best fit towards the wider digital strategy and Trust aims and objectives, aligning with the direction of travel within the Nottingham and Nottinghamshire ICS. The Trust is forming a development partnership with Nervecentre and University Hospitals of Leicester who have recently signed a ten-year contract with the supplier for their EPR/EPMA solution. Other ICS partners may sign up to the same solution which would further strengthen the development partnership.

The key drivers for change include:

- Reduction in patient harm;
- Improved patient experience;
- Improved formulary adherence;
- Improved staff efficiency;
- Improved clinical coding;
- Reduced claims incidence;
- Improved discharge;
- Reduction in transcription and prescribing errors;
- Data-driven compliance with commissioner requirements

The project aims to take the medicines processes from paper to digital thereby enhancing communication of prescribing, aiding choice, administration and supply of medicine via information and decision support and providing a robust audit trail for the entire medicines process.

The plan is to pilot EPMA on a ward in February 2021 onwards before being rolled out to all adult inpatient areas (excluding critical care) across the Trust. In summary, the implementation of EMPA aims to deliver the following:

- Electronic generation of the prescription;
- Electronic recording of medicines administration;
- Electronic transmission of medicine supply requests to Pharmacy;
- VTE electronic assessment;
- Discharge prescription, summary of care and electronic communication to GP's;
- Alerts and decision support;
- Pathology link for access to test results;
- Up to date, locally defined medicines formulary;
- Allocation of electronic devices to wards, including PC's on wheels, laptops and iPads to support mobile working.

Aspects that are not included for delivery within the first phase (but may be developed as a part of future phases of implementation) are:

- Scan4Safety (Barcode recognition of medicines)
- Medicines stock control
- Outpatient prescribing
- Paediatric prescribing
-

Future phases of development will become part of the lifecycle management of the system and the DPIA will be reviewed and updated accordingly.

Overview of the proposal: *What the project aims to achieve*

The EPMA implementation will result in a reduction of severe avoidable medication-related harm and facilitate wider improvements to clinical practice.

The current paper-based prescribing and administration system leads to:

- A high reliance on physical transportation, locating of the medicines charts and medication orders;
- Time wasted by medical, nursing, pharmacy staff chasing the paper trail and delayed medicines administration and discharges for patients;
- Disconnect between clinical professional groups;
- Transcription errors leading to errors and wastage;
- Illegible handwriting on prescriptions and charts.
- Potential lack of availability of records, due to lost or misplaced medicine charts which could lead to a clinical incident

The anticipated benefits of the project include:

Efficient and Safe

- A reduction in medication errors;
- Up to date and locally defined medicines formulary;
- Clinical decision support to help with prescribing and administration of medicines;
- A robust audit trail for the entire medicines process;
- Enabling achievement of future CQUIN or equivalent targets;
- Significant improvements to processes that impact on patient flow;
- Enabling better antimicrobial stewardship;
- More timely supply of medicines (including medicines for discharge);
- Releasing time to care;
- Eliminate the need to search for misplaced drug charts and rewriting drug charts.
- Availabity of information at the right time

Communicating and Working Together

- Legible prescriptions and discharge prescriptions;
- Digital entry and management of prescriptions;
- Electronic communication between wards/departments/pharmacy;
- Improvements in existing workflow and processes;

- Removal of paper prescription charts;
- Enhance communication with GPs and wider primary care, enabling a seamless transition to interoperability standards.

Aspiring and Improving

- The Trust remaining at the forefront of clinical technology use – currently EPMA remains the largest gap in comparison to peers.

Implementing Organisation:	Sherwood Forest Hospitals NHS Foundation Trust

Staff involved in PIA assessment (Include Email Address):	Elaine Torr, Divisional General Manager, Diagnostics & Rehabilitation elaine.torr@nhs.net Paresh Jogia, Lead EPMA Pharmacist paresh.jogia1@nhs.net Michelle Peet, Project & Business Change Manager michelle.peet@notts-his.nhs.uk Paul Ramsey, Nervecentre Project Manager pramsey@nervecentresoftware.com Jacquie Widdowson, IG Manager & DPO jacquie.widdowson@nhs.net

Key Stakeholders/Customers:	Sherwood Forest Hospitals NHS Foundation Trust Nervecentre Software Ltd

