Data Protection Impact Assessment (DPIA)

1. Project/activity details

Project title			
Oxfordshire Care Summary platform upgrade to Cerner Health Information Exchange (HIE)			
Project sponsor	[redacted]	**Lead organisation**	Oxfordshire CCG
Project lead	[redacted] Manager)	**Division (OUH)**	Corporate
Telephone		**Directorate**	GDE Programme
Email	[redacted]	**Proposed start date**	Dec 2019 (Phase 1)
Will you be using personal data?[1]	Yes ☒ No ☐	If no personal data will be collected or processed, the DPIA is complete.	

2. Project purpose

What is the purpose of the proposed project, and why is it necessary?
The Oxfordshire Care Summary (OCS) is a single electronic view of specific, up-to-date, clinical information from general practice and Oxford University Hospitals Foundation Trust (OUH) records used to support patient care in NHS organisations in Oxfordshire. HIE is a Cerner-provided replacement for the OCS. HIE will access data from several sources including primary care, OUH, and mental health services (Oxford Health) (phase 2). This project is the first step towards a local integrated health record (The Oxfordshire Care Record) which will be based around the Cerner Millennium platform. Users will access HIE either directly through their usual clinical systems (e.g. Millennium EPR at OUH, EMIS for general practice), or directly via a web portal via a secure N3/HSCN network connection. HIE is a 'read only' source of health records. It does not provide facilities to alter the content of the source patient records. Updates, amendments and overlays depend on changes being recorded on the originating system, and those changes being made available to the HIE. HIE records originating from multiple systems are linked using the unique patient identifiers assigned by the system that originated the record. The NHS number and the OUH medical record number will be used to match records in conjunction with key demographic elements, following NHS Digital recommendations. HIE implementation will be phased, ultimately providing access to users across Oxfordshire. Phase 1 will provide access for OUH, primary care, and a small number of OH users and is expected to complete by March 2020. The DPIA will be reviewed again for phase 2 of the project. HIE is a necessary step towards the provision of a secure integrated record across the health economy.

[1] Personal data means any information relating to an identified or identifiable natural person ('data subject'). An identifiable natural person is a living person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

3. Data requirements

What personal data is required? – *Provide details of each data field used, and justification for each, e.g. name, DoB, MRN, email address etc. For large numbers of data fields, please summarise here and provide full details on a separate sheet.*

Data fields	Justification
OUHT: ADTs, lab results and clinical information Primary care demographics, encounters and clinical information **EMIS:**	To support the continuity of direct care between care providers

Summarise the proposed system/use of data—*How will the data be used?*

The data will be used for direct patient care. Providing the clinician with data from multiple sources will enhance care and save time.

Is the proposed system/data use reliant on an existing system/data use? – *e.g. adding new data fields to an existing survey collecting patient data.*

HIE replaces the existing Oxfordshire Care Summary (OCS) and uses essentially the same data but handled in a different way. Primary care data from EMIS will continue to be accessible via the Medical Interoperability Gateway (MIG), supplied by Healthcare Gateway Ltd .(HGL). Data from OUH will be made available from Cerner Millennium and the Trust integration engine.

Whose data will be processed? –*Staff, patients, members of the public etc;*

Staff	☐	*If other please state :*
Patients	☒	
Members of the public	☐	
Other	☐	

How many individuals' data will be involved?

1-50	☐	500-1000	☐
50-100	☐	1000-5000	☐
100-300	☐	5000-10,000	☐
300-500	☐	10,000+	☒

From where will data be obtained, and how?

Data will be collected from primary care and OUH systems.

Will any of the data be shared with a third party? **Yes** ☒ **No** ☐ *(If Yes, please give details below.[2])*

Data will be shared between OUH and GP Practices, to be available to clinical staff providing care, and non-clinical staff supporting the provision of direct care services.

[2] A Data sharing agreement must be in place before data is shared with other organisations. Contact Information Governance for details.

