Data Protection Impact Assessment

Step 1: Identify the need for a DPIA

Explain broadly what project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.

The British Spine Registry is a clinical database which keeps a record of patients diagnosed and treated by spinal surgeons in the United Kingdom (the 'Registry').

The Registry commenced in 2011. Prior to 2016 entering patients diagnosed and treated by spinal surgeons was voluntary. However, in 2016 usage of a registry was mandated as part of a contractual obligation to commissioners for all spinal surgery in the UK. The Registry therefore now fulfils a regulatory requirement.

The Registry contains identifiable personal information including the name, date of birth and address along with clinical information about the patient, including past medical history, spinal diagnosis and spinal treatments.

The type of processing comprises the following:

- Personal information initially being entered to the Registry by hospital-based practitioners including surgeons and administrative staff. Only administrative staff who have been delegated administrative rights by the clinician responsible may enter or view such data.
- Clinical information regarding the outcome of treatments in the form of patient reported outcomes scores (known in the profession as PROMS) is entered both by patients and hospital staff.
- Consent to add a patient to the Registry is obtained from the patient as part of the process of collecting this clinical outcome data.

There are great benefits to collecting this data. It is as stated a regulatory requirement, but the Registry has value because:

1. Individual surgeons use the Registry to keep an accurate record of their clinical activity and the outcomes achieved. Recording such data is essential for the surgeons' professional revalidation.
2. The data contained on the Registry may be used for clinical audit or research purposes. It is anticipated that the data will be used to measure and compare variation in clinical outcomes between surgeons so as to identify clinical outliers (both positive or negative). This may help improve clinical outcomes.
3. The data may also be used to identify whether different medical procedures used for the same clinical conditions are associated with better or worse clinical outcomes. Patient care in the United Kingdom may therefore meet the best standards because the Registry can yield valuable evidence.

Step 2: Describe the processing

Describe the nature of the processing: how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or other way of describing data flows. What types of processing identified as likely high risk are involved?

The data is collected, used, stored and deleted as follows:

1. The clinician decides to enter a patient onto the Registry. This is usually after a decision is made to operate on that patient although some clinicians save data on patients not planned for surgery.
2. The clinician or administrator obtains either written or verbal consent from the patient for their personal data including their email to be entered onto the Registry. A clear and unambiguous privacy policy is given to all patients as part of this process.
    i) If the patient's written consent is obtained then that consent is recorded as GIVEN by the administrator.
    ii) If the consent, though given, is NOT RECORDED then the patients personal information is stored for 180 days and then automatically anonymised.
    iii) If consent is NOT GIVEN by the patient then all personally identifiable data is anonymised but a clinical record of diagnosis and treatment is retained.
3. All patients who have an email address are contacted by email once registered and asked to confirm consent electronically.
4. Once a patient is registered on the system the clinician or his delegates are able to enter clinical information regarding diagnosis and treatment including complications.
5. At various timepoints, pre- and post-treatment, patients are contacted either by email or post and asked to update their clinical outcomes (PROMS).

The process of removal of a patients' data is as follows but is slightly complicated by virtue of the historic process of collecting such data.

This is because since the Registry commenced, the recording of consent has been incomplete.

However, a strategy for correcting this has been implemented. From 16th June 2018 all personal data for patients for whom consent is either NOT GIVEN or WITHDRAWN will be anonymised. From 31st October 2018 all patients whose consent is NOT RECORDED will be anonymised if they have been on the Registry for over 31 days.

All patients may ask for anonymization of their data at any time. Instructions on how to do this are available on the Registry website and also set out in the privacy policy.

Describe the scope of the processing: what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?

The data scope of the processing of the data collected on the Registry, is detailed above. The geographical area of the data held on the Registry is national.

The data held on the Registry does take the form of special category data in that it comprises clinical data. In addition, the Registry enables a data analysis facility so that by using the Registry, individual clinicians are able to run reports on their own patient group at any time in any way that they choose.

However, there is a carefully prescribed process for search of the Registry.

Searches which cover the whole national database may only be performed with the approval of the British Association of Spinal Surgeons executive.

For a national search of the Registry to be performed there is an application template (see appendix) which must be completed and sent to the BSR clinical leads (Mr David Bell and Mr Robert Lee). Those individuals then submit the application to the BSR executive committee for approval. All national data for analysis is anonymised.

Data is only held on the Registry as long as necessary to fulfil the regulatory and patient outcome objectives detailed above.

