**Shared Health and Care Analytics (SHcAB) Board**

**Policy and Operating procedures**

|  |  |
| --- | --- |
| Document Name: | SHcAB  Policy and operating procedures |
| Version: | 1.7 (11th May 2021) |

**Document revision history**

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Revision | Author |
| January 2021 | 1 | Document created from SHcAB joint Controllers Operating procedures | Helen O’Neil, Head of Corporate Governance and DPO, Kent & Medway CCG |
| 12/02/2021 | 1.3 | Reviewed by SHcAB representatives at weekly IG group | SHCAB reps |
| 17/02/2021 | 1.4 | Reviewed by HO’N following comments in preparation to send to organisations for review and approval | Helen O’Neil |
| 18/02/2021 | 1.5 | Reviewed by Latifa Aina, GP Data Protection Officer and updates made | Latifa Aina, GP data Protection Officer, K&M CCG/Helen O’Neil |
| 18/02/2021 | 1.6 | Corrections and comments made | Abraham George, Assistant Director / Consultant Public Health & Educational Supervisor |
| 04/03/2021 | 1.6 | Comments and revisions | Debbie Adey, IG Compliance Manager  Kent Community Health NHS Foundation Trust |
| 10/05/2021 | 1.7 | Final revisions and corrections | Adam Tuckett, South Central and West Commissioning Support Unit/Helen O’Neil |

**Document Approval:**

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Committee Group | Comments |
| 17/05/2021 | 1.7 | Shared Health and are Analytics Board |  |

Contents

[1. Introduction 4](#_Toc64463126)

[2. Purpose 5](#_Toc64463127)

[3. Agreement governance and administration 6](#_Toc64463128)

[Schedule A – Operational management of the SHcAB JCA 10](#_Toc64463130)

[Schedule B – Procedure for reviewing and approving access to Jointly Controlled Data 12](#_Toc64463131)

[Schedule C - Communications and Engagement procedure 19](#_Toc64463140)

[Appendix A – SHcAB Terms of Reference 20](#_Toc64463141)

[Appendix B - The Information Governance and Data Access Group (Triage and Panel) Terms of Reference 21](#_Toc64463142)

[Appendix C - Application form and checklist for new organisations (On-Boarding Process for the SHcAB Joint Controllers Agreement) 25](#_Toc64463144)

[Appendix D – Conformation of Joining letter 29](#_Toc64463145)

[Appendix E – Schedule of Joint Controllers (The Parties) 31](#_Toc64463146)

[Appendix F – The Processors. 33](#_Toc64463147)

[Appendix G - Pseudonymised Data Access Request Form 34](#_Toc64463148)

[Appendix H - SHcAB Data Protection Impact Assessment 37](#_Toc64463149)

[Appendix I – Triage checklist 48](#_Toc64463165)

[Appendix J – Data Access Contract 51](#_Toc64463166)

[Appendix K – Template Privacy Notice 61](#_Toc64463274)

# Introduction

* 1. **The SHcAB**

The SHcAB directs joint health and care data analytics, research and population health management projects within the over-arching governance of the Kent and Medway Integrated Care System (ICS) , to whom it is accountable through both the Programme and Clinical and Professional Boards. The SHcAB was established on a formal basis within ICS (previously STP) programme governance in September 2018 with the purposes of the group agreed as:

* Inform the planning, implementation and evaluation of population health strategy on behalf of the Kent and Medway ICS and its work streams.
* Support the ICS in the delivery of projects, particularly around data and analytical requirements.
* Lead the use of data to improve the lives of Kent and Medway residents, generating a national reputation for excellence in analytics.
* Create a robust and flexible framework to maximise the completeness, accuracy and validity of patient and citizen information for the benefit of Kent and Medway residents and the health and care organisations who serve them.
  1. **SHcAB Joint Controllers Agreement**

The use of data for purposes other than direct care is rightly subject to strong control. Where two or more data controllers jointly determine the purpose and means of processing, they are Joint Controllers. This requires an arrangement between the joint controllers that ensures individual rights and freedoms are protected and set out how the arrangement is managed.

