Privacy Impact Assessment for REDCap

1. Introduction

Will you be sharing information with another organisation (for example a system supplier)?
No data will be shared with other organisations at the system level.
Within the context of a project, de-identified only data may be shared with other organisations, if a project has the required approvals to do so.

If you are procuring new software does it allow you to amend data when necessary?
Yes, REDCap is a data capture system. Data will be entered into REDCap and can be amended. An audit log is maintained when data are manipulated.

How are you ensuring that personal data obtained from individuals or other organisations is accurate?
Project teams are responsible for accuracy of direct data entry.
The Digital Research Environment (DRE) are responsible for quality of data feeds from EPR.

What retention periods are suitable for the personal data you will be processing?
Retention periods will be specified on a project-by-project basis according to R&D approval documentation.

Are you procuring software which will allow you to delete information in line with your retention periods?
REDCap can archive or delete research projects.

Will the systems you are putting in place allow you to respond to subject access requests more easily?
REDCap can provide the information stored in the system. If data are not captured in EPR, then project teams may be required to support subject access requests for additional data.

If the project involves marketing, have you got a procedure for individuals to opt out of their information being used for that purpose?
N/A

Do any new systems provide protection against the security risks you have identified?
Yes with de-identification of data before use and role based data access.

What training and instructions are necessary to ensure that staff know how to operate a new system securely?
Project teams will be given pointers to learning materials (including videos, documents and web info) that are provided by the REDCap community. The DRE team will offer weekly user support sessions on anything related to REDCap.

Will the project require you to transfer data outside of the EEA?
REDCap servers will be hosted within GOSH. Data transfers outside of GOSH for research projects would be reviewed as part of the R&D approval process.

If you will be making transfers, how will you ensure that the data is adequately protected?
Project data transfers should be done according to the conditions described in their R&D approval documentation.
REDCap provides a number of controls around data export, such as, controlling ability to export data and providing option to de-identify data for export, both based on user role permissions.

How will individuals be told about the use of their personal data?

Projects would need to have individual consent for any identifiable data used for research.

If you are relying on consent to process personal data, how will this be collected and what will you do if it is withheld or withdrawn?

Projects would collect individual consents for the use of personal data, which would be documented as required by the R&D governance process for approval.
Since REDCap is a data capture system, if an individual withdraws consent, the assumption is that they would stop providing any further data directly to the study. The DRE would need to be informed of any individuals who withdraw their consent. If data feeds from EPR have been set-up, the DRE would then exclude those individuals from the data feeds.
Since REDCap is a data capture system, we expect that individual consents would be required for all research studies that use it and CAG support would not be applicable to REDCap.

Have you established which conditions for processing apply?

Legal basis for processing personal data for research:

- **'Task in the public interest' 6(1)(e) for research**
- **Processing of special categories of data 9(2)(j) for research provided certain safeguards are met to protect the rights and freedoms of data subjects**

Have you identified the social need and aims of the project? Are your actions a proportionate response to the social need?

N/A

Have potential new purposes been identified as the scope of the project expands?

N/A

2. Information Flows

In total, three REDCap servers are being set-up (Figure 1):

1. A REDCap **Test** server (1) for testing and to manage upgrades going forward.
2. A REDCap **Private** server (2) that will primarily be used for GOSH-only studies. It may be used for GOSH-led multi-site studies ONLY IF a project has the required governance approvals to do so within the supported environment. It will be accessible only by staff with a GOSH user account.
3. A REDCap **Public** server (3a and 3b) that will be used for GOSH-led multi-site studies. It will be accessible by external users.

