Data Protection Impact Assessment (DPIA)

This Data Protection Impact assessment (DPIA) was 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. It should assist in identifying the risks of processing and sharing personal data, and in creating solutions to reduce them.

Project/activity details

Project title			
Rare Benign Lesions of the Jaws Registry			
Project sponsor	The British Association of Oral and Maxillofacial Surgery (BAOMS)	**Lead organisation**	The British Association of Oral and Maxillofacial Surgery (BAOMS)
Project lead **Telephone** **Email**		**Division** **Directorate** **Proposed start date**	
Will you be using personal data?[1]	Yes ☒ No ☐	If no personal data will be collected or processed, the DPIA is complete.	

Project purpose and description

What is the purpose of the proposed project, why is it necessary, and how will it be achieved?
In response to the publication of the 1st GIRFT report for Oral and Maxillofacial Surgery (OMFS), 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. QOMS operates a series of registries as audits or service evaluations across several OMFS subspecialties or for specific conditions or procedures for which little or no data, recommendations or guidelines are available nationally. The Rare Benign Lesions of the Jaws (RLJ) registry is one of the latter. Numerous benign lesions, cysts or solid tumours may present in the jaws. They may be of either odontogenic (tooth-forming, in the dental alveolus) or non-odontogenic (mainly bone) origins in the mandible and maxilla. From a diagnosis perspective, these lesions may have similar imaging features and their location, margins, internal contents, and effects on adjacent structures are important features to diagnose them. These rare benign lesions and tumours of the jaws (RLJ) can vary in behaviour, and despite being benign, some can grow rapidly and result in destruction of surrounding structures. Many require often-morbid treatment to prevent their recurrence. In recent years / decades, less invasive and adjunctive treatments have become available to lessen the morbidity associated with surgical treatment. As the molecular and genomic pathogenesis of these lesions is better understood, more directed treatments may lessen the burden for patients. By collating the data of patients affected by these conditions in a specific / dedicated registry, we want to establish the epidemiology of RLJ in the UK and assess how they are treated.

[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.

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**
Name	Consent
Email	Consent
NHS, CHI or hospital number	To identify and track patients across hospital systems
Postcode	To look at the effect of IMD and potential postcode lottery in condition epidemiology and treatment
Sex	For descriptive purposes
Dates (inc. DOB)	To draw an exact picture of condition and treatment history
Ethnicity	
	Full list of collected field is provided in Supporting Document 1 (SD1)

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

Primary aims:

The data will be used (1) to ascertain the epidemiology of these conditions, (2) to see how they are treated nationally and (3) to identify variations in treatment and management.

Secondary aims:

(1) Development of a discussion forum for clinicians. Unless requiring extensive reconstruction, rare benign lesions of the jaws are usually not discussed in multidisciplinary team (MDT) meeting. We would like to create an online forum (similar to an MDT), run quarterly, at either the national or regional level for clinicians to discuss their cases.

(2) Secondary research will be possible on the data collected as part of the registry.

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])* .

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.

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

From where will data be obtained, and how?

Directly from patients' records and medical notes by the treating team or individuals within the Trust / Health Board tasked to collect that information.

The data collection solution 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? Yes ☒ No ☐ *(If Yes, please give details below.[3])*

The data is stored at a third party's installation (Barts Cancer Research UK Centre, Queen Mary University of London BCC, QMUL) and managed by the QOMS Project Manager.

The BCC is responsible for the management and maintenance of the servers where the data is stored. 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).

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? Yes ☐ No ☒ *(If Yes, please provide details below)*

Compliance with Caldicott principles[4]

Good information sharing is essential for providing safe and effective care. There are also important uses of information for purposes other than individual care, which contribute to the overall delivery of health and social care or serve wider public interests.

These principles apply to the use of confidential information within health and social care organisations and when such information is shared with other organisations and between individuals, both for individual care and for other purposes.

The principles are intended to apply to all data collected for the provision of health and social care services where patients and service users can be identified and would expect that it will be kept private. This may include for instance, details about symptoms, diagnosis, treatment, names and addresses. In some instances, the principles should also be applied to the processing of staff information.