The SHcAB Joint Controller Agreement establishes the collaborative governance needed to provide a fair, lawful and transparent framework for the co-ordination of joint processing of health and care data (The Jointly Controlled Data) for the following Agreed Joint Purposes:

(a) Planning, implementing and evaluating population health strategy

(b) Managing finances, quality and outcomes

(c) Risk stratification for early intervention and prevention

(d) Co-ordinating and optimising patient or service user flows

(e) Undertaking research

(f) Public Health

* 1. **KERNEL**

The Kent Research Network for Education and Learning (KERNEL) is the new linked health and care population dataset for Kent & Medway developed by the HISBi Data Warehouse team, building on the success of the Kent Integrated Dataset (KID). The KERNEL encompasses pseudonymised linked data from health & care organisations in Kent.

Pseudonymised data will always be the output. Re-identification will only take place in very exceptional cases where there is duty of care to do so e.g. detection of previously undiagnosed disease or adverse outcome in patients undergoing clinical trials. Applications for access to such data will undergo further assessment by the Database Access Committee and wider SHcAB group where necessary.

* 1. **KID**

The KID is a person level data linking routinely collected administrative activity and cost data from almost all NHS providers across Kent and many non NHS organisations from April 2014. The KID stopped receiving regular data flows from local providers as of April 2019. It is now currently a static pseudonymised dataset only capable for historical analyses and no RE-ID function. However, this remains a valuable information asset that has potential to generate much more insights into our population health.

# Purpose

This policy and associated operating procedures set out how the SHcAB will meet its responsibilities set out in the JCA to ensure that robust governance and assurance mechanisms are in place. This includes:

* 1. **Standard Operating Procedures**

|  |  |  |
| --- | --- | --- |
| REF | SOP NAME | SOP PURPOSE |
| Schedule A | Procedure for the management of the SHcAB agreement | * + Effective due diligence and on-boarding of new Joint Data Controllers   + Annual due diligence and assurance of existing Data Controllers   + Maintenance of the schedules – joint controllers and processors |
| Schedule B | Procedure for reviewing and approving access to Jointly Controlled Data | * + Reviewing applications for access to Jointly Controlled Data necessary for specific projects and activities.   + Completion of Data Protection Impact Assessments for each Agreed Joint Purpose, activity or project. |
| Schedule C | Communications and Engagement procedure | * + Publishing and maintaining a web presence to communicate the SHcAB’s agreed joint purposes and describe the activities and projects undertaken in furtherance of those purposes together with associated documentation.   + Citizens panel   + Social media campaigns. |

* 1. **Template documents and terms of reference**

|  |  |
| --- | --- |
| REF | NAME |
| Appendix A | The SHcAB terms of reference |
| Appendix B | The Information Governance and Data Access Sub-group and Panel terms of reference (including the Information Governance and Access Triage group terms of reference) |
|  |  |
| Appendix C | Application form and checklist for new organisations (On-Boarding Process for the SHcAB JCA) |
| Appendix D | Confirmation of joining letter (joint controllers) |
| Appendix E | Schedule of the Joint Controllers |
| Appendix F | Schedule of Processors |
| Appendix G | Pseudonymised Data Access form (KID and Kernel data) |
| Appendix H | Data Protection Impact Assessment (DPIA form |
| Appendix I | Triage Checklist |
| Appendix J | Template Contract (Data Processing Agreement (DPA)) |
| Appendix K | Template Privacy Notice |

# Agreement governance and administration

This section describes the roles and responsibilities of the four main structures contributing to the process of operational management of the SHCAB JCA. It includes:

* + - The SHCAB - see Appendix A for Terms of Reference;
    - The IGDA Sub Group (Panel and Triage) - see Appendix B for Terms of Reference;
    - The Caldicott Guardian,
    - The Data Protection Officer; and
    - The Project Manager.
    - Administrative support
  1. **The SHcAB**

The SHcAB shall exercise the following responsibilities:

1. Governance, oversight and assurance of the JCA and its Schedules for and on behalf of the Parties.
2. Amendment of the JCA following annual review recommendations or at other times as required maintaining its fitness for purpose.
3. Nominating or appointing a Caldicott Guardian and Data Protection Officer Designate from the membership to fulfil the duties set out in below.

