Maidstone and Tunbridge Wells NHS Trust

Ref: FOI/GS/ID 5831

Please reply to:
FOI Administrator
Trust Management
Maidstone Hospital
Hermitage Lane
Maidstone, Kent
ME16 9QQ
Email: mtw-tr.foiadmin@nhs.net

12 March 2020

Freedom of Information Act 2000

Thank you for your request for review of the Trust handling of your FOI request reference FOI/GS/ID 5831 and the information disclosed.

The questions on your original request are as follows:
Please provide copies of any DPIA conducted for your Sunrise EPR implementation

Having carried out a review of your request the Trust is able to supply the information detailed below/attached. Please note this is a draft document.

Maidstone and Tunbridge Wells NHS Trust

Data Protection Impact Assessment

Document Owner	Version	Status	Approved by	Issue Date
Simon Parker	0.1	Draft		

Maidstone and Tunbridge Wells NHS Trust

Document management

Revision History

Version	Date	Summary of Changes
1.0	May 2018	First Iteration

Maidstone and Tunbridge Wells NHS Trust

Data Protection Impact Assessment (DPIA) screening questions

The following questions must be answered fully to determine the need for a DPIA .

Project Name
Sunrise EPR Programme
Project Sponsor
Peter Maskell – Medical Director
Project Manager
Simon Parker
Will the project involve the collection of new information about individuals?
No
Will the project compel individuals to provide information about themselves?
No
Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?
No
Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?
No
Does the project involve you using new technology which might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition.
No
Will the project result in you making decisions or taking action against individuals in ways which can have a significant impact on them?
No
Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records or other information that people would consider to be particularly private.
Yes
Will the project require you to contact individuals in ways which they may find intrusive?
No

If answering 'Yes' to any of the questions it is likely a PIA is required.

Maidstone and Tunbridge Wells NHS Trust

Data Protection Impact Assessment

Step 1: Identify the need for a DPIA

Explain broadly what the project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.

The Sunrise EPR Programme aims to replace the collection of Patient Clinical Information on paper with the collection of Patient Clinical Information on an EPR (Electronic Patient Record) computer system. This will allow Clinical Practitioners to see the up to date Patient Record in near real time which will improve the flow of patients through the hospital and facilitate improved patient care.

Implementation of the Sunrise EPR is recognised as being a transformational change to the way that we will work with our patients and with each other. The EPR is an electronic version of each patient's medical history that is maintained and updated for every interaction and attendance. It will include their demographics, clinical notes, activity, medication, vital signs, past medical history, diagnostic reports and scheduling. In addition the system will provide the user with decision support tools to help our clinicians in their decision making i.e. prescribing and pathway management.

DPIA is required to ensure that the Trust identifies the privacy risks associated with the processing of personal data and for implementing appropriate controls to manage those risks before the EPR system goes live.

Step 2: Describe the information flows

Describe the nature of the processing: How will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or another way of describing data flows. What types of processing identified as likely high risk are involved?

The data will be collected and stored in Allscripts Sunrise as appropriate by Trust Staff who have authority to do so following current approved processes already in place. This will include recording information provided by patients and or their carers which was previously recorded in their paper notes.

Patient PMI data and appointment related information will be sent via an interface through a TIE from Allscripts PAS through to Sunrise EPR via NHS virtual private network. In addition information will be sent through the TIE to and from Telepath system (to facilitate the ordering and receipt of pathology tests). In

addition a number of systems are tab integrated within Sunrise to aid clinicians to access radiology images and electronic notes (including those scanned) in context and so speed up access to information important to delivery of patient care. This will reduce delays previously seen with paper records as information will be easily accessible when required.

The patient identifiable information linked to the hospital number, is fully encrypted, is retained within a secure server that is dedicated to Allscripts Sunrise EPR. This complies with all required standards and no data with EPR is stored in any other server.

Information stored within Sunrise will be able to accessed by health care professionals who have been involved in a patients care according to their secure password role based access authorisation level . This will include employees of organisations outside of the Trust who have undergone specific checks before being granted access to Sunrise

Describe the scope of the processing: What is the nature of the data and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?

The data collected by Trust staff will include clinical information provided by patients and or their carers which was previously recorded in their paper notes which has been added into the EPR. This will be collected for every attendance or interaction staff members have with patients. For documents or functionality which has not been enabled within the EPR the information collected will remain in paper records.

Electronic records will be retained for a minimum of 8 years or longer as per the Trust retention policies. This period is measured from last activity. Some exceptions may be applied to retention by the Data Controller where the Records Management Code of Practice Health and Social Care 2016 stipulates a different retention schedule based on data type.

Geographical area covered is Maidstone and Tunbridge Wells NHS Hospital NHS Trust catchment area circa 500,000 patients. The system will only be available within the two main sites - Maidstone Hospital and Tunbridge Wells Hospital. It will not be used for any of the services that are held in satellite clinics. It also excludes Maternity and neonate services.

Describe the contact of the processing: What is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?

