# Data Protection Impact Assessment Template

This Data Protection Impact assessment (DPIA) is a template designed for the QOMS Salivary Gland Cancers 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 | Salivary Gland Cancers registry |
| Project sponsor | The British Association of<br>Oral and Maxillofacial Surgery (BAOMS) |
| Lead organisation | BAOMS |
| Clinical lead (central) | Michael Ho, Consultant Maxillofacial Oncology |
| Contact details | Leeds Teaching Hospitals NHS Trust, Leeds Dental Institute, Worsley Building, Clarendon Way, LS2 9LU |
| Email | michael.ho2@nhs.net |
| Project manager (central) | Fabien Puglia, PhD |
| Contact details | Royal College of Surgeons of England, 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 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.

## 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 overarching aims of the project are (1) to measure quality of care provided by oral and maxillofacial surgery departments, (2) to identify unwarranted variation and (3) improve quality of care provided to patients. QOMS operates a series of registries across several OMFS subspecialties or for specific conditions or procedures for which little or no data, recommendations or guidelines are available nationally. The QOMS registries are considered audits or service evaluations.<br><br>The Salivary Gland Cancers (SGC) registry is a new registry under the QOMS umbrella specifically designed to collect information on the diagnosis, treatments and outcomes of patients affected by salivary gland cancers (SGC) in the UK.<br><br>In the UK, salivary gland cancers are a group of relatively rare cancers (8 or 9 per 1m people pa, or < 800 new cases pa). The most common type overall is adenoid cystic carcinoma, followed by mucoepidermoid carcinoma for the parotid glands and acinic cell carcinoma. Unfortunately, the clinical behaviour of many subtypes is still to be identified. SGC are generally slow growing and necessitate extended follow-up, making RCT impossible to conduct for this group of cancers. By collating the data of patients affected by these conditions in a specific / dedicated registry, we want to establish the epidemiology of SGC in the UK, assess how they are treated and ultimately support the development of guidelines for the treatment of these conditions.<br><br>Although led and supported by BAOMS, the QOMS SGC registry is open to medical and surgical specialties treating patients with salivary gland cancers. |

## 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, Location, Online identifier, Medical |
| What personal identifier are collected? Why? | |
| Data field | Justification |
| Name | Consent |
| Email | Consent / As an alternative to send reminder for PROM |
| Mobile number | As an alternative to send reminder for PROM |
| 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 and treatment |

| | |
|---|---|
| Sex | For descriptive purposes |
| Dates (inc. DOB) | To draw an exact picture of condition and treatment history |
| List of fields collected (other) | 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?* | 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. |
| 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 incidence of SGC in the population treated within the Trust. Expected to be 10's records pa |
| From where will data be obtained, and how? | |
| Clinical data: Directly from patients' records and medical notes by the treating team or individuals within the Trust / Health Board tasked to collect that information.<br>PROM: Directly from patients. Patients are contacted on a yearly basis and asked to answer a online PROM questionnaire<br>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 |
| 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.<br>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.<br>The QOMS Project Manager is non clinical and receives yearly training in Information Governance (same as BCC staff).<br>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. | |

[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.

| | |
|---|---|
| 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)? | Yes. The SGC registry does not focus on children or other vulnerable population(s) but should individuals be affected by salivary gland cancers, they could be recruited to partake to the registry |
| Is consent required of the child? | No. Consent for the registry is limited to individuals aged 16 or above. Below that age, a parent or a guardian need to give consent on behalf of the child |
| Has parental permission been obtained for the use of this information, if the child is not of age or capacity to consent? | Yes |
| 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? | No |
| Is the project for the offering of online preventive or counselling services to a child? If so, parental consent should not be sought | No |
| Does the project involve direct marking to a child? | No |
| 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**<br>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**<br>Patients will be consented.<br>Data sources:<br>(1) Clinical data, including confidential information, are collected by the treating team / designated individuals in the hospital and entered via a secure portal in the online registry. Data is curated there until it is used.<br>(2) PROM: patients are contacted on a yearly basis by email or text messages and asked to complete a PROM questionnaire online.<br>Data exports:<br>(1) Data collected locally remains accessible to the treating team. They are able to download and use it locally as needed.<br>(2) Central dataset is 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.<br>(3) Third party requests to access the data for secondary analysis remain possible. Only anonymised dataset are shared with them.<br>See data flow provided in Appendix 1 |
| 2 | **Use confidential information only when it is necessary**<br>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 | Consent and PROM: patient name and contact details are collected as part of this process only. Email and/or phone number are used to contact the patient to ask them to complete PROM questionnaire. The process is built-in REDCap. No patient details are shared outside of the project.<br>Clinical data: NHS, CHI or Hospital number, date of birth, sex, postcodes and dates are collected. No |

[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.