The SHcAB is accountable to the ICS Programme and Clinical and Professional Boards.

For the purposes of this Agreement:

|  |  |
| --- | --- |
| The DPO Designate is | INSERT NAME |
| The Caldicott (Privacy) Guardian Designate is | INSERT NAME |
| The Project Manager is (also acting as the agreement administrator) | INSERT NAME |

* 1. **The Information Governance and Data Access (IGDA) Sub-group**

The IGDA subgroup is accountable to the SHcAB, and will provide support by making recommendations and providing guidance to assist the development of safe and secure data flows and access to the KID and KERNEL systems for the agreed joint purposes as set out within the SHcAB JCA. The sub group will oversee the operational management of the standard operating procedures. Terms of reference are included at Appendix B.

The group is responsible for recommending to the SHcAB whether applications for access to data should be agreed. Applications for access to data are forwarded to the SHcAB to note and to provide a means to object.

The sub group will sit monthly, on the first Friday of every month. In the case of a bank holiday, the sub group will sit on the following Friday.

Members of the sub group will be drawn from a pool of suitably qualified and experienced members which includes:

* Caldicott Guardian (Chair)
* Data Security and Protection Leads
  + Data Protection Officer
  + IG lead – Primary Care
  + IG lead – Provider Trust
* Clinicians
* Consultants in Public Health;
* Analytics/BI Representatives
* Kent and Medway R&I Manager or equivalent
* Appropriate CCG representatives and/or commissioning representative
* Academic Representative
* Patient representative
* SHcAB Project Manager

Members must have attended induction training to ensure that they are fully familiar with the SHcAB JCA and associated policies and operating procedures and will ensure that they have completed the NHS data security and protection training. In addition, those with specialist roles (Caldicott Guardian and Data Protection Officer) will be required to complete specialist data security and protection training suitable to their role. The SHcAB Project Manager will keep a log of training completed which will be made available to the SHcAB and joint controllers on request.

* There will be a quorum and meetings will go ahead as long as the following members can attend
* Chair / Caldicott Guardian
* DPO and 1 IG lead
* At least 1 PPI member
* At least one Clinician
* At least one BI/Analytics representative

It is legitimate for one individual (other than the lay person) to “wear two hats”. As far as practical, the combination of members should be selected to provide a good range of perspectives and relevant skills. The sub group may call for specialist advice as appropriate.

## Conflict of Interest

Conflict of interest means any activity, commitment, or interest that may adversely affect, compromise, or be incompatible with the obligations of a sub group member. It includes but is not limited to situations where a significant financial or other interest could affect a sub group member’s judgment.

Members should be required to declare their interests before joining the sub group and a register will be kept by the Project Manager. All members will also be required to update their declaration on an annual basis. The Chair, supported by the Project Manager will be in a position to bear these in mind when organising Panels. As an additional safeguard, at the beginning of every meeting, the Chair should require any member to declare any relevant interests. Anyone declaring any interest may, depending on the nature of the interest be required by the Chair not to take any part in any discussion or outcome of the application to access data.