Project Sign Off

	Name	Job Title	Organisation	Date
Information Asset Owner	Morgan Thanigasalam	Clinical Lead for Digital Innovation and Transformation	Sherwood Forest Hospitals NHS Foundation Trust	**23rd October 2020**
Information Governance	Jacquie Widdowson	IG Manager & DPO	Sherwood Forest Hospitals NHS Foundation Trust	**9th October 2020**

Third-Party Representative *(someone aware of project and appropriate level of responsibility)*	Paul Volkaerts, pvolkaerts@nervecentresoftware.com	CEO	Nervecentre Centre Ltd	
SIRO Sign Off	Paul Robinson	Chief Financial Officer/ SIRO	Sherwood Forest Hospitals NHS Foundation Trust	**24th November 2020**
Caldicott Guardian Sign Off	Shirley Higginbotham	Director of Corporate Affairs	Sherwood Forest Hospitals NHS Foundation Trust	**25th November 2020**

Assessment Summary

To be completed by Information Governance / NHIS

Outcome of Privacy & Security Impact Assessment:	
1. Project/Implementation is recommended **NOT** to proceed, as significant corporate/customer risks have been identified.	☐
2. Project/Implementation to proceed once identified risks have been mitigated as agreed.	☒
3. Project/Implementation has met required legislative compliance and poses not significant risks. No further action required.	☐

Summary of Privacy & Security Impact Assessment; including legislative compliance and identified risks:

Summary:
The Nervecentre EPMA solution offers the best fit towards the wider digital strategy and Trust aims and objectives, aligning with the direction of travel within the Nottingham and Nottinghamshire ICS. The Trust is forming a development partnership with Nervecentre and University Hospitals of Leicester who have recently signed a ten-year contract with the supplier for their EPR/EPMA solution. Other ICS partners may sign up to the same solution which would further strengthen the development partnership.

Risks to NHIS/SFHT:
All risks are located in Stage - 4 Identified Risks and Mitigating Action

Recommendations for Action

Summary of Identified Recommendations? :		
Recommendations:	**Recommendation Owner:**	**Agreed Deadline for action:**
Lack of BCP can put the whole project at risk, therefore risk should be higher, project cannot proceed without it – MT comment, this risk has been updated in line with the project plan. The addition of EPMA strengthens the current BCP	IAO	31.10.20
DPIA to be revisted when new functionality is added, lifecycle management of project. Initially reviewed 6 months after go live. – MT comment, agree including review of risk log, action has been added to the project plan for August 2021	IAO	30.08.21

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 PIA will be undertaken on a case-by-case basis by NHIS / SFHT IG.

Q	Screening question	Y/N	Justification for response
1	Will the project involve the collection of information about individuals?	Y	Patient information will be collected e.g. allergy status, height & weight and medication history etc., which will aid the reduction of severe avoidable medication-related harm.
2	Will the project compel individuals to provide information about themselves?	Y	Individuals will provide information about themselves in the same way as the current paper-based method but this will be collated electronically on the EPMA system.
3	Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?	N	

Q	Screening question	Y/N	Justification for response
4	Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?	Y	Some patient information will be used differently to the current method, for example, to aid decision support. Data analytics will also help the Trust prioritise patient care.
5	Are there processes in place to ensure data is relevant, accurate and up-to-date?	Y	Although staff are already familiar with Nervecentre e-Obs, specific EPMA training will be undertaken.
6	Are there security arrangements in place while the information is held?	Y	An audit trail of alert overrides etc will be available.
7	Does the project involve using new technology to the organisation?	N	Clinicians are familiar with the types of technology that will support the deployment e.g. COW's, iPads, laptops.
8	Will the project result in you making decisions or taking action against individuals in ways which could have a significant impact on them?	N	
If you have answered "Yes" to any of the questions numbered 1-8 please proceed and complete stage 2.			
9	Is a Patient Safety Review required?	Y	The EPMA patient safety case is under review by the NHIS Patient Safety Team.
10	Is a Quality Impact/Technical Security Review required?	Y	Angela Hawley, NHIS Head of Technical Operations has been asked if a Quality Impact/Technical Security Review is required.

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

Stage 2 – Data Protection and Security Impact Assessment

2.1	What is the change					
	New purpose?	☒	Revised/changed?	☐	Other?	☐
	If Other please specify.		Nervecentre is currently used in the Trust for e-Obs and assessments. EPMA is another module of this system and will be used for recording medicines information and any related communications.			

