Quality and Outcomes in Oral and Maxillofacial Surgery Programme

General Privacy & Fair Processing Policy

Version: 3.0 *Date: January 2024*

Section 1 – Introduction

What is the aim of the QOMS?

The British Association of Oral and Maxillofacial Surgeons (BAOMS) is a national professional association for the oral and maxillofacial surgical specialty. BAOMS and other similar associations have been created to promote the exchange of clinical and scientific information amongst clinicians working in the same field and to advance and harmonise standards of patient care. To fulfil this role, BAOMS set up the Quality and Outcomes in Oral and Maxillofacial Surgery (QOMS) programme in 2018.

QOMS aims to measure the quality of care and outcomes for patients receiving oral and maxillofacial treatments in NHS and private hospitals and to improve the quality of care by providing comparative information for hospitals nationwide. QOMS operates a series of registries to collect patient information across different areas of practice within the oral and maxillofacial surgery (OMFS) specialty.

Depending on the area of care and the nation, QOMS registries may rely on patient's consent or other information governance process (for example section 251 support in England and Wales, see below for details) to collect information.

Information governance

"Information Governance" is the legal framework governing the use of personal confidential data. In the context of healthcare, it ensures that information is handled in a secure and confidential manner to allow organisations and individuals to manage patient, personal and sensitive information legally, securely, efficiently and effectively in order to deliver the best possible healthcare and services.

Each UK nation has its own information governance framework.

Data Controller

A "data controller" determines the purposes (the why) and means (the how) of processing personal data.

BAOMS is using information collected from medical records and/or directly from patients to undertake this work. BAOMS acts as data controller and is therefore responsible for looking after and using that information properly.

Data Processor

A "data processor" is any person (other than an employee of the data controller) who processes the data on behalf of the data controller.

For QOMS, the Barts Cancer Research UK Centre, Queen Mary University of London (BCC, QMUL) is the main data processor. QOMS may have other data processors, e.g. a statistician, who will analyse data on the project's behalf but will not have access to directly identifiable information.

Data collection without patient consent in the UK

Where possible and appropriate, QOMS collect patient data without consent. Approvals to do so have been obtained from the devolved administration.

- In England, the process is commonly called "section 251" and is applied for via the Confidential Advisory Group of the Health Research Authority (CAG, HRA). Section 251 in England is also subject to the national data opt-out (see below).
- Section 251 applies to both England and Wales but in the case of the latter, there is no national data opt-out.

- In Scotland, a similar process exists (though it does not have a name) and is applied for via the NHS Scotland Public Benefit and Privacy Panel for Health and Social Care (HSC-PBPP). PBPP is a governance structure that scrutinises and considers applications purpose for public benefit and information governance requirements.
- There is no equivalent process to section 251 or PBPP in Northern Ireland.

What is "section 251"?

"Section 251" (s251) refers to section 251 of the National Health Service Act 2006 and its current regulations, the Health Service (Control of Patient Information) Regulations 2002.

S251 exemption enables the common law duty of confidentiality to be temporarily lifted so that confidential patient information can be transferred to an applicant without the discloser being in breach of the common law duty of confidentiality. In practice, this means that the person responsible for the information (the data controller) can, if they wish, disclose the information to the applicant without being in breach of the common law duty of confidentiality. They must still comply with all other relevant legal obligations e.g. the Data Protection Act 2018.

In practice, it means that patients need not give their consent in order for the registry to collect, store and process identifying information. The rights to access, change or remove information are nevertheless maintained. If a patient withdraws from QOMS, no further information about them will be collected. If requested by the patient, we will arrange for their information to be deleted as soon as possible, some might be kept for future reference and audit trail. To safeguard patient rights, we will use the minimum personally identifiable information possible.

The process to obtain s251 means that the person(s) receiving the information has undergone an independent review of their purposes and governance arrangements.

Similar principles apply to the PBPP process.

The national data opt-out

In England, the national data opt-out (NDO) was introduced in May 2018 and became mandatory in October 2022. The NDO enables patients to opt out from the use of their data for research or planning purposes, in line with the recommendations from the National Data Guardian's Review of Data Security, Consent and Opt-Outs. The NDO applies to projects relying on section 251 support to collect patient information without consent.

More information can be found here.

→ If you are a patient, please read sections 2 and 4

→ If you are a registry user, please read sections 3 and 4

Section 2 – Patients

Where is patient data collected from? QOMS captures data on patients with specific conditions and/or undergoing specific oral and maxillofacial surgical procedures in hospitals (details can be found here). The data covers the care patients received, for example the investigations and treatments received, how long it took for different parts of treatment to be given and their clinical outcomes.

What information do we collect about you and how do we use this?

The personal information collected are date of birth, NHS number, hospital number, postcode and sex. Names and contact information are only collected when patient consent is sought. Data are submitted directly to QOMS by the clinical teams treating the patient or from hospital records and includes information about the patient's general health, the type of surgery and the care received before, during and after surgery.