* 1. **Data Protection Officer Designate**

The Data Protection Officer Designate shall perform the following duties for and on behalf of the SHCAB:

1. Offer independent opinion and advice on UK GDPR compliance with respect to SHCAB Joint Controller processing operations.
2. Monitor compliance during the lifecycle of each project or activity and consider the risks of associated processing operations.
3. Review the JCA on an annual basis and propose improvements.
4. Act as a contact point for matters relating to processing of Jointly Controlled Data.
   1. **Caldicott (Privacy) Guardian Designate**

In respect of processing of Jointly Controlled Data for any project or activity in pursuance of the Agreed Joint Purposes, the Caldicott (Privacy) Guardian Designate shall:

1. Consider its necessity and proportionality.
2. Apply the Caldicott Principles.
3. Consult and take into consideration the opinions of organisational Caldicott Guardians and IG leads of the Joint Controllers.
4. In accordance with the Common Law Duty of Confidence (CLDC), ensure the nature and extent of processing does not exceed the ‘reasonable expectations’ of a ‘reasonable person’.
5. Approve or decline projects and activities on the basis of the diligence described above.
6. In accordance with UK GDPR Art. 9(3) the Caldicott Guardian Designate is the UK GDPR Art.9(3) ‘responsible health professional’ for processing undertaken for the Agreed Joint Purposes and accordingly must be a registered health professional as defined in the Data Protection Act 2018 s204.
   1. **Project Manager (and agreement administrator)**

The Project Manager shall manage appropriate approvals for new and change processing operations involving Jointly Controlled Data and shall also administer and update the Agreement for and on behalf of the SHcAB and the Joint Controllers. Specifically, the Agreement Administrator shall:

1. Manage applications and maintain the integrity and accuracy of the Schedules.
2. Maintaining the smooth running of the Operating Model described in the schedules.
3. Maintain records associated with the execution of the JCA.
4. In compliance with UK GDPR Art. 30, ensure Records of Processing Activity (ROPA) are maintained for processing of Jointly Controlled Data.
5. Project manage any necessary pending IG approvals and / or authorisations essential to the smooth running of the operating model and linked dataset development eg. Data Access Request Service (DARS) applications to NHS Digital.
   1. Administrative Support

(a) Carry out administrative tasks as related to the remit of SHCAB including maintaining log of approved projects, declared interests register etc.

# Schedule A – Operational management of the SHCAB JCA

**On-boarding of Data Controllers**

On-boarding describes the process of a Data Controller joining the SHcAB JCA subsequent to its initial signing by founding Parties. Candidate parties may submit an Application Form (Appendix C) at any time to the Project Manager for consideration at the IGDA sub group. Confirmation of their inclusion in the Agreement shall be confirmed using the Confirmation of Joining template (Appendix E).

Prior to submission, the following actions shall have been completed:

* 1. The candidate party has received a copy of the Agreement and its Schedules.
  2. The candidate party completes the Application Form (Appendix C).

Process for review:

1. On receipt of an Application Form, the Project Manager shall consider the candidates application and seek clarification on any areas of assurance from candidate parties.
2. Following receipt of a complete application form the Project Manager will arrange for discussion at the next IGDA sub group as per the checklist at Appendix C.
3. The IGDA sub group review the application and agree whether adequate assurance is in place which would enable the party to meet the requirements of the SHCAB JCA.

**Annual assurance of existing controllers**

On an annual basis all existing parties to the JCA will be asked to confirm their compliance with the following areas and compliance will be reported to the SHcAB for assurance. As per the JCA, each party reserves its rights to inspect another party’s arrangements for the processing of Jointly Controlled Data and to terminate their participation in the Agreement or participation in a specific project where it considers that the one or more parties is not processing the Jointly Controlled Data in accordance with this Agreement.

