Data Protection Impact Assessment (DPIA)

This Data Protection Impact assessment (DPIA) template is designed to help ensure 'privacy by design', to identify the most effective way to comply with data protection law, and to protect the rights and freedoms of individuals, be they patients, staff or members of the public. This should assist in identifying the risks of processing and sharing personal data, and in creating solutions to reduce them.

Once complete, or if you have any questions, please contact the Information Governance Team: information.governance@ouh.nhs.uk.

1. Project/activity details

Project title			
Oxfordshire Care Summary platform upgrade to Cerner Health Information Exchange (HIE)			
Project sponsors	David Walliker/ Gareth Kenworthy (Population Health Programme SROs)	**Lead organisation**	Oxford University Hospitals NHS Foundation Trust and Oxfordshire CCG
Project lead	Stephen Hill	**Division**	Corporate
Telephone	07748 180 242	**Directorate**	Digital
Email	stephen.hill13@nhs.net	**Proposed start date**	April 2020
Will you be using personal data?[1]	Yes ☒ / No ☐	If no personal data will be collected or processed, the DPIA is complete.	

[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.

2. Project purpose and description

What is the purpose of the proposed project, why is it necessary, and how will it be achieved?
The Oxfordshire Care Summary (OCS) is a single electronic view of specific, up-to-date, clinical information from general practice and Oxford University Hospitals NHS Foundation Trust records used to support patient care in NHS organisations in Oxfordshire. Health Information Exchange (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 Oxford Health NHS Foundation Trust users from April 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.

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. Add additional rows as necessary, or for large numbers of data fields, please summarise here and provide full details on a separate sheet.*

Data field	**Justification**
OUH/OH: Patient demographics, admission, discharge transfer details. Reports of investigations, clinical correspondence and other necessary clinical information.	To support the continuity of direct care between care providers
EMIS: demographics, encounters and clinical information	

Summarise the proposed system/use of data—*How will the data be used?*
For phase 1 data will only used for direct (individual) patient care. Providing clinicians with data from multiple sources will enhance care, save time and ensures compliance with the duty to share (Caldicott Principle 7).

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.* **Yes** ☐ **No** ☐ *(If Yes, please give details below.[2])* .

HIE replaces the existing mechanism underpinning the 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 OUH 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.[3])*

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. The HIE platform is supplied by Cerner UK, acting as a data processor on behalf of OUH

Has the third party ever received any decisions against it from a supervisory body regarding data breaches? **Yes** ☐ **No** ☒ *(If Yes, please provide details below)*

4. Compliance with Caldicott principles[4]

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 to support and enhance direct (individual) patient care.

2 A data sharing or data processing agreement must be approved by Information Governance and in place before data is passed to other organisations. Contact Information Governance for details.

3 A data sharing or data processing agreement must be approved by Information Governance and in place before data is passed to other organisations. Contact Information Governance for details.

4 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?
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 correctly 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 in routine use. Making it available to other care providers is 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 HIE will be restricted to those using its source systems, which in turn have access controls. Every access is recorded andcan be audited.
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.	The legal basis for sharing is described in section 5 below.
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 users are required to be up to date with the basic national data security and protection annual training.
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.	Fully supported.

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. Please note that collection, storage, anonymisation and sharing are separate processes, each of which requires a legal basis. Use this section to record the legal basis for acquiring any personal data. If a different legal basis is appropriate for storage, anonymisation or sharing, this should be described in the relevant sections (6 & 7).

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

GDPR Article 6		**GDPR Article 9**	
1(a) Consent	☐	2(a) Explicit consent	☐
1(b) 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.	☐

How will the common law duty of confidentiality be satisfied?[5]

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

Please explain reasons for the above choice:

There is reasonable expectation that this information will be shared with others delivering care to patients; this will be supported by the publication of information in privacy notices by each organisation.

[5] 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 (requires a formal public interest test), 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 National Health Service Act 2006 and its current Regulations, the Health Service (Control of Patient Information) Regulations 2002. 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.

