Data Protection Impact Assessment (DPIA)

This Data Protection Impact assessment (DPIA) is a template designed for the QOMS Restorative Dentistry / oral rehabilitation for Head and Neck cancer patients (RD) registry. It should help in completing a hospital's / Trust's or Health Board's own DPIAs required for that project. If you have any questions or problems, contact the project manager.

Project/activity details

Project title	QOMS Restorative Dentistry / oral rehabilitation for Head and Neck cancer patients (RD) registry
Project sponsor	The British Association of Oral and Maxillofacial Surgery (BAOMS)
Lead organisations	The British Association of Oral and Maxillofacial Surgery (BAOMS) and The British Orthodontic Society (BOS)
Clinical lead (central)	Michael WS Ho MD FRCS(OMFS) FEBOMFS DOHNS
Contact details	Consultant Maxillofacial Oncology | Leeds Teaching Hospitals NHS Trust | Leeds Dental Institute | Worsley Building | Clarendon Way | Leeds | LS2 9LU
Email	michael.ho2@nhs.net
Project manager (central)	Fabien Puglia, PhD
Contact details	RCSEng, 38/43 Lincoln's Inn Fields, London WC2A 3PE
Email	baomsprojectmanager@baoms.org.uk
In your hospital / Trust / Health Board	
Project lead	
Telephone	
Email	
Division	
Directorate	
Proposed start date	
Will you be using personal data?[1]	Yes

[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

Project purpose and description

What is the purpose of the proposed project, why is it necessary, and how will it be achieved?

In 2018, the British Association of Oral and Maxillofacial Surgeons (BAOMS) initiated a specialty-wide quality improvement and clinical effectiveness programme, called the Quality and Outcomes in Oral and Maxillofacial Surgery (QOMS) project. The project aims to (1) measure quality of care provided by oral and maxillofacial surgery departments, (2) identify unwarranted variation, and (3) improve quality of care provided to patients. This programme of work stretches across several OMFS subspecialties, including oncology.

Oral cancer is the 15th most common cancer in the UK, accounting for around 2% of all new cases. Disease and treatment (surgery, chemotherapy and radiotherapy) can lead to various oral complications, including oral defects, function impairment, tissue deformation (aesthetics), and trismus in patients.

Restorative dentistry service is an integral part of the patient's journey and is responsible for the assessment of their overall oral health to decide whether some teeth should be kept or extracted. They are also responsible for the maintenance and restoration of function and aesthetics. Restorative dentist is key within the head and neck MDT, from dental pre-assessments to complex oral rehabilitations following extensive surgical management.

The recently published (Oct 2022) NHS's Clinical standard for restorative dentistry provides a list of performance indicators to be collected to benchmark and measure the quality of care provided by Restorative Dentistry.

The QOMS Restorative Dentistry / oral rehabilitation for Head and Neck cancer patients (RD) registry proposes to achieve this by capturing clinical and patient-reported outcomes for restorative dentistry. The project has already obtained approval from CAG (section 251, England and Wales) to collect clinical data as part of the QOMS Oncology & Reconstruction registry.

The QOMS Restorative Dentistry / oral rehabilitation for Head and Neck cancer patients (RD) registry proposes to collect PROM data using the Oral Health Impact Profile questionnaire (OHIP-14) at three time points: before treatment (baseline) and at 18 and 36 months post-surgery.

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.

Data requirements

Whose data will be processed? –Staff, patients, members of the public etc.	Patients
Identify types of data that are/will be processed	Name, identification number, and contact information (other identifiers and items are already collected as part of the Oncology & Reconstruction registry)
What personal identifier are collected? Why?	
Data field	**Justification**
Name	Consent
Contact information	Consent / To send reminder for PROM
NHS, CHI or hospital number	To identify and track patients across hospital systems / Link with data collected in the Oncology & Reconstruction registry
List of fields collected (other)	The full PRO questionnaire is provided in Supporting Document 1 (SD1)
Summarise the proposed system/use of data—*How will the data be used?*	The data will be used to establish an overview of the quality of care and how it changes over the course of treatment (baseline to 36 months post-surgery) from a patient's perspective both at trust / health board and national levels. In time, hospitals will be able to compare their results against a national average and against similar institutions. Units with good performance scores will be encouraged to share with others how they achieved their results and units who "underperformed" will have the opportunity to consider how they might learn from others and improve their service and outcomes.
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.*	No
How many individuals' data will be involved?	This depends on the volume of orthognathic surgery performed in the hospital. Expected to be 10's records pa
From where will data be obtained, and how?	
The PROM data will be collected directly from patients. Patients will be asked on three occasions during their treatment journey (before the start of treatment and twice after surgery) to complete an online questionnaire.	