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

	Sensitive Personal Data (special categories):	
	Children	TBC
	Vulnerable groups	TBC
	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	Please justify response **Yes or No**
	Y	Data will be used to prescribe, administer and supply medicines to patients.

2.3.1	How will you collect, use, store and delete data?
	Data will be collected from SFH systems (e.g. Medway), secure national NHS spine enabled systems and/or the data subject directly. The data will be stored on secure servers,and kept as per the existing Nervecentre data storage and in line with the DoH guidelines. NHIS host the virtual servers on a infrastructure which has a number of solutions in place to protect the servers and data such as high availability across two data centres. The EPMA system will be accessed by SFH staff using equipment purchased via NHIS.

2.3.2	What is the source of the data? (ie from data subject or other third party)
	Inpatient data is already stored on the Nervecentre system. For EPMA purposes data will be collected from patients, carers, GP's, nursing homes and primary care pharmacies. This will include inpatient information including diagnosis, follow-up actions and discharge prescriptions will be sent to GP's via MESH or FHIR. The patient will receive a paper discharge summary as is the current process. MESH (Message Exchange for Social Care and Health) is the main messaging service

	used across health and social care. It works on the Spine infrastructure. It's used to transfer electronic messages directly from one application to another, so different organisations can communicate securely. As an example, pathology labs use MESH to communicate test results to GP practices. MESH replaced the Data Transfer Service (DTS). FHIR (Fast Healthcare Interoperability Resources) is a standard describing data formats and elements (known as "resources") and an application programming interface (**API**) for exchanging electronic health records (EHR) FHIR builds on previous data format standards from HL7, like HL7 version 2.

2.3.3	How much data will you be collecting and using?
	Data specific to medicines management will be collected and entered onto the system including – allergies, current and previous medications, relevant medical history, patient height and weight, relevant pathology results from ICE In the future GP Connect will provide information in relation to current medications, relevant medical history etc. Allergies are already being recorded on Nervecentre eObs. Information will only be collected that is relevant to the patient's treatment plan during their inpatient episode.

2.3.4	How often? (for example monthly, weekly)
	Initially, it will be for inpatient admissions and later in the project may extend to Day case, Emergency Department and outpatient encounters.

2.3.5	How long will you keep it? https://www.sfh-tr.nhs.uk/media/1974/records-management-code-of-practice-health-and-social-care-2016.pdf
	Data will be kept in line with recommendations from The Records Management Code of Practice 2016.

2.3.6	Where will the data be stored? i.e. Medway, Shared Drive
	Data will be stored within the Nervecentre System on secure servers located in NHIS. Backup and maintenance plans are already in place.

2.3.7	How many individuals are affected?
	Once EPMA is rolled out across the Trust it will affect all inpatients and later in the project all patients in Day case, ED and outpatients.

2.3.8	What geographical area does it cover?
	Patients who geographically currently access Sherwood Forest Hospitals NHS Trust will not change.

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.*
	Data Controller	Sherwood Forest Hospitals NHS Trust
	Data Processor	Nervecentre Software Ltd

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** Supplier Assurance Framework V1.0.pdf Supplier Assurance Framework V1.0.xlsx
	Y	The Supplier Assurance Framework document received from Paul Ramsey on 23/06/2020. No issues identified by NHIS 8th July 2020 and Nervecentre are ISO 27001:2013

2.5.1	Please describe access and controls in place
	Access is linked to active directory which is given by (NHIS) and the user name and password for EPMa is managed by EPMA IAAs. Access and permissions will be monitored by the IAA's.

2.5.2	Please provide a copy of the contract in place
	ComIT 2 Nervecentre (Sherwc

2.5.3	Have arrangements for retention and destruction been included in the contract when the service/contract expires?	
	Yes, information is contained under section 24 in the contract between SFH and Nervecentre Software Ltd	
2.6	Will this information be shared outside the organisations listed above?	
	Y/N	if answered **Yes** please describe organisation/s and geographic location
	N	

2.7	Does the Work involve employing contractors external to the Organisation?	
	Y/N	If **Yes**, provide a copy of the confidentiality agreement or contract?
	N	Please see contract attached in 2.5.2

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	EPMA Workflow V3.0.pdf

2.9	What format is the data?					
	Electronic	☒	Paper	☒	Other (Please describe)	The discharge summary will be sent electronically to GP's with a paper copy printed for the patient and the medical notes until the Trust procures and deploys an EPR solution. This aligns with the current process used for Orion Discharge.