The data will be collected and stored in Allscripts Sunrise as appropriate by Trust Staff who have

responsibility to deliver patient care following current approved processes already in place. This will include recording information provided by patients and or their carers which was previously recorded in their paper notes. This will include children and vulnerable groups.

Patients expect clinical teams to be recording information about them as this was previously recorded on paper. Increasingly within the NHS electronic patient records are becoming more routine especially in primary care and this is not novel. The Trust is deploying new computers and workstations on wheels to support the deployment of the EPR system. This includes new servers and network capability.

Describe the purposes of the processing: What do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing for you, and more broadly?

The aim of the EPR is to help us to treat our patients more effectively by giving each staff member easier access to a single version of up-to-date information. It will also use this information to improve care through the use of decision support tools and in giving staff the functionality and data needed to be safer and more efficient through greater awareness of that patient as a result of the information available to them.

Some of the benefits to both MTW staff and our patients include:

- Releasing time to care
- Rapid access to information needed to manage patient's care
- Simplified processes reducing time wasted on data entry
- Improved clinical outcomes and patient safety
- Access to information across clinical systems – Sunrise EPR will be a portal for other systems reducing the number of separate systems needed to be accessed by clinical teams
- Reducing reliance on paper to become a paper-lite organisation
- Enhanced data collection to inform research and audit

Step 3: Consultation requirements

Consider how to consult with relevant stakeholders: Describe when and how you will seek individual's views – or justify why it is not appropriate to do so. Who else do you need to involve within the Trust? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?

Stakeholders include clinicians within Maidstone and Tunbridge Wells NHS Trust and the electronic patient record supplier Allscripts. At all points of the design subject matter experts from all the relevant departments within the Trust will be consulted on what information needs to be collected and the design in how the documentation in the electronic system should work based on existing paper practices. In addition the legal department, health records committee and information governance teams will be involved in approving design before the system goes

live.

The Trust IT department have taken the lead on procurement and quality assurance on all aspects of the project and related assets (hardware and software).

Step 4: Assess necessity and proportionality

Describe compliance and proportionality measures, in particular: What is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?

Clinical records are required to be captured to ensure patients receive the correct care for their medical conditions in a timely manner. By 2024 all NHS providers are required to move from paper records to collecting clinical information electronically. Alternative systems such as scanning handwritten clinical notes or integrating a number of existing systems can be deployed to create a single electronic record.

The EPR programme being implemented within the Trust is split into three distinct phases and is being governed to ensure functionality adheres to the agreed contract with the system provider. At each stage of the design clinical teams will be consulted in the information to be collected before being involved in testing to ensure data quality and ease of use.

As the electronic record is implemented within the Trust, staff will explain why the system is being used and how this will form their clinical record. They will be informed that the information collected will be linked to their hospital number. An information leaflet will be produced to explain the process and why the information is being recorded electronically and what will happen to data collected. In addition posters and flyers will be put around the Trust to ensure all patients are aware during every visit.

The Trust has a policy in place which allows their patient to request copies of records that are stored on their patient record. Records contained within the EPR system would also be able to be printed off and provided to the patient under the existing policy for access to patient records

Maidstone and Tunbridge Wells NHS Trust

Step 5: Identify and assess risks

Describe the source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.

Risk	Likelihood of harm	Severity of harm	Overall risk
	Remote, possible or probable	Minimal, significant or severe	Low, medium or high
1) Cyber attack on Allscripts EPR could mean system is unavailable for clinical staff to access patient clinical records			
2) Staff accessing records inappropriately			
3) Risk that data is breached by unauthorised access through loss, theft or malicious intent on mobile devices e.g. computer on wheels			
Add additional rows as required.			

Step 6: Identify measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5.

Risk	Options to reduce or eliminate risk	Effect on risk	Residual risk	Measure approved
		Eliminated, reduced or accepted	Low, medium or high	Yes/no
2)	Role based security access set up			
Add additional rows as required.				

Step 7: Sign off and record outcomes

	Name/date	Notes
Measures approved by:		Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:		If accepting any residual high risk, consult the ICO before going ahead.
DPO advice provided:		DPO should advise on compliance, step 6 measures and whether processing can proceed.
Summary of DPO advice:		
DPO advice accepted or overruled by:		If overruled, you must explain your reasons.
Comments:		
Consultation responses reviewed by:		If your decision departs from individual's views, you must explain your reasons.
Comments:		
This DPIA will be kept under review by:		The DPO should also review ongoing compliance with the DPIA.

Contact points for future privacy concerns

Maidstone and Tunbridge Wells NHS Trust

Step 8: Integrate the DPIA outcomes back into the project plan

- Who is responsible for integrating the DPIA outcomes back into the project plan and updating any project management paperwork? Who is responsible for implementing the solutions that have been approved? Who is the contact for any privacy concerns which may arise in the future?

Action to be taken	Date for completion of actions	Responsibility for action

Annex A – Data flow diagram