The data collection system used is the Research Electronic Data Capture (REDCap) system. Data is collected and stored in secure servers, hosted and managed by the Barts Cancer Research UK Centre, Queen Mary University of London (BCC, QMUL).	
Will any of the data be shared with a third party? *(Details below.[2])*	Yes
Data is collected centrally, outside of the Trust / Healthy Board, on servers manged by the Barts Cancer Research UK Centre, Queen Mary university of London. Staff are trained in Information Governance yearly and have clause in their contract about confidentiality. They to do not have access to the data. A Service Level Agreement is place. The QOMS Project Manager is non clinical and receives yearly training in Information Governance (same as BCC staff). Anonymised data will be shared with a statistician for analysis. Secondary research may be possible on the data collected. Any application has to be made through the Project's Working Group and BAOMS. No identifiable data is shared. Application from commercial third parties are not considered.	
Has the third party ever received any decisions against it from a supervisory body regarding data breaches?	No

Processing of data from children and vulnerable populations

Are you processing personal data of children or other vulnerable population(s)?	To be consented, patients should be 16 years of age or over. Patients need to be of a certain age to be able to answer the questionnaire.
Is consent required of the child?	No
Has parental permission been obtained for the use of this information, if the child is not of age or capacity to consent?	Provisions have been made to obtain parental consent, if the patient is not of age or capacity to consent.
Are there measures in place to seek consent from the child when they become of age or capacity to do so?	No
Has the privacy notice been written in clear, plain language which a child can understand?	Yes
Is the project for the offering of online preventive or counselling services to a child? If so, parental consent should not be sought	N/A

[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.

Does the project involve direct marking to a child?	N/A
Does the project involve automated profiling of a child?	No

Compliance with Caldicott principles[3]

No.	Principle	How will the project comply?
1	**Justify the purpose(s) for using confidential information** Every proposed use or transfer of confidential information should be clearly defined, scrutinised and documented, with continuing uses regularly reviewed by an appropriate guardian.	**Data flow** • Data collection. Patients will complete questionnaires directly online. • Data storage. Data are stored on secure servers administered by the BCC, QMUL and curated by the project's working group. • Data usage/access. Data is accessible to (1) participating departments (limited to their own patients only) for local analysis/use and (2) the project manager to produce hospital- and national-level results. • Dissemination. Results will be shared with participating departments, in reports, scientific publication and at conferences. Only patient aggregated data (completely anonymised) will be released. → See data flow in Appendix 1.
2	**Use confidential information only when it is necessary** Confidential information should not be included unless it is necessary for the specified purpose(s) for which the information is used or accessed. The need to identify individuals should be considered at each stage of satisfying the purpose(s) and alternatives used where possible.	Patient name and contact information are collected as part of this process and will be used to contact the patient to collect follow-up data (18 and 36 months questionnaires).

[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, *Information: To share or not to share? The Information Governance Review (2013),* introduced a seventh principle regarding the duty to share. The Principles were updated in December 2020 and an eighth principle added.