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	Yes, the system offers a full audit trail including access. This will be managed by the EPMA Team and management. It is not thought that Nervecentre will need to access this information.

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	ICE and potentially in the future JAC, Orion and GP Connect. GP Connect is a service that allows authorised clinical staff to share and view GP practice clinical information and data between IT systems quickly and efficiently. Currently used widely in GP Practices the service is gradually being extended for other services and the plan is to eventually feed it into EPMA. Nervecentre isn't currently linked to the national Spine. A Medway link is already in existence for the Nervecentre System. The MESH solution will initially be deployed for the discharge summary and is already FHIR compliant band will be deployed when the receiveing systems become compliant.

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?
	During a patient encounter, users will review the information and where appropriate update the information on the system. Accuracy of medicines information will be validated by the pharmacy team as part of the medicines reconciliation and discharge process. Data will be

	audited to address any incomplete information.

2.13	Who will have access to the information? (list individuals or staff groups)
	All staff groups who are involved in the patients' care will have access to the information including: Consultants Doctors Nurses Pharmacists Medicines Management Technicians AHP's HCA's Plus Data analysts

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)	☐

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	Discharge summaries will be sent to the GPs and relevant caring organisations which will describe the treatment that the patient has received as well as the medications that they need to take after discharge. This will be done using secure messaging processes e.g. MESH +/- FHIR
	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)	☒
	We intend to use MESH +/- FHIR or an approved NHS encryption methodology i.e. ICE communications			

2.17	Are disaster recovery and business contingency plans in place for the information?	
	Y/N	Please describe if answered **Yes.** Please state why not if response is **No.**
	Y	NHIS host the virtual servers on a infrastructure which has a number of solutions in place to protect the servers and data such as high availability across two data centres. All servers are backed up daily too. This is in development. It will be tested before pilot and there will be frequent validation procedure that will be put in place to ensure the contingency plan is functional at all times. The plan will include arrangments for the downtime of the system.

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	Staff training has been proposed and will be undertaken before access to the system is given. The training will include confidentiality and security, integrity

2.19	Will reports be produced?	
	Will reports contain personal/sensitive personal or business confidential information?	Only if required and these will mostly be for prioritising care to our patients and some confidential information may be needed to achieve this.
	Who will be able to run reports?	Data analyst and Trust approved staff members
	Who will receive the reports and will they be published?	Frontline users and management staff will have access to prioritise work

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	Refer to contract - Record Retention and Right of Audit.

2.21	Will explicit consent be obtained for processing of personal data?	
	Y/N	Please describe if answered **Yes**
	N	If **No**, list the reason for not gaining consent e.g. relying on an existing agreement, consent is implied, the project has s251 approval or other legal basis?
		Direct care

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.**
	N	No change to current practice, refer to privacy notice.

2.23	Is there a process in place to remove personal data if data subject refuses/removes consent	
	Y/N	Please describe if answered **Yes.** Please state why not if response is **No.**
	Y	The data cannot be removed from the front end however a support call can be raised to Nervecentre. The clinical safety officer will review the request and Nervecentre will have a process of removing the data from the database.

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	This is for direct care purposes. Patient data is currently used to optimise and prioritise care.

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's Data Protection and Confidentiality Policy and Procedure will be followed

2.26	Who are the Information Asset Owner(s) and Administrator(s)?	
	IAO	Morgan Thanigasalam
	IAA	Paresh Jogia Sarah Khu Khu

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.**
	Y	Response from Angela Hawley NHIS Head of Technical Operations - As EPMA is an extension of a current system I do not feel that a Technical Assessment is needed, should the requirements change, such as the future linkage to GP Connect, then this will need to be reviewed

2.28	Are there any current issues of public concern that you should factor in?	
	Y/N	Please describe if answered **Yes.**
	N	

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?
	Better patient care, improved workflow, reduced medication errors, enhanced governance processes, improved working for staff, live/warehouse data analytics to improve Trust reputation and efficiency.

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?
	Staff engagement session, Trust communications, utilise Business Change principals to engage with stakeholders. Trust executives, EPMA project board and senior clinical leads have already endorsed and are supporting the changes that EPMA will bring.