|  |
| --- |
| Annual Assurance Check List |
| 1. The organisation must be registered with the Information Commissioners Office (ICO) and have a current Data Protection Registration Number |
| 1. The organisation must have published a Data Security and Protection (DSP) Toolkit self-assessment to provide assurance that they are practicing good data security and that personal information is handled correctly. |
| 1. The organisation has an up to date, publicly available Privacy Notice covering all the data processing relevant to the service. |
| 1. The organisation will ensure compliance at all times with obligations for NHS Information Security requirements to identify risks and incidents they have a responsibility to manage. |
| 1. The organisation must have implemented measures to ensure all IG incidents are reported in accordance with the NHS Digital Guide to the Notification of Data Security and Protection Incidents for reporting, managing and investigating Information Governance Serious Incidents |
| 1. The organisation must be compliant with the Data Protection Act 2018. If not already compliant with the Data Protection Act 2018, the organisation must have in place an implementation plan to be compliant and provide a statement of assurance that they will be complete during financial year 2019-20 |

# Schedule B – Procedure for reviewing and approving access to Jointly Controlled Data

1. **Overview**
   1. A member of the SHcAB or its wider ‘community of interest’ or a Party to this Agreement organisation may propose new projects as a sponsor.
   2. Activities differ from projects in that they describe processing for ongoing or business-as-usual purposes, e.g. patient-flow dashboards or periodic reports. These shall be determined by the SHcAB or mutually agreed between Parties to the JCA and are therefore not covered by this standard operating procedure.
2. **Principles**
   1. In furtherance of the Agreed Joint Purposes, candidate project proposals should focus on articulating how an activity or project:
   * Furthers the Agreed Joint Purposes.
   * Contributes to wider public benefit.
   * Meets UK GDPR/DPA 2018 requirements.
   1. All projects are expected to apply the PRINCE 2 methodology and to appoint a project manager to plan and coordinate the project in broad accordance with the SHcAB swim-lane diagram.
   2. All data will be pseudonymised, any Partners accessing pseudonymised dat are obliged not to seek to re-identify data, and not to use the data to identify any individual or make any decisions relating to any individual, unless authorised on an exception basis by the IGDA and / or Database Access Committee
   3. The IGDA Sub Group will ensure that the principles of the JCA are upheld, in that:
   * There is a lawful basis to process Jointly Controlled Data.
   * Data Protection Impact Assessments are completed for each Agreed Joint Purpose, activity or project.
   * Access to Jointly Controlled Data is restricted to authorised individuals on a ‘need to know’ basis only and subject to appropriate technical and organisation controls and sanctions.
   * Any additional technical and organisational measures necessary to secure data in transit and at rest for each purpose, project and activity are established.
   * Understanding how data flows from an organisation storing the data to the organisation(s) conducting analysis.
   * Ensuring data flows are appropriately managed and documented in accordance with UK GDPR Art. 30. (c).
   1. The SHcAB JCA requires five key conditions are met before patient information is processed for purposes other than direct care:

* Processing is fair, lawful, necessary and proportionate, and in accordance with the UK GDPRs seven data protection principles?
* People know who you are, how you use their data and are able to object?
* Processing is visible, open and transparent?
* Use of data is within the ‘reasonable expectations’ of a ‘reasonable person’?
* Controls respect privacy and protect confidentiality.

1. **Consultation and engagement with data controllers**
   1. Prior to a Party’s data being brought ‘into play’ for a candidate project or activity, their named contact shall be informed of the intent by email and provided with a DPIA, project proposal and the name of the project or activity sponsor.
   2. On receipt of the above documents the relevant Party(s) shall have 20 working days within which to respond.
   3. Parties have a right to object to the processing of data they provide into Joint Control for any candidate project or activity. Where they do so, they should provide an explanation or reason.
   4. It is envisaged that as projects must meet the purposes of the SHcAB JCA and UK GDPR/DPA 2018 requirements to receive approval by the IGDA Group, objections will be of a minimum. However, in the event that a party to the SHCAB JCA does raise an objection, or seek clarification, further information will be provided as soon as possible, but no later than five working days. In this instance all parties will seek to reach a resolution within 20 days of the objection or request for clarification being raised.
2. **Governance arrangements**
   1. The Project Manager, Data Protection Officer (Designate) and Caldicott Guardian (designate), shall have been consulted prior to the DPIA being issued to the controller(s), and the request for access shall be discussed and approved at the IGDA sub group.
   2. All requests for data access will be notified to the SHcAB to note the approval of data access and giving them a means to object prior to consulting with joint controllers.
   3. Figure 1 summarises the agreed procedure which is described in more detail in the step by step process below.