3	**Use the minimum necessary confidential information** Where use of confidential information is considered to be necessary, each item of information must be justified so that only the minimum amount of confidential information is included as necessary for a given function.	Name and contact information are necessary to contact the patient to collect follow-up data. NHS, CHI or hospital number is necessary to link with clinical data, collected elsewhere.
4	**Access to confidential information should be on a strict need-to-know basis** Only those who need access to confidential information should have access to it, and then only to the items that they need to see. This may mean introducing access controls or splitting information flows where one flow is used for several purposes.	Access control is in place whereby: - Local designated clinical leads at participating hospitals can only access data entered from their own institution. - Members of staff at the BCC may also have access but it is limited to database maintenance and data retrieval purposes. - BAOMS BOS Project Working Group. Only the project manager (non-clinical) has access to the full dataset, including hospital name. Access to the online registry is under a 2-factor authentication process. Each user is given a unique username and password.
5	**Everyone with access to confidential information should be aware of their responsibilities** Action should be taken to ensure that all those handling confidential information understand their responsibilities and obligations to respect the confidentiality of patient and service users.	Within each hospital involved in the project, members of staff have confidentiality clauses in their contracts and complete mandatory training modules/courses for information handling and data security. The project manager is a non-clinical member of the project Working Group and is neither an NHS nor a QMUL employee. They have however received the same level of training as BCC employees.
6	**Comply with the law** Every use of confidential information must be lawful. All those handling confidential information are responsible for ensuring that their use of and access to that information complies with legal requirements set out in statute and under the common law.	The project depends on the following organisations BAOMS, BOS and the BCC, QMUL. The persons responsible for ensuring that the organisation complies with legal requirements are: - BAOMS: Mr Jeremy McMahon, Caldicott Guardian (E: office@baoms.org.uk), - BCC: Sharon Robinson, Information Governance Lead (E: s.robinson@qmul.ac.uk).

7	**The duty to share information for individual care is as important as the duty to protect patient confidentiality** Health and social care professionals should have the confidence to share confidential information in the best interests of patients and service users within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.	Data collection is prospective. Participation in the project will be not alter a patient's diagnosis or treatment. There should not therefore be any incidental findings regarding patients.
8	**Inform patients and service users about how their confidential information is used** A range of steps should be taken to ensure no surprises for patients and service users, so they can have clear expectations about how and why their confidential information is used, and what choices they have about this. These steps will vary depending on the use: as a minimum, this should include providing accessible, relevant and appropriate information - in some cases, greater engagement will be required.	Prior to taking part in the project, patients will be given a patient information leaflet (PIL) before being consented. The PIL will provide information about what the project is, who is organising it and why, which identifiable information is collected and why, the patient's right to withdraw at any time, and the project team's contact details. The most recent version of the PIL and consent form are provided as attachments 1a and 1b, respectively.

Data subject rights

Have individuals been informed about the proposed use of their personal or special categories of personal data?	Yes. A information leaflet has been written for patients and consent will be sought after reading this document.
How can data subjects exercise their rights to access, view or request copies of their personal data?	Contact details for the treating team and the project team are available on the consent form, patient information leaflet and online (project team only).
How can data subjects exercise their rights to request rectification of any inaccuracy in their personal data?	N/A
How can data subjects exercise their rights to erasure ('right to be forgotten')?	Patients can get in touch their treating team or the project team. Contact details are available on the information leaflet and the consent form.
How can data subjects exercise their rights to restrict the processing of their personal data?	Patients can get in touch their treating team or the project team. Contact details are available on the information leaflet and the consent form.
How can data subjects exercise their rights to data portability?	Patients can get in touch their treating team or the project team. Contact details are available on the information leaflet and the consent form.
How can data subjects exercise their rights to object to the sharing/processing of their personal data?	Patients can get in touch their treating team or the project team. Contact details are available on the information leaflet and the consent form.
Will the processing of data include automated individual decision-making, including profiling?	No

Legal basis

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 (Special category data)**	
1(a) Consent	☒	2(d) Legitimate interest	☒
1(e) Necessary for performance of a task carried out in public interest or in exercise of official authority	☒	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	☒
See with your Trust / Health Board's IG Team, which legal basis (Articles 6 & 9), they think is the most appropriate. Interpretation of the articles may differ between Trusts/ Health Boards.			
How will the common law duty of confidentiality be satisfied?[4]	Consent		
Please explain reasons for the above choice:			

[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 (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.