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).
	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). 6(1)(e) public interest or public duty

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)
	There will be no change to current practice.

2.33	What measures do you take to ensure processors comply?
	Policies and procedures already in place are up to date.

2.34	How will you prevent function creep?
	Limiting access to roles and auditing data on usage

Stage - 3 Work Flow Mapping

EPMA Workflow V3.0.pdf

{include a flow chart of info flows or table as required]
* if additional tasks are identified please add to the notes section and Corporate Governance will add on completion of form.
Please note: Have the information flows and assets that are identified within this DPIA been added to your departmental information flow map and asset register?

Stage - 4 Identified Risks and Mitigating Action

Risk:	Primary controls(s):	L	C	Current Risk Rating*	Gaps in control:	L	C	Acceptable Risk Rating*	Mitigating actions required
Time required to complete end to end prescribing processes increased to an unsustainable level due to poor quality implementation	It has been identified that an appropriately resourced and qualified implementation team will be required for pilot and roll-out	4	2	8	Sufficient training and go live implementation support is in the project plan.	3	2	6	Time in motion study to be undertaken to evaluate the impact of changing to EPMA. Team to support frontline staff ensuring the most efficient processes are utilised.
As the system is still in development it may not meet all the Trusts needs and requirements	Supplier to work in partnership with SFH clinicians in designing and developing functionalities. Regional partnership developments with UHL and possibly other Trusts.	3	3	9	No perfect system available. Work with clinicians and supplier to fix key issues	2	3	6	EPMA Team working with supplier and UHL to ensure that product is fit for purpose. UAT testing to be undertaken and gating/high ranked issues raised will be evaluated by the Patient Safety Group (PSG) to prioritise delivery of functional requirements for pilot and live system

Poor adoption through insufficient training due to not being able to recruit clinical resource and competing priorities.	A recruitment strategy is in place	2	3	6	No significant gaps in control	2	3	6	EPMA team have already approached key stakeholders who have agreed to release staff recruited internally for rollout. DSG are supportive of the project implementation requirements including recruitment
Clinical safety risk from introducing new digital solution	Mandatory supplier compliance with DCB0129. Trust compliance with DCB0160. Extensive Testing. Clinical Safety Officer sign off assurance.	2	3	6	Unintended consequence of digitisation	1	3	3	PSG to review issues and ensure the system is safe for deployment. Where risks are gating the supplier will be contractually required to fix. If not addressed the system deployment will be postponed
Implementation delay leading to national funding recall, further investment required or benefits realisation delay	Robust implementation plan with realistic timelines	2	4	8	No significant gaps in control	1	4	4	EPMA team to reach out NHSD/X and establish revised deadlines given COVID pandemic and implications of a possible delayed rollout.
Clinical safety risk - Migration of the current mixed system of paper-based and electronic systems	Suitably planned roll-out order. Team of sufficient size to roll-out at pace. Cover to support clinically during rollout.	3	3	9	Manage risks of switch as part of rollout	2	3	6	Standard Operating Procedures and training materials will be provided to clarify where and how a mixed economy of paper and electronic system should be used
Business Continuity Plan (BCP)	Nervecentre system already has a BCP for live use. This is being reviewed as part of the EPMA implementation and will be ratified through BCP approval proess. The plan will include arrangements for the downtime of the system. EPMA will be included in the database backup and maintenance plans for Nervecentre	2	2	4	No significant gaps in control. Gap in control is no BCP in place. Cannot go live without this.	1	2	2	Revert to paper-based prescriptions in event of complete failure
Nervecentre Software have not submitted 2019/20 Data	Submission deadlines have been extended to 30 September 2020. A	2	1	2	Not applicable	1	1	1	Nervecentre Software have submitted a ‘standards met’ Data Security and

Security and Protection Toolkit assessment	'standards met' assessment was submitted in 2018/19. Nervecentre Software are registered as a data controller with the ICO. Registration number ZA081284								Protection Toolkit assessment 22nd September 2020

* SFHT Risk Assessment Matrix to be used
** if additional risks are identified please add to the notes section, Governance will add on completion of form.

Stage – 5 Legal Compliance

Compliance to be determined by NHIS/SFHT IG 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.

Notes:

Click here to enter text.