| | | |
|---|---|---|
| | satisfying the purpose(s) and alternatives used where possible. | personal identifiable are shared outside of the project. Given the specifically sensitive nature of the postcode, they are only 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<br>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 SGC are treated in the UK (service evaluation).<br>The dataset only collects data routinely created as part of the process of care.<br>The different items collected have been selected by clinicians as relevant to the purpose of the registry. |
| 4 | Access to confidential information should be on a strict need-to-know basis<br>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.<br>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.<br>Members of staff at the BCC may also have access but it is limited to database maintenance and data retrieval purposes.<br>Other members of the registry's Working Group have access to anonymised data only.<br>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<br>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.<br>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**<br>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:<br>- BAOMS: Mr Jeremy McMahon, Caldicott Guardian (E: office@baoms.org.uk),<br>- 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**<br>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**<br>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.<br>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.<br>The most recent version of the PIL and consent form are provided as Supporting Documents 2a and 2b, 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 on line (project team only). |
| **How can data subjects exercise their rights to request rectification of any inaccuracy in their personal data?** | Clinical data is collected directly from medical records. Should there be a mistake, patients should contact the Trust. |

| | |
|---|---|
| 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<br>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(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. | ☒ | 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 organisations and devolved administrations.* | | | |
| How will the common law duty of confidentiality be satisfied?[4] | | Consent | |
| Please explain reasons for the above choice: | | | |
| The SGC registry project includes components, the collection of which necessitates obtaining consent:<br>- The collection of patient reported outcomes(directly from patients)<br>- The access to existing imaging and biological and histological samples. | | | |

[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.<br>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<br>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):<br>Mr Jeremy McMahon<br>Consultant Maxillofacial Head & Neck Surgeon \| BAOMS Caldicott Guardian<br>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)* | |
| Fabien Puglia<br>BAOMS Project Manager<br>Data Security Awareness Level 1 (07/11/2022)<br>'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.<br>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. |

System or Info Security summary

| | |
|---|---|
| Does the system use cloud technology? | Yes |
| Access control<br>including guests, regular users, administrators or super users, etc. | Yes |
| Password complexity | Yes |
| Automatic user suspension | Yes |
| Auto-log-off or screen lock function | Yes |
| Remote access capability | Yes |
| Audit trail<br>including read/view access; creation/modification/deletion of data; import/export of data from removable media | Yes |
| Automated retention rules within the system | |
| Data deletion relating to a data subject request | Yes |
| Encryption Facilities<br>including server, database, email, file, removable media etc. | Yes |
| Network security management (Cloud considerations) | Yes |

| | |
|---|---|
| Penetration Tests for external-facing systems | Yes |
| External communication capability | |
| Data recovery / Business Continuity | Yes |
| Emergency Access ('Break glass' feature) | |
| Malware Protection/Detection | Yes |
| Privacy and security monitoring and reporting function | Yes |
| Security incident response plan | Yes |
| User education and training | Yes |
| Health data integrity and authenticity | Yes |
| Storage (for pyshical record) | Yes |
| UKCA or CE marking | Not applicable |
| Cyber Security Product Upgrades for third party systems<br>Who has the ability to install/upgrade the system's security patches: IT service desk staff; TP staff with physical on-site access or remote access? | Yes |
| If transferring/sharing information, which route is in use? | Secure file transfer |
| Are there any additional security being applied to the personal data? Encryption, password protection, phone confirmation, etc. | No |

## 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.)* | (1) Barts Cancer Research UK Centre Queen Mary University of London for storage<br>(2) Dr Fabien Puglia, Project manager<br>(3) Anonymised 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. |
| **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.<br>• 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.<br>• Access to the database is through individual login (unique username and password) and 2-factor authentication is in place.<br>Access is managed centrally by the project manager.<br>• 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.)* | All transferred dataset will be anonymised and 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?**<br>*Job role, organisation.* | Fabien Puglia, Project Manager, BAOMS |
| **How will accuracy of the data be assured?**<br>***What processes are in place to assure good data quality?*** | 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?**<br>*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?**<br>*This should align with the Trust's retention schedule.* | 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?**<br>*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?**<br>*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

| | |
|---|---|
| **Who will you be consulting with?** | Patients and Staff |
| **How were individuals consulted?** *(e.g. meetings, surveys, focus groups, patient panels, professionals.)* | The SGC registry was developed by a Working Group<br>An online meeting was organised with a group of 9 patients from the Salivary Gland Cancers UK patient group. Ahead of the meeting, the group was provided with the SGC registry protocol (including patient leaflet and consent form) to read in preparation. |
| **What concerns have been raised and how are these being addressed?** *(e.g. invasion of privacy, risks etc.)* | |
| The concerns raised by the group were around:<br>- The aims of the registry to make sure that the data would be used to improve quality of care and support the development of guidelines<br>- Outreach: to make sure that both patients and clinicians are aware of the registry to be able to contribute. The SGC registry should be a multidisciplinary project and not limited to OMF surgeons.<br>- Secondary benefits: to promote the public and clinicians' awareness of the conditions.<br>- Content: to make sure that all cases are captured along with all the necessary relevant information<br>The SGC Working Group has tried, where possible, to address those issues and include these suggestions in the SGC registry.<br>The patient group understood the aim of the registry and the need to collect information. The group was also happy with the data collection arrangement and o particular concerns around invasion of privacy, risks were raised. | |