Describe the context of the processing: what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?

The nature of our relationship with the individuals is as described above.

The patients have ultimate control in that their consent is sought before processing.

The patients would expect us to use their data in this way and the purpose of the processing is made clear in the consent they are asked to provide.

Patients do include children and other vulnerable groups but the safeguards detailed in this Assessment demonstrate how their insterests are secured. Clearly a parent or other guardian signs any necessary consent in this instance.

The processing benefits from IT security which represents the current state of technology in this area.

We are very aware of general public concern in the context of personal data security, particularly in the healthcare sector, and we have factored this in the steps we have taken.

Describe the purposes of the processing: what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for you, and more broadly?

The intended effect on the patients and surgeons is as detailed above, together with the benefits of the processing.

Step 3: Consultation process

Consider how to consult with relevant stakeholders: describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?

The privacy impact assessment (PIA) will be shared with the British Association of Spinal Surgeons executive and also with a sample group of ten patients.

The privacy notice and PIA will be reviewed by a solicitor with expertise in data law and the General Data Protection Regulation (GDPR) to ensure that it meets the published guidance issued by the Information Commissioner's Office.

Once so reviewed, it will be published on the BSR website.

A copy of the privacy policy will be emailed to all BSR clinicians, delegates and patients. The privacy policy will be available upon logging in to the BSR .

Step 4: Assess necessity and proportionality

Describe compliance and proportionality measures, in particular: what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?

The lawful basis for processing is legitimate interests. The processing does achieve our purpose. It is not considered there is an alternative way to achieve the same outcome. Data minimization and quality is assured because we only seek the essential core data as described above. Our privacy policy – together with the consent form demonstrates how we support patients rights. There is no international transfer of the data.

Step 5: Identify and assess risks

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.

The source of risk and nature of potential impact on individuals varies according to the category of the individuals.

Risk	Likelihood of harm	Severity of risk	Overall risk
Risk to surgeons	Remote / Possible / Probable	Minimal / Significant / Severe	Low / Medium / High
Benchmarking and outcome stratification may identify performance outliers. It is essential that prior to any form of outcome analysis that the data set is complete and validated.	Remote	Significant	Medium
Being identified as a negative clinical outlier is likely to be associated with considerable emotional stress	Remote	Significant	Medium
Risk to patients			
Inadvertent data breaches could result in patient clinical information being published	Remote	Significant	Medium
Appropriate management of outcome data could result in identification of adverse clinical outcomes related to an individual surgeon or hospital. Patient will need to be notified of this.	Possible	Significant	Medium
Risk to organisations			
BASS/Amplitude Clinical Solutions– reputational and financial risk of potential legal action taken by a surgeon or patient due to data breach or mishandling	Remote	Severe	Medium

Step 6: Identify measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5

Risk	Options to reduce or eliminate risk	Effect on risk	Residual risk	Measure approved
		Eliminated / Reduced / Accepted	Low / Medium / High	Yes / No
Identification of underperforming surgeon				
The solution is: a. The implementation of a Data validation policy to be agreed by BSR committee. The timeline for implementation is April 2019. b. Registration with HQUIP to ensure appropriate framework for outcome assessment risks c. BSR to agree escalation policy for clinical outliers. Points ii) and iii) are scheduled to be implemented by April 2019		Eliminated	Low	Yes
Malicious or inadvertent data breach releasing patient clinical information				
a. Ensure that all patients' identifiable data is consented for. Scheduled for implementation in June / October 2018 b. Ensure appropriate data security is in place at Amplitude Clinical Services Ltd Scheduled for implementation in September 2018 c. Ensure that surgeon users are aware of risks of saving or exporting patient sensitive data Scheduled for implementation in September 2018		Eliminated	Low	Yes

Step 7: Sign off and record outcomes

Item	Name/date	Notes
Measures approved by:		Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:		If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:		DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice: Maintenence of the Registry inevitably carries a risk to personal data and given the clinical character of the personal data the risks are understood to be greater. However those risks have been carefully identified and steps taken to meet the same such that it is believed adequate compliance is in place or scheduled for full implementation in accordance with the timelines set out in this Assessment.		
DPO advice accepted or overruled by:		If overruled, you must explain your reasons
Comments:		
Consultation responses reviewed by:		If your decision departs from individuals' views, you must explain your reasons
Comments:		
This DPIA will kept under review by:		The DPO should also review ongoing compliance with DPIA