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 the UK, by as third party. The data processor responsible for data storage is the Bart's Cancer Research UK Centre, Queen Mary University of London (BCC, QMUL)
Details about the BCC, QMUL	EE133904-ECC04 Barts CR-UK Centre (BCC) 22/23 Standards Met 20/06/2023 ISO27001 certification: 225111 (see attached)
Relationship between the project's data controller and data processor	BCC, QMUL stores data on behalf of BAOMS. An service level agreement (SLA) between the 2 organisations is in place and is renewed annually

How information will be stored? *(Include physical and cyber security arrangements.)*

Physical security arrangements

- The IT infrastructure is hosted in a tier 3 commercial datacentre. The building is manned 24/7 by security guards. CCTV cameras are installed around the perimeter of the building at all entrances and exits as well as at every access point and other critical areas throughout the building. Dual factor authentication (formal ID card and fingerprint) is required to access the building through a mantrap. A private cage on the data floor is used to further secure the IT equipment.

System information

- All systems will be protected by a multi-layer approach involving firewall, intrusion detection and prevention systems, e-mail scanning and endpoint malware protection. These are in addition to security measures taken by QMUL central IT Services at the perimeter network.
- The system used consists of a front-end application server and a back-end database server. Windows Server 2016, REDCap v9 and MySQL v8 are used.

- The computer system is network connected (LAN). The database server is placed in the CLINICAL-DB network. This network is used to contain database servers for clinical trials only. The application server is placed in the DMZ network to enable external web application access.
- Direct remote connections to these networks are prohibited.
- Firewall controls are in place to ensure only the required ports (database listener) on the database server are explicitly open to the designated application server. The application server is placed in the DMZ network and only secure HTTP port is allowed externally.
- All other traffic is dropped by the firewall.
- These systems are managed by BCC IT.

Who is the Information Asset Owner?[5] *(Give name and job titles and details of relevant training)*

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

BAOMS (central): Mr Jeremy McMahon, Consultant Maxillofacial Head & Neck Surgeon | BAOMS Caldicott Guardian MRC Research, GDPR and Confidentiality – what you really need to know' modular course	Your Hospital / trust / Health Board:
Who is the Information Asset Manager?[7] *(Give name and job titles and details of relevant training)*	
BAOMS (central): Fabien Puglia, BAOMS Project Manager Data Security Awareness Level 1 (2023 11 03) 'MRC Research, GDPR and Confidentiality – what you really need to know' modular course	Your Hospital / trust / Health Board:
Who will have access to the data? *(Give names and job titles and details of relevant training)*	
Clinical leads and data entry staff at participating hospitals will have access to date collected form their own patients. The clinical lead should be at consultant level. All staff should have completed suitable training from their Trust / Health Board. As part of the Working Group, the project manager is a non-clinical member of the project team. The role is currently fulfilled by Dr Fabien Puglia (see details above). They annually complete the NHS Digital Data Security Awareness Level 1.	
Do you have a disaster recovery/business continuity plan?	Yes. We follow the BCC business continuity plan – see Attachment 3.

External data transfer

Will data be transferred outside?	**Yes – Within the UK**
To whom and where will the data be transferred? *(Please give details. If outside the EEA, please also give the country.)*	Only anonymise data will be shared. They will be shared with the statistical team / statistician for analysis and upon request (and review) to non-commercial, NHS or academic third parties for secondary analysis.
Are there different levels of access granted to the different parties? How is access granted, reviewed and removed?	Users are under access control and all actions within the database are recorded in the audit trail. • Users are assigned to a data access group (this means they can only access data collected within that group ~ here the Trust) and to a role, which dictates what they can or cannot do within the database. • Access to the database is through individual login (unique username and password) and 2-factor authentication is in place. Access is managed centrally by the project manager. New users need to be approved by the local clinical lead who also needs to update the project manager with any changes. The project manager will also regularly query users with the local lead.
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.)*	Only anonymised data will be shared via email in password-protected documents. The password will not be sent with the data.