Project request form received by Project Manager, recorded on project log and forwarded to HISBi team to clarify data spec

Request form checked for completeness by Project Manager with consultation with DPO and Caldicott Guardian as required.

Request for not agreed – Sponsor/project lead notified of decision

Further information requested from sponsor/project lead as necessary

Request form reviewed by IGDA sub group virtually within 10 working days of receipt using triage checklist

Assigned for consideration at next available IGDA sub group (meets on a monthly basis) with sponsor/project manager invited to attend for discussion.

Request form agreed: Full data access form (including DPIA) sent for completion to project sponsor/project manager

Completed information received. Project Manager check for completeness and completes due diligence/assurance on the information received. Incomplete or missing information is requested back to project sponsor and manager

Meeting papers to IGDA sub group at least 3 working days in advance of meeting.

IGDA sub group meets and considers each application and evidence; and determines recommendation to SHCAB.

* Agreed
* Not agreed OR
* Defer – pending further information

Minutes of meeting; outcome and rationale written up within 5 working days of meeting.

Outcome communicated to SHcAB at bi-monthly SHcAB meeting.

Project sponsor and manager advised of decision and rationale in writing within 5 working days of meeting and next steps

**Figure 1: Data Access Review and Approval Process**

* **At**

Decision assigned for consideration at next SHcAB to note and means to object.

Meeting papers to SHcAB at least 3 working days in advance of meeting.

SHcAB meets and considers application and decision

**Object:** Project sponsor and manager advised of decision and rationale in writing within 5 working days of meeting and next steps

**Decision noted and no objection:**  Recorded in SHcAB minutes and project/data access log

Following reporting to SHcAB and engagement of Joint Controllers, template contract (inc DPA) is completed by Project Manager and forwarded to all parties for signature

Following receipt of signed contracts data access given

Step 1: Triage process

Note: Requests for data access to research studies/clinical trials (particularly where DEIF/REID of trial participants is required will be sent to the Database Access Committee for consideration

**Decision agreed**: Joint Controllers named contact informed of the intent by email and provided with a DPIA, project proposal and the name of the project or activity sponsor. On receipt of the above documents the relevant Party(s) shall have 20 working days within which to respond

Step 2: Review by Information Governance and data Access Sub Group

**Object:** Project sponsor and manager advised of decision and rationale in writing within 5 working days of meeting and next steps

Step 3: Reporting to SHCAB

Step 4: Engaging Joint Controllers

SHcAB website and project log updated to include project details steps

Step 5: Contracts and Data Access

Step 6: Comms

**Step 1 – Request received and triaged**

* 1. Only requests set out on the standard form, and providing all the required information, will enter into the process.
  2. The Project Manager, DPO and Caldicott Guardian where required, will be able to provide advice to requestors on how to complete the request form and about the review process.
  3. Initially, the Data Access (Appendix G) and DPIA form (Appendix H) should be completed and returned to the generic SHcAB email address [Kmccg.shcab@nhs.net](mailto:Kmccg.shcab@nhs.net)

## Check for Completeness

## The date of receipt will be recorded for all requests received. Within three working days of receipt of the form, the Project Manager will check the submission form and ensure:

* + - Appropriate parts of the form have been fully completed;
    - All supplementary documentation referred to is attached; and
    - The submission has been approved by a suitable representative of the requesting organisation.

The Project Manager will decide when the request is sufficiently complete to proceed to the next stage of determining whether the submission is appropriate for consideration by IG and Data Access triage group. The Project manager will also forward the request to the HISBi team to ensure that clarity can be sought on the data specification as required.