4. Compliance with Caldicott principles[3]

No.	Principle	How will the project comply?
1	**Justify the purpose(s)** Every proposed use or transfer of personal confidential data within or from an organisation should be clearly defined, scrutinised and documented, with continuing uses regularly reviewed, by an appropriate guardian.	The purpose of sharing the data is for medical care
2	**Don't use personal confidential data unless it is absolutely necessary** Personal confidential data items should not be included unless it is essential for the specified purpose(s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose(s).	Patients must be identified for safe delivery of care
3	**Use the minimum necessary personal confidential data** Where use of personal confidential data is considered to be essential, the inclusion of each individual item of data should be considered and justified so that the minimum amount of personal confidential data is transferred or accessible as is necessary for a given function to be carried out.	The data involved is routinely required and necessary for safe and effective care.
4	**Access to personal confidential data should be on a strict need-to-know basis** Only those individuals who need access to personal confidential data should have access to it, and they should only have access to the data items that they need to see. This may mean introducing access controls or splitting data flows where one data flow is used for several purposes.	Use of the system is restricted to those using its source systems, which in turn have access controls. Every access is recorded and audits will be undertaken.
5	**Everyone with access to personal confidential data should be aware of their responsibilities** Action should be taken to ensure that those handling personal confidential data — both clinical and non-clinical staff — are made fully aware of their responsibilities and obligations to respect patient confidentiality.	All users will be up-to-date with their organisation's IG training, as agreed in the Oxfordshire Information Sharing Framework (2018) Data Sharing Agreement
6	**Comply with the law** Every use of personal confidential data must be lawful. Someone in each organisation handling personal confidential data should be responsible for ensuring that the organisation complies with legal requirements.	All organisations will have signed up to the Data Sharing Agreement.

[3] The Caldicott Principles originate from the *Report on the Review of Patient-Identifiable Data (1997)* by a committee chaired by Dame Fiona Caldicott for the Department of Health. They have been widely accepted and adopted as the foundation for the safe and confidential handling of patient data. A second report, I*nformation: To share or not to share? The Information Governance Review (2013)*, introduced a seventh principle regarding the duty to share.

No.	Principle	How will the project comply?
7	**The duty to share information can be as important as the duty to protect patient confidentiality** Health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by these principles.	This project supports the seventh principle

5. Legal basis

Every use of personal data must be lawful and must comply with the Data Protection Act (2018)/GDPR and satisfy the common law duty of confidentiality.

Data Protection Act (2018)/GDPR
Select a legal basis from *GDPR Article 6*. For patient data, select also a legal basis from *GDPR Article 9*.

GDPR Article 6		GDPR Article 9	
1(a) Consent	☐	2(a) Explicit consent	☐
1(a) Necessary for the performance of a contract to which the data subject is or about to be party	☐	2(b) Necessary in connection with employment	☐
1(c) Necessary for compliance with legal obligation	☐	2(c) Necessary to protect the vital interests of the data subject	☐
1(d) Necessary to protect the vital interests of the data subject	☐	2(d) Legitimate interest	☐
1(e) Necessary for performance of a task carried out in public interest or in exercise of official authority	☒	2(e) The data subject has manifestly made the information public	☐
1(f) Legitimate interest (does not apply for public authorities)	☐	2(f) Necessary for establishment, exercise or defence of legal claims	☐
		2(g) Necessary for reasons of substantial public interest	☐
		2(h) Necessary for provision of health and/or social care, including preventative or occupational medicine	☒
		2(i) Necessary for reasons of public interest in the area of public health	☐
		2(j) Necessary for archiving purposes in the public interest, scientific or historical research purposes.	☐
		2(j) Necessary for archiving purposes in public interest, scientific or historical research purposes.	☐

How will the common law duty of confidentiality be satisfied?[4]

Consent	☒	Legal obligation	☐
Public interest	☐	Section 251 approval	☐

[4] The common law duty of confidentiality is separate from and in addition to data protection legislation (DPA, GDPR). It requires that information given in confidence must not be shared with a third party without the individuals' valid consent or some other legal basis such as overriding public interest, statutory basis or court order. Where obtaining consent is impracticable, the Confidentiality Advisory Group of the Health Research Authority may set aside this requirement under Section 251 of the Health and Social Care Act. Under common law, consent may be implied by virtue of the patient freely giving the information with the reasonable expectations that privacy is respected but the information will be shared with other staff providing their direct (personal) care. If in doubt, please discuss with the Caldicott Guardian.

Please explain reasons for the above choice:

There is reasonable expectation that this information will be shared with others delivering care to the patients and care; this is supported by the publication of information in Privacy Notices by each organisation. Consent is thereby implied.

6. Data storage

Where will the information be stored? *Where information is being stored outside the Trust you will need to provide assurance documents for review (see below).*

Within OUH	☐	Within EEA	☐
Within the UK	☒	Within EEA – cloud based service	☐
Within the UK – cloud based	☐	Outside EEA	☐
Within the UK – cloud based within N3 network	☐	Outside EEA – cloud based service	☐

How information will be stored? *(describe physical and cyber security arrangements as relevant)*

Primary Care – EMIS via MIG

A subset of the data collected on the GP EMIS system is 'retrieved on demand' via the Medical Interoperability Gateway (MIG); no EMIS data is stored within the HIE.