The information collected is used by doctors, nurses and medical researchers to:

- Produce information on the quality of care received by patients undergoing OMFS surgery in hospital.
- Ensure that any changes or improvements to services benefit patients.
- Learn about the best ways in which doctors and nurses can use patient information to improve quality of care.
- Understand what happens to patients after they leave the hospital after a treatment, and whether the surgery has had a beneficial effect on their long-term health.

By collecting and sharing this information, QOMS is able to highlight areas where hospitals are doing well, and areas in which they can improve the quality of care for patients so that they can put plans in place to achieve this. It also allows OMFS units to compare themselves with others in the country and in doing so improve the quality of care by sharing examples of good practice.

No information that can identify individual patients will be published.

For the QOMS Oncology & Reconstruction, Trauma and Orthognathic Surgery registries we have also collected past data (retrospective data) to pre-fill the database. However, the directly identifiable data in these datasets have already been removed.

Legal basis for collecting and processing personal data

Under GDPR, the following legal bases apply:

- Article 6 (1) (e): processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller and
- Article 9 (2) (i): processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of healthcare and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy.

Management of patient data and confidentiality

The QOMS project team conforms to the General Data Protection Regulation (GDPR) and other legislation that relates to the collection and use of patient data and follows strict security measures in place to safeguard patient information.

The patient information received and managed by the QOMS project team is treated as confidential. Data collected as part of the non-consented (s251) audit project will be retained for 4 years after the end of data collection, in order to assess the long-term effects of the procedures.

Data retention for consented projects will depend on the project itself and will be clearly stated in the information leaflet given to patients to read prior to signing consent for their data to be used.

We maintain the confidentiality and security of patient information in the following ways:

Data collection, curation and analysis:

- All information is available for viewing/editing only to the individuals or local teams who collected that data at the participating hospital where a patient was treated. Local teams must follow the information governance rules of their hospitals.
- The project's designated data manager is the only member of the QOMS Project Team to have access to the full dataset. Their access is limited to specific tasks. Other members of the project team have only access to pseudonymised data (i.e. all patient identifiable information like NHS or CHI number, date of birth, have been removed). Staff at the Barts Cancer Research UK Centre can access the data for database maintenance and data retrieval purposes.
- All access to, and activities on, data are documented in the audit trail.

Reporting and publications:

- All reports and publications are produced at an aggregate level (national, regional, hospital), i.e. they are completely anonymised, and it is impossible to identify patients.
- In each audit publication, the statistical information is reviewed to ensure the risk of identification is minimised, and where necessary, small numbers are suppressed. This assessment follows guidelines issued by the Office for National Statistics - Review of the Dissemination of Health Statistics: Confidentiality Guidance.

Level of security

The database system has various levels of security built into it, including:

- ID password security: the data is stored on a password protected system, which prevents unauthorised users gaining access.
- Each user is assigned a unique username and password, and a two-factor authentication is in place.
- Users are assigned to a group (here their hospital/unit) and can only access the data entered by users in the same group.
- Users are assigned to specific roles with different 'privileges' to view, edit, export and delete records. User are assigned to a role compatible with their QOMS duties.
- The stored data files are encrypted.

Data sharing and linkage with organisations curating administrative and other registry databases

- QOMS only shares patient-level data following a strict governance procedure to ensure compliance with the General Data Protection Regulation (GDPR).
- Linkage to administrative datasets enables QOMS to ascertain data coverage (i.e. compare retrospectively the number of records submitted to the registry with the number recorded in that administrative dataset) to ensure high data quality.
- Linking enables to obtain patients' long-term outcomes, e.g. mortality rates in the first 30 days after treatment.
- Administrative datasets include but are not limited to the Health Episode Survey (HES) managed by NHS England or the Patient Episode Database for Wales (PEDW), managed by the NHS Wales Informatics Service (NWIS). In England, HES data are used by the National Consultant information Programme (NCIP) and QOMS is collaborating with NCIP to validate our respective data entry processes.

- Linkage to datasets from other registries can have similar uses but can also increase data accuracy and decrease data entry workload by sharing coincident data fields. Other registry datasets include but are not limited to the UK National Flap Registry (UKNFR) managed by the British Association of Plastic, Reconstructive and Aesthetic Surgeons (BAPRAS).

Data sharing with other third parties

- Data sharing with other third parties will be limited to anonymised data. This means that directly identifiable information (like name, NHS number, date of birth…) would have been removed prior to the data being transferred.
- Data analysis for QOMS will be performed by statisticians from third party institutions, which include but are not limited to Brunel University London, and University of Kent.
- Third-party researchers may apply to the QOMS Data Controller for access to QOMS data. These requests undergo a stringent approvals process. Only anonymised data will be shared.

What if a patient does not want their information used by QOMS?

If a patient chooses to not participate to QOMS from the onset, their care will not be affected by their decision. They should however communicate this decision by:

- Either emailing qoms@baoms.org.uk and put "Patient request to opt-out" in the subject line. The team will then contact the hospital to request that they do not enter the patients details into the audit.
- Or notifying directly a member of their local care team that they wish to opt out.