[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, *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.

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** Patients will be consented. Data, including confidential information, will be collected by the treating team / designated individuals in the hospital and entered via a secure portal in the online registry. Data will be curated there until it is used. Data export: (1) Data collected locally will remain accessible to the treating team. They will be able to download it and use it locally as needed. (2) Central dataset will be analysed regularly to check for progress and identify data collection issues. Once a sufficient amount of data has been collected, it will be analysed for trends… by a statistician. Only anonymised dataset will be shared with them. (3) Third party request to access the data for secondary analysis remains possible. Only anonymised dataset will be shared with them. See data flow provided 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.	Consent: patient name and contact details will be collected as part of this process only. No patient details shall be shared outside of the project. Clinical data: NHS, CHI or Hospital number, date of birth, sex, postcodes, ethnicity and dates will be collected. No personal identifiable shall be shared outside of the project. Given the specifically sensitive nature of the postcode, they will be only be kept for a year before being transformed into a LSOA, the index of multiple deprivation and a distance from hospital. A full list of collected fields is provided in supporting Document 1 (SD1)
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.	Although secondary research remains a possibility, the primary aim off the registry is to assess how patients affected by RLJ are treated in the UK (service evaluation). The dataset only collects data created as part of the process of care. The different items collected were selected by clinicians as relevant to the purpose of the registry.

No.	Principle	How will the project comply?
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.	Data within the registry is identifiable. The only user who has access to the whole dataset is the project manager. Other users are under access control whereby they can only access the data collected in their own institution. Members of staff at the BCC may also have access but it is limited to database maintenance and data retrieval purposes. Other members of the registry's Working Group have access to anonymised data only. Finally, third parties do not have access to the online registry. If their application to access data is successful, only anonymised data will be shared.
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 BCC 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 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.

No.	Principle	How will the project comply?
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 being enrolled in the registry, patients are 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 Supporting Documents 2a and 2b, respectively.

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 (Special category data)**	
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 or statistical 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:

[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.

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 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? *(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? *(Give name and job titles and details of relevant training)*

BAOMS:

Mr Jeremy McMahon

Consultant Maxillofacial Head & Neck Surgeon | BAOMS Caldicott Guardian

MRC Research, GDPR and Confidentiality – what you really need to know' modular course

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

Fabien Puglia

BAOMS Project Manager

Data Security Awareness Level 1 (07/11/2022)

'MRC Research, GDPR and Confidentiality – what you really need to know' modular course

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

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 ☒ 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.)*
We follow the BCC business continuity plan – see Supporting Document 3 (SD3)

External data transfer

Will data be transferred outside?			
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.)*			
Data 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.			
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 transferred dataset is anonymised and shared via email in password-protected documents. The password is not to be sent with the data.			

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?*
Fabien Puglia BAOMS Project Manager British Association of Oral and Maxillofacial Surgeons	Data accuracy depends on the quality of data entry. Data is checked for potentially erroneous information (e.g. unlikely ages, size…). The registry does not have the resources to perform double data entry or to quality control.
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.*
Jonathan Croft Head of Research Computing Bart's Cancer Research UK Centre IT Queen Mary University of London	The data are to be retained for 10 years after the end of collection of follow-up data.

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?*
Jonathan Croft Head of Research Computing Bart's Cancer Research UK Centre IT Queen Mary University of London	To ensure secure deletion, a product that overwrites data many times must be used, such that the information cannot be recovered.

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.)*

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

What concerns have been raised and how are these being addressed? *(e.g. invasion of privacy, risks etc.)*

Data subjects' rights and opt-outs

How will data subjects be informed about the processing, and what information has or will be provided?
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.

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.	

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)	1	1	1	Staff training, data minimization, pseudonymization / anonymization, access controls and contractual agreements	1	1	1
	Relevant Threats: Server hacking	2	3	6	Firewall/security measures (see Information Security Policy and BCC Secure Platform network diagram)	2	2	4
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.

Appendix. Data flow