Data accuracy and retention

Who will be responsible for data accuracy? *Job role, organisation.*	Fabien Puglia, BAOMS Project Manager, BAOMS
How will accuracy of the data be assured? *What processes are in place to assure good data quality?*	Accuracy is not relevant here. PROM collects information about patient's individual perceptions. Accuracy is not relevant under such circumstances.
Who will retain and hold this data? ***Job role, organisation***	Jonathan Croft, Head of Research Computing, Bart's Cancer Research UK Centre IT, Queen Mary University of London
For how long will the data be retained? *This should align with the Trust's retention schedule.*	The data are to be retained for 4 years after the end of collection of follow-up data.
Who will be responsible for secure disposal of data? ***Job role, organisation.***	Jonathan Croft, Head of Research Computing, Bart's Cancer Research UK Centre IT, Queen Mary University of London
How will data be disposed of securely? *What method(s) will be used to destroy the data securely?*	To ensure secure deletion, a product that overwrites data many times must be used, such that the information cannot be recovered.

Transparency

<table>
<tr><td>Who will you be consulting with?</td><td>Patients</td></tr>
<tr><td>How were individuals consulted? <i>(e.g. meetings, surveys, focus groups, patient panels, professionals.)</i></td><td>A group of patients was contacted through personal networks.</td></tr>
<tr><td colspan="2">What concerns have been raised and how are these being addressed? <i>(e.g. invasion of privacy, risks etc.)</i></td></tr>
<tr><td colspan="2">Patients had a general positive opinion of the QOMS Restorative Dentistry / oral rehabilitation for Head and Neck cancer patients (RD) registry. They were satisfied with registry design, aims, etc, with the precautions taken to ensure data security and confidentiality and with the steps taken to ensure patient's rights.</td></tr>
</table>

Data subjects' rights and opt-outs

<table>
<tr><th colspan="2">How will data subjects be informed about the processing, and what information has or will be provided?</th></tr>
<tr><td colspan="2">A patient information leaflet (PIL) has been produced by the Working Group in collaboration with patient representatives. The PIL provides information about the background and aims of the work, the nature and extent of the collected information, its use and retention and the subject's right to withdraw at any time. As this is a consented project, the opt-out scheme does not apply.
A copy of the patient information leaflet and consent form are provided as Attachment 1a and 1b.</td></tr>
<tr><td><b>Will data subjects be able to opt-out of the data use at any time?</b></td><td>Yes</td></tr>
<tr><td colspan="2"><i>Note: For England only, this registry does NOT need to comply with national data opt out.</i></td></tr>
</table>

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	**Risks of unauthorized disclosure**							
	Controversial or unethical use; Misuse (financial gain, espionage, extortion, fraud)	5	2	10	Staff training, data minimization, pseudonymisation / anonymisation, access controls and contractual agreements	2	2	4
	Relevant Threats: Server hacking	5	3	15	Firewall/security measures (see Information Security Policy and BCC Secure Platform network diagram)	3	2	6
2	**Potential threats to data integrity:** Data quality	3	3	9	Ensuring the clarity and readability of questionnaires	2	2	4
3	**Risks of data loss, destruction or corruption are present at each step of data processing.** Restoring a previous version of the database may be accompanied by some data loss	3	3	9	Staff training / Backup and restore procedures / IT support	2	2	4