If a patient decides to no longer participate to QOMS:

- If their details have already been entered into the registry, their rights to access, change or remove their information may be more limited, as QOMS needs to manage this information in specific ways in order for research and reports to be reliable and accurate.
- If their data has not yet been used for analysis, it will be removed from QOMS.
- If their data has already been used for analysis, we will not be able to remove the information that has already obtained and used. However, the data will be removed and no longer be available for further analysis.

In all cases, to safeguard their rights, we will use the minimum personal identifiable information possible.

In some circumstances, an individual has the right to request their data are erased. This does not apply to an individual's healthcare record.

→ Please read section 4

Section 3 – Registry users and others

What data are collected and why

- To access QOMS, potential users need to contact the QOMS project manager to register with the BCC to obtain a username and temporary password.
- Part of the registration process for using the webtool is to accept the BCC terms & conditions.
- Once registered, each user will be invited to the audit(s) to their current activities and assigned to a group and a role, which determines their level of privileges to access and/or enter data for their group/team(s).
- The user data collected includes their full names, a working email address and their current institution(s)
- In the case of local clinical leads and deputy clinical leads, their details may be shared with other members of their group (to enable communication within teams), may be used by the project team to contact them in the event of essential issues regarding data entry, which need to be rectified or with essential updates regarding the project, including the release of results, deadlines for data entry and dataset changes...

Note: if a user does not login to the system for 4 months, their account will be temporarily disabled, and they will need to contact the helpdesk to reactivate it. If an account inactivity of 12 months or more, the account will be permanently deleted. The user will then have to re-register with the BCC.

Data sharing outside the project team

In order to deliver this service, these user data will be shared with:

- Other registry users so that essential communication can occur between teams (see above)
- The clinical lead of the programme if required
- Details for clinical lead contacts registered in QOMS may be shared with NHSE including the CQC and appropriate bodies in Wales and Northern Ireland. This is largely dependent on audit results, particularly outlier status in mortality reporting.

This data will be retained in QOMS to:

- Maintain a record of their activity,
- Deactivate their account after long periods of inactivity (4 months without logging in),
- Delete their account after extended periods of inactivity and/or subject to organisational requirements.

Registered user's rights

Registered users have the rights to the following:

- *Access your data, request a copy of the data about them in standard format and/or update their information: they* have the right to ask for a copy of the information held about them and to have any inaccuracies corrected. To do so they should email the helpdesk at qoms@baoms.org.uk to request that information is provided and/or updated.
- *Restricting the use of their data, stopping their data being used, and/or deleting their data.* If a user wishes to restrict, stop and/or delete their data from the registry user database, they should the helpdesk at qoms@baoms.org.uk and they will apply those restrictions.

→ Please read section 4

Section 4

What information is captured from public visitors to the website?

Some information will be systematically collected by browsing the public section of the BAOMS website (including reading pages or download information). This information will not identify them and relates to:

- The internet domain (e.g. www.organisation.co.uk) and IP address from which the website was accessed,
- The type of browser (e.g. Internet Explorer or Chrome…), and operating system, such as Windows used,
- The date and time of the visit,
- The pages visited,
- The address of the web site from which they linked to us (if applicable),
- The query activities which they process, e.g. if applicable which document was downloaded…,
- This information will be used to make each visit more rewarding and to provide us with information to help improve our service. We do not know (nor do we want to know) the identities of people who visit us in this way.

Project newsletter mailing list

If someone (patient, clinicians or member of the public) signs up for our newsletter, then we would hold their name, email address, GMC code (if applicable) and place of work. Our legal basis for collecting and processing this information is "Legitimate Interest". The contact information provided will be handled in accordance with the General Data Protection Regulation (GDPR), and will not be used for any other purpose, unless consent has been received for other uses. Those individuals have the right to access data, request a copy of the data about them and/or update their information. To do so they should email qoms@baoms.org.uk to request that information is provided and/or updated.

Data protection

BAOMS and its collaborators on the project take the security of your data seriously.

In order to prevent unauthorised access or disclosure, we have put in place suitable physical, electronic and managerial procedures to safeguard and secure the information we collect online.

Local clinical teams enter patient data into a secure web-based tool (Research Electronic Data Capture – REDCap) provided by the BCC, QMUL. Only registered users at the participating hospitals and the QOMS project team will have access to the web-based tool. Security and confidentiality are maintained through the use of passwords and a person specific registration process.

Changes to our privacy policy

We keep our privacy policy under regular review, and we will always make the latest version of this document easily accessible. The privacy policy was last updated in January 2024.

Who can I contact about this notice?

if you wish to contact the QOMS Project Team with any queries about the information in this privacy notice, email qoms@baoms.org.uk.

People concerned also have the right to lodge a complaint with the Information Commissioner's Office (ICO), the supervisory authority in the UK responsible for the implementation and enforcement of data protection law, if you have concerns about the way your personal data is being handled. You can contact the ICO via their website or by calling their helpline – 0303 123 1113.