6. Data storage and system security

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 the HSCN network[6]	☒	Outside EEA – cloud-based service	☐

How information will be stored? *(Describe physical and cyber security arrangements, including)*

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

Acute – Cerner Millennium

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

Who is the Information Asset Owner?[7] *(Give name and job titles and details of relevant training)*

David Walliker Chief Digital and Partnership Officer (CDPO) OUH

Who is the Information Asset Manager?[7] *(Give name and job titles and details of relevant training)*

Larry Murphy Interim Head of Digital (OUH)

Who will have access to the data? *(Give names and job titles and details of relevant training)*

Available to all users of HIE. Users are expected to have completed mandatory data security and protection training.

Will any of the data be accessible from outside the Trust's network? Yes ☒ No ☐ *(If Yes, please give full details below, including security arrangements)*

Data transmission is encrypted, and access controlled via source system login. Cerner UK offers HIE as a Software as a Service (SaaS) within its UK-based private cloud.

Do you have a disaster recovery/business continuity plan? Yes ☒ No ☐ *(If Yes, please supply separately. If No, please explain below why not and/or discuss with Information Governance to determine whether one is required.)*

The Cerner UK Business Continuity Plan has been reviewed and is on file.

[6] The Health and Social Care Network (HSCN) replaces the NHS N3 network

[7] See the Trust's Information Governance Framework for details of information asset owners and managers.

7. External data transfer

Will data be transferred outside OUH?			
No	☐	Yes – outside UK, within the EEA	☐
Yes – Within the UK	☒	Yes – outside the EEA	☐
To whom and where will the data be transferred? *(Please give details. If outside the EEA, please also give the country.)*			
HIE provides users with access to data from existing systems: it is not a storage repository.			
What is the proposed method for secure data transfer? *(Give full details including encryption method used, and whether the data will be anonymised or pseudonymised.)*			
All data transfers are via secure, TLS-encrypted links.			
What is the specific legal basis for transferring data to a third party/outside OUH? *This may be the same legal basis as Section 5 above, but could be different* As above (Section 5)			

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?*
HIE 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.*	**For how long will the data be retained?** *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 of securely?** *What method(s) will be used to destroy the data securely?*
Cerner UK	

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: the 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.

What concerns have been raised and how are these being addressed? *(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, and what information has or will be provided?

Privacy notices and professional conversations.

Will data subjects be able to opt-out of the data use at any time? **Yes** ☒ **No** ☐

Please note that the National Data Opt out applies to any use/processing of data other than direct/individual care. From March 2020 you must not use data from any patient that has opted out unless it is for their direct care.

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. This should be recalculated in the final columns to take into account proposed solutions/actions.

Risk	Description	Risk score see matrix below			Proposed solutions/actions	Revised Risk score see matrix below		
		Impact	Likelihood	Risk Rating		Impact	Likelihood	Risk Rating
1	System vulnerable to external attack	5	3	15	Cerner UK has Cyber Essentials + accreditation	5	1	5
2	Users may access records of patients with whom they do not have a legitimate access	3	3	9	Users must have had data security and protection training	3	2	6
3	Patients' expressed wishes regarding confidentiality not observed	3	3	9	Opt-out codes and privacy settings in EMIS. However suppression of individual data items is not currently possible.	6	2	6

Risk matrix

	Impact (How bad it may be)		Likelihood (The chance it may occur)			Risk Rating				
						1	2	3	4	5
5	Catastrophic	**5**	Almost certain	CONSEQUENCE	**5**	**5**	**10**	**15**	**20**	**25**
4	Major	**4**	Likely		**4**	**4**	**8**	**12**	**16**	**20**
3	Moderate	**3**	Possible		**3**	**3**	**6**	**9**	**12**	**15**
2	Minor	**2**	Unlikely		**2**	**2**	**4**	**6**	**8**	**10**
1	Negligible	**1**	Rare		**1**	**1**	**2**	**3**	**4**	**5**

Likelihood (L) x Impact (I) = TOTAL RISK RATING

Total Risk Rating	Risk
1-3	Low
4-6	Moderate
8-12	High
15-25	Extreme

12. Review

	Name	Date
IG review completed by:	Dr Christopher Bunch: Data Protection Officer for Oxford University Hospitals NHS Foundation Trust	6th April, 2020
Next review due (normally annually)**:**		30th September 2020

A DPIA is a dynamic process and the form should be updated if any circumstances change, and reviewed at least annually.

DPIA Form version 3.8 11th November, 2019