If the submission is not sufficiently complete the Project Manager will return it (and any accompanying material) to the requestor within 3 working days of receipt.

Within 10 working days of receipt, submissions will be triaged by the IG and Data Access Group. The role of the triage is to filter out applications which are not appropriate to be put before the IGDA sub group because the application should be determined through another process (e.g the Data Base Access Committee) or there is insufficient information to support the sharing of data based on UK GDPR/DPA compliance and/or the sharing does not been with the agreed purposes set out within the SHCAB JCA.

If the Triage Group rejects the application the Project Manager shall write to the requestor giving reasons for the decision.

* 1. **Redirection of Inappropriate Requests**

If the Triage Group decides that the request is classifiable as a request for data for research or clinical trial, then the request shall be forwarded to the to the Database Access Committee for consideration using this process.

Where the Triage Group do not refer an application to the IGDA sub group, the Triage Group shall record the reason the request was refused and direct the Project Manager to take the appropriate action. The Project manager will return the submission to the requestor within 6 working days of the Triage Group’s decision.

This will either advise that the request has been transferred to the Database Access Committee or that the request was refused, stating the reasons for this.

The Project Manager will maintain a record of transferred or refused requests, noting the

* + - date received, the date scrutinised, and the date returned;
    - reason why the request was refused; or
    - that the request has been transferred to the Database Access Committee.

Triage Group is conducted by members of the IGDA sub group. Terms of Reference are detailed in Appendix B.

## Step 2 – Review by IGDA sub group

## The Project Manager will open a file for each request approved by the Triage Group, a reference number will be assigned and information inputted into a single database.

## The Project Manager (and Triage Group as necessary) will decide what further information, and/or specialist advice, is required to enable the Panel to consider the request. The Project manager will maintain a list of specialists in order that advice can be sought. The Project manager will enter appropriate notes of the information and specialist advice on the SHCAB access database.

## Where a decision is made to refer a request to the Panel, the requestor will be advised in writing that the request has been accepted and will proceed to Panel. The letter may also specify further information that has been called for, and the timeframe within which it should be received. The Project Manager will take any steps necessary to ensure that the submission is fully complete and all supplementary information has been received.

## Requests should be allocated for consideration at the next available Panel meeting.

* 1. The Project Manager is responsible for all the logistical arrangements for Panel meetings and will prepare the agenda and papers for each Panel meeting, in consultation with the Data Protection Officer and Caldicott Guardian. For each application requiring a recommendation, the agenda should set out the project name and supporting documents (e.g data access and DPIA form, UK GDPR/DPA checklist).
  2. Members should receive the agenda and supporting papers no less than 3 working days in advance of each Panel meeting. If a member requests further information or raises a question about the papers in advance of the meeting, both the request/question and the response should be circulated to all members as soon as possible.
  3. The Chair is responsible for the conduct of the meeting, determining whether the meeting is quorate, and ensuring that the agenda is completed.
  4. During the meeting the members of the Panel will consider new requests, approved requests which have been forwarded to data controllers for consultation and will also note decisions made by the Triage Group.
  5. When considering a request, the Panel may recommend as follows:
     + The request will be agreed;
     + The request will be refused;
     + The request cannot be fully assessed because more evidence/information is required and is therefore deferred awaiting further information.
  6. Panels may decide to defer recommendation because information called for before the meeting is not yet available, or because the Panel members decide at the meeting that they need more information.
  7. The status of deferred submissions must be reviewed within one month of the decision to defer. All submissions must be concluded within three months of the date of the first decision to defer.
  8. Once the Panel is in a position to make a recommendation, it may recommend:
     + The request will be agreed.
     + The request will be refused.
  9. The minutes of a Panel meeting will be written up by the Secretary to the meeting and approved by the Chair within 5 working days of the meeting.
  10. The Panel’s outcome will be communicated in writing.