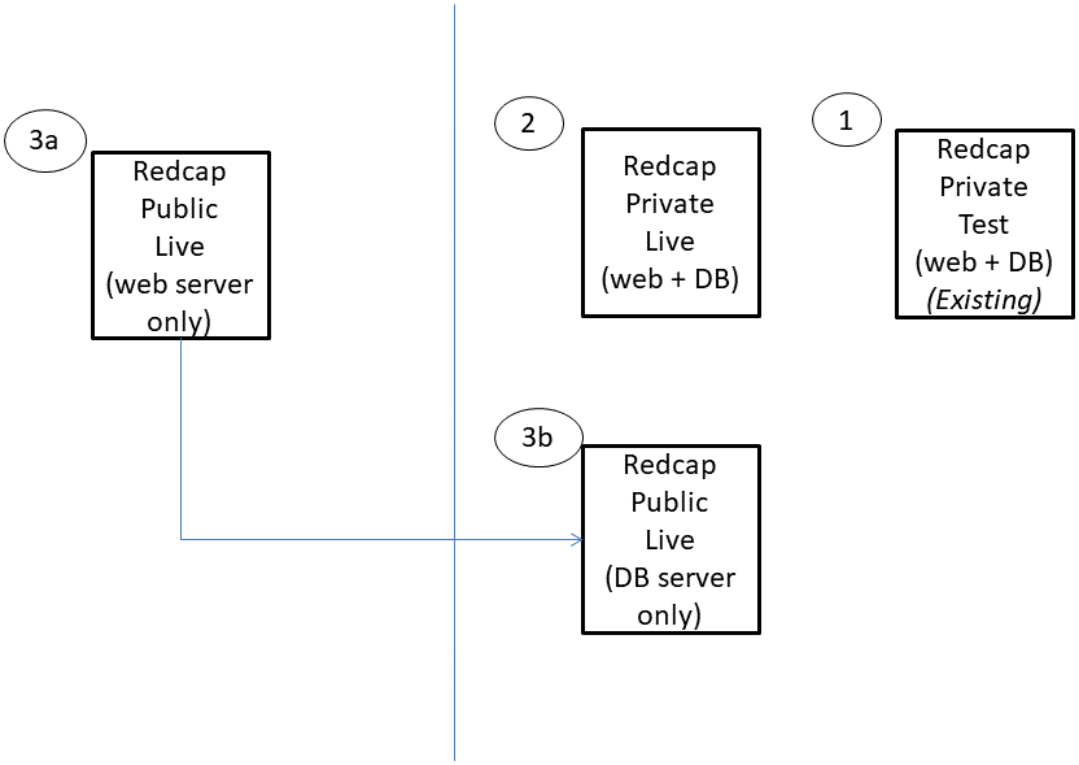

Figure 1: REDCap architecture

4. Privacy and DPA Compliance Risks

These will be managed by the Research Data Access Group (Chaired by The Caldicott Guardian), to oversee all governance issues.

Identify the privacy risk		Identify privacy solutions			
Privacy issue	**Risk (to individuals, compliance or organisation)**	**Solution**	**Action to be taken**	**Action Lead**	**Action Status**
Consent	Relying on consent to process personal data, how will this be collected and what is the process if it is withheld or withdrawn?	Projects should collect individual consents and document process as part of R&D approval. Consent for GOSH patients may need to be recorded in EPIC's clinical trials module. The DRE should be informed of consent withdrawals.	DRE to record evidence of R&D approval. Project team and DRE team responsibilities to be defined in REDCap SOP. Project, EPIC and DRE teams to agree on consent management process.	DRE	
Consent	Communications with patients to inform them how their data will be used	Projects should manage communications with participating patients as per their R&D approval documentation.	DRE to record evidence of R&D approval. Project team and DRE team responsibilities to be defined in REDCap SOP.	DRE	
Data Transfer	Ensuring safe/ adequately protected transfer of data. For example, outside of EEA or to external suppliers	Project related data transfers should be done according to conditions described in their R&D approvals. Data export controls to be applied based on user role permissions.	DRE to record evidence of R&D approval including information on permitted external data transfers. Project team and DRE team responsibilities to be defined in REDCap SOP.	DRE	
Security	Does the system provide protection against the security risks identified	The system supports data de-identification and role based data access. Projects are responsible for defining user permissions according to documentation in their R&D approvals. Only de-identified data should be loaded on the Public REDCap server for multi-site de-identified data studies.	DRE to record evidence of R&D approval. DRE to assign project admin role to project PI or nominated user who would be responsible for managing project-level user permissions according to R&D approval documentation. Project team and DRE team responsibilities to be defined in REDCap SOP. DRE to carry out an annual audit of the Public REDCap server to assess if identifiable	DRE	

			data have been included contrary to the governance for that server. Up to five studies would be selected at random for the audit. Risk to be added to REDCap risk log and reviewed by RDAG annually.		
Data Quality	Ensuring that personal data obtained from individuals or other organisations is accurate	Project teams are responsible for the accuracy of the data that they directly enter into their project space. If a project requires data from EPR, then the DRE will provision that data and ensure data quality is maintained during transfer from EPR. Data feeds will be automated over time. Data quality is also subject to EPR data quality.	DRE to gradually automate data flows from EPR. Risk to be added to REDCap risk log and reviewed by RDAG annually.	DRE	
System	Retention periods are suitable for the personal data being processed	Retention periods will be defined on a project-by-project basis according to R&D approval documentation.	DRE to record evidence of R&D approval including information on retention periods. Risk to be added to REDCap risk log and reviewed by RDAG annually.	DRE	
Anonymisation	The risk to study participants of re-identification by users who should not have access to identifiable information	Projects should have R&D approval including information on capturing study participants identifiable information, anonymisation and appropriate user access. Project teams are responsible for ensuring capture of identifiable data by appropriate project team members. Project teams are responsible for appropriate anonymisation of the data that they directly enter into their project space where required. Only de-identified data should be loaded on the Public REDCap server for multi-site de-identified data studies. If a project requires data from EPR, then the DRE should follow the same data request and approval process as for the DRE research platform, which includes risk assessment for re-identification.  Draft project application process.p	DRE to record evidence of R&D approval including information on identifiable data items. Project team and DRE team responsibilities to be defined in REDCap SOP. DRE to carry out an annual audit of the Public REDCap server to assess if identifiable data have been included contrary to the governance for that server. Up to five studies would be selected at random for the audit. Risk to be added to REDCap risk log and reviewed by RDAG annually.	DRE	

		Only appropriate staff will be able to extract data from EPR.			
Access rights	The system may be accessed by staff who shouldn't or no longer have a right to see it	Projects are responsible for defining user permissions according to documentation in their R&D approvals. Specified members of the DRE team will have system and project admin rights. DRE should ensure that DRE team members access remain up-to-date with starters and leavers.	Process for updating DRE team members' access to be defined in REDCap SOP.	DRE	
Information Ownership	If the system does not have an owner there is the risk of no accountability for issues or breaches around the system and its use	An Information Asset Owner to be appointed (and Information Asset Administrators as appropriate). This member of staff will record the asset on the Trust asset register and all information flows related to it. Additionally they will manage any information risks or breaches for the system.	CRIO is the IAO.	CRIO	

5. Consultation and Sign Off

The Research Data Access Group (RDAG) is being consulted about this PIA. RDAG members include:

- Caldicott Guardian
- Chief Research Information Officer
- Information governance manager
- R&D research governance leads
- DRE lead

The ICT security and governance manager has reviewed this PIA.

To be completed:

This PIA has been signed off by the Caldicott Guardian and formally approved by RDAG on 29 January 2019.