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

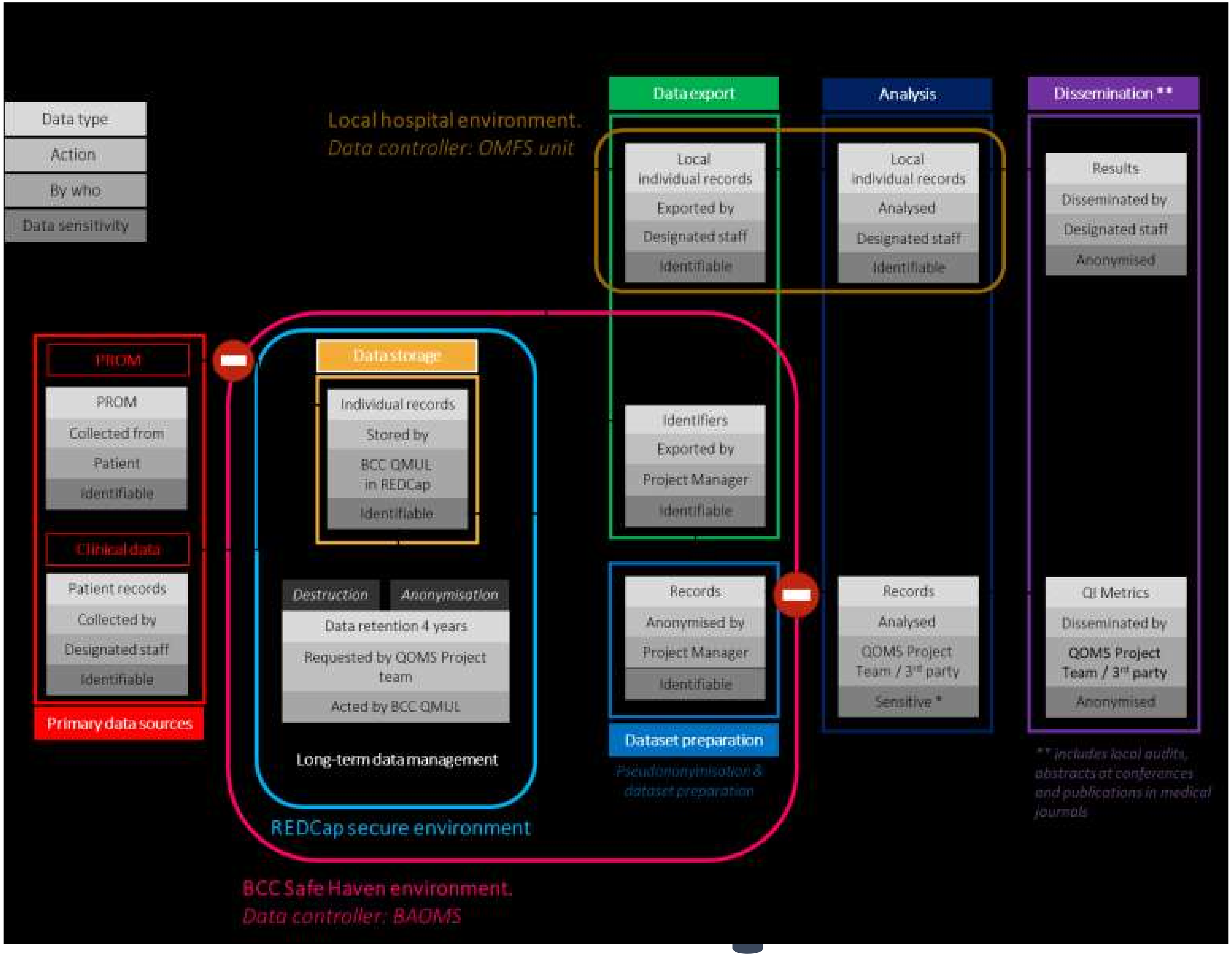
Review

	Name	Date
IG review completed by:		
Next review due (normally annually):		

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

DPIA Form version 3.10 10th December, 2020

Appendix. Data flow



Data type
Action
By who
Data sensitivity

Local hospital environment.
Data controller: OMFS unit

Primary data sources

PROM
PROM
Collected from
Patient
Identifiable

Clinical data
Patient records
Collected by
Designated staff
Identifiable

REDCap secure environment

Long-term data management

Data storage
Individual records
Stored by
BCC QMUL in REDCap
Identifiable

Destruction	*Anonymisation*
Data retention 4 years	
Requested by QOMS Project team	
Acted by BCC QMUL	

BCC Safe Haven environment.
Data controller: BAOMS

Data export

Local individual records	Identifiers
Exported by	Exported by
Designated staff	Project Manager
Identifiable	Identifiable

Dataset preparation

Pseudonanymisation & dataset preparation

Records
Anonymised by
Project Manager
Identifiable

Analysis

Local individual records	Records
Analysed	Analysed
Designated staff	QOMS Project Team / 3rd party
Identifiable	Sensitive *

Dissemination **

Results	QI Metrics
Disseminated by	Disseminated by
Designated staff	QOMS Project Team / 3rd party
Anonymised	Anonymised

*** includes local audits, abstracts at conferences and publications in medical journals*