However the Cerner audit tool screen captures the landing page of the record being visited by the clinicians which contains PID data of the patient. This screen shot is then stored on the HIE server, but is only available to authorized staff for audit purposes.

Acute – Cerner Millennium

A subset of the data collected on the OUH Cerner Millennium EPR is propagated via HL7 messaging to HIE where it stored within a secured database.

Cerner has confirmed that the server sits within its UK Data Centre.

7. External data transfer

Will data be transferred outside OUH?

No	☐	Yes – outside UK, within EEA	☐
Yes – Within the UK	☒	Yes – outside EEA	☐

What is the proposed method for secure data transfer?

The current OCS runs on servers maintained by OUH. It aggregates and presents patient data from GP and hospital systems in real time when requested by clinicians using the system. GP clinical records are held in a secure data centre owned by the GP system supplier (EMIS). The Medical Operability Gateway (MIG), owned by Healthcare Gateway Ltd, is able to access EMIS data.

When a clinician requests access to a patient's clinical information, OCS interrogates MIG for evidence of a Read code refusing consent to share. If this is found, OCS looks no further, and returns a result indicating that the patient has declined to participate in OCS. Otherwise it returns the data sets described above. OCS will then interrogate other clinical systems for agreed data sets. The information will be displayed on OCS screen, with the source clearly identified. No data is retained within OCS.

HIE will assemble the aggregated information on request in the same way, via Cerner's servers.

All data transfers are via secure, encrypted links.

8. Data accuracy and retention

Who will be responsible for data accuracy? *Job role, organisation.*	**How will accuracy of the data be assured?** *What processes are in place to assure good data quality?*
This project does not use or generate new data. It draws on existing sources. The responsibility for data accuracy and quality rests with the information asset owner and owning organisation.	N/A
Who will retain and hold this data? *Job role, organisation.*	**How long will the data be retained for?** *This should align with the Trust's retention schedule.*
Cerner UK will on demand access and temporarily store data from originating sources and display to the requesting user.	For the duration of the user interaction. A snapshot of the data accessed will be retained separately and securely for audit purposes.
Who will be responsible for secure disposal of data? *Job role, organisation.*	**How will data be disposed securely?** *What method(s) will be used to destroy the data securely?*
Cerner UK	Cerner adheres to the NIST Special Publication 800-88 Guidelines for Media Sanitization. Supporting documentation includes a media destruction log, electronic medial disposal process workflow, electronic media disposal process work instruction and supplier certificate of destruction. Cerner can provide a Certificate of Destruction for drives with specific serial numbers, in accordance with any industry requirements and best practices. Cerner will work with the customer to ensure media is separated when it is destroyed so tracking can be completed accordingly.

9. Transparency

The Trust has a duty to inform individuals how their data is being processed. In assessing new uses of data, it is often helpful to consult with groups of individuals whose data may be involved, to identify any concerns or risks with the proposed use of data.

Who will you be consulting with?			
Patients	☐	Staff	☐
The public	☐	No-one	☒

How were individuals consulted? *e.g. meetings, surveys, focus groups, patient panels, professionals.*

N/A

If consultation has not taken place and is not planned, please explain why

This is not a new use of data - HIE draws on existing data routinely used for patient care in different settings making it available to all in those settings who are involved in the delivery of that care.

A public consultation was carried out ahead of the original Oxfordshire Care Summary project. Current OCS patients' wishes 'not to share' will continue to be respected. However new patients registering at a practice will not be able to opt-out, as their data is being used for their direct care under provisions in the Data Protection Act (2018).

What concerns have been raised? *e.g. invasion of privacy, risks etc;*
N/A

10. Data subjects' rights and opt-outs

How will data subjects be informed about the processing?	
Privacy notices and professional conversations.	
Will data subjects be able to opt-out of the data use at any time?	**Yes** ☐ **No** ☒

11. Risk assessment

The level of risk is scored out of 25. A score of 0-5 is attributed to both the impact on the rights and freedoms of the individual, and the likelihood of those rights and freedoms being compromised. The two scores are then multiplied to create the composite risk score using the risk matrix below.

Risk	**Description**	**Risk score** see matrix below			**Proposed solutions/actions**	**Result** risk accepted, eliminated, or reduced?
		Impact	**Likelihood**	**Risk Rating**		
1	**See attached HIE Hazard Log**					

12. Approval

	Name	**Date**
IG review completed by:	[redacted]	4th October, 2019
Next review due (normally annually)**:**		4th October, 2020