**Step 3 - Reporting to the SHcAB\***

* 1. The outcome of the panel’s decision will be reported at the next available SHcAB meeting, for the outcome to be noted and as a means to object. Meeting papers, to include a copy of the application (including DPIA) and panel minutes will be circulated to SHcAB at least 3 working days in advance of the meeting. On receipt of the documents the SHcAB shall have 20 working days within which to respond.
  2. The Project Manager will update the project log with a summary of any discussion at the SHCAB.
  3. Should the SHcAB require object/clarification on any matters relating to the request, further information will be sought from the project lead at the earliest opportunity with the input of the DPO and Caldicott Guardian as necessary. In this case, the SHcAB will seek to agree virtually based on the additional information or evidence provided.

**Step 4 - Reporting to Joint data Controllers[[1]](#footnote-1)**

* 1. Within 3 working days of the panel meeting, following the Chair’s approval of the minutes, the Project Manager will notify all data controllers whose data is in scope of the project, using the contact details provided on the JCA (agreement contact, Data Protection Officer and Caldicott Guardian) Their named contacts shall be informed of the intent by email and provided with a DPIA, project proposal and the name of the project or activity sponsor.
  2. On receipt of the above documents the relevant Party(s) shall have 20 working days within which to respond.
  3. Should the SHcAB require object/clarification on any matters relating to the request, further information will be sought from the project lead at the earliest opportunity with the input of the DPO and Caldicott Guardian as necessary.

**Step 5 - Issuing of contracts and final actions**

* 1. Following successful reporting to the SHcAB and engagement of Joint Controllers, a template contract (incorporated data processing agreement) is completed by Project Manager and forwarded to all parties for signature.
  2. The Project Manager will update the project log with details of discussion at panel, SHcAB and consultation with joint controllers. The Project Manager will also update the following to ensure this reflects the project within 10 working days of the contract being signed:
* Schedule of processors
* Summary information available on the public facing website
* Privacy Notice
* ROPAs will be made at this point prior to the processing beginning.
  1. The Project Manager is responsible for the final task of ensuring that:
     + All documentation relating to each request is properly identified, controlled and filed;
     + Quality assurance checks are completed;
     + Files are updated, closed and securely stored;
     + Electronic data are properly documented, secured and stored; and
     + Information likely to be required for audit is available in suitable format.
  2. In keeping with the requirement of Records Management: Code of Practice (DH, 2020), copies of DPIAs (and associated paperwork) should kept in archive for a minimum of 6 years.

## Proposed Time Periods for Stages of the Process

|  |  |
| --- | --- |
| Stage | Time period |
| Check request submission is complete – incomplete forms returned | Within 3 working days of receipt of completed form |
| Triage for appropriateness | Within 10 working days of receipt of completed form |
| Redirect inappropriate requests | Within 6 working days of triage |
| Panel papers distributed in advance of scheduled meeting | At least 3 working days prior to scheduled meeting |
| Panel recommendation | As soon as possible but no later than 3 months from date first considered by Panel |
| Minutes approved by Panel Chair | Within 5 working days of Panel meeting |
| Decision communicated to SHcAB | Next available meeting – papers to be made available 3 days in advance |
| Decision communicated to Joint Controllers for engagement | Within 3 working days of Panel meeting. |
| Consideration by Joint Controllers | 20 working days to respond. |
| Template contract (incorporating DPA) circulated for agreement) | Within 3 working days |
| Updates to key documentation by Project Manager | Within 10 days of contract signature |
| Retention of documents relating applications | At least 6 years |

# Schedule C - Communications and Engagement procedure

# Appendix A – The Shared Healthcare Analytics Board Terms of Reference

# Appendix B - The IGDA Group (Triage and Panel) Terms of Reference

1. **Background and rationale**

The SHcAB directs joint health and care