## 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.<br><br>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 |
| *Note: For England only, the SGC registry does NOT need to comply with national data opt out.* | |

## Risk assessment

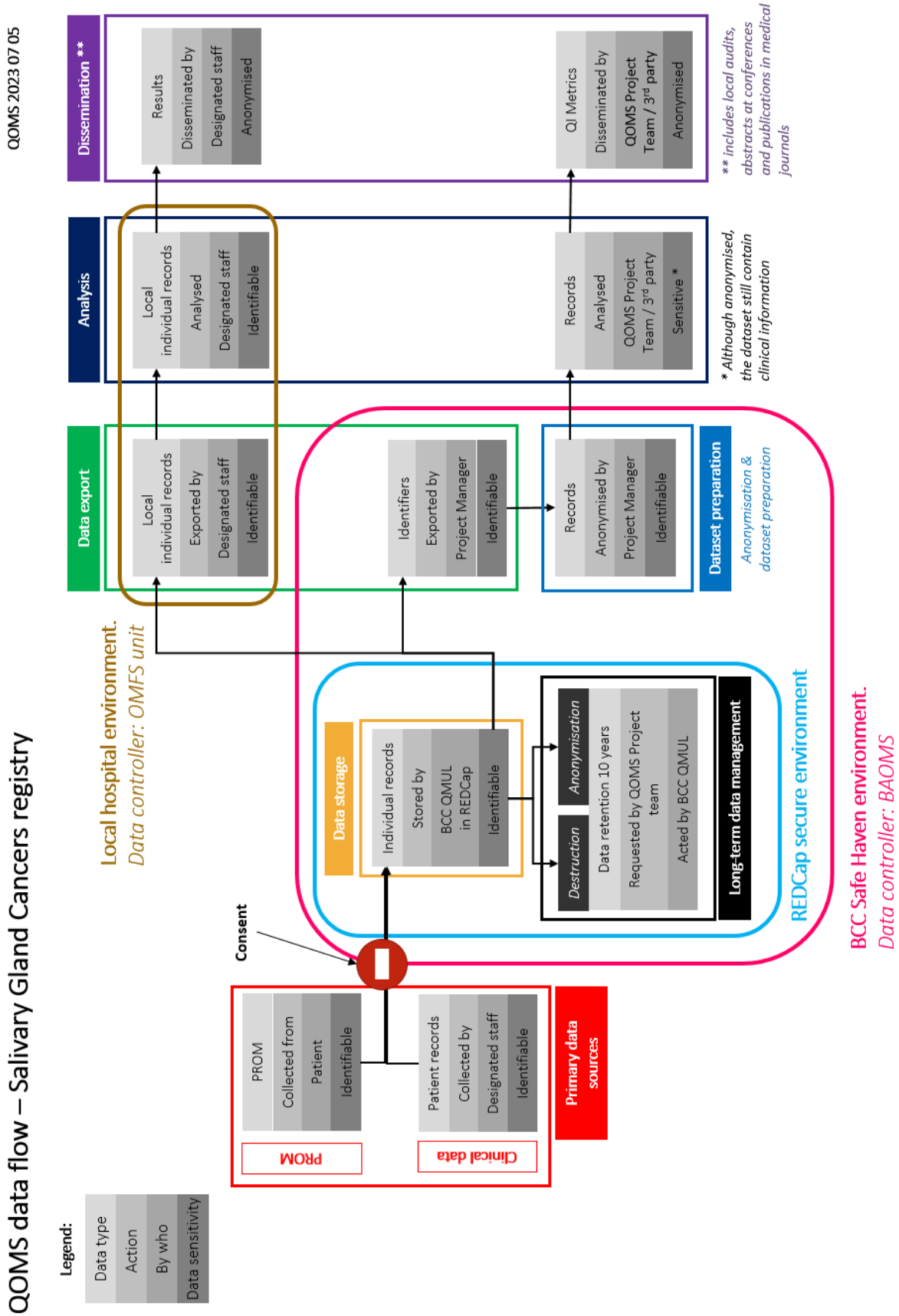
The level of risk is scored out of 25. A score of 0-5 is attributed to both the impact on the rights and freedoms of the individual, and the likelihood of those rights and freedoms being compromised. The two scores are then multiplied to create the composite risk score using the risk matrix below. This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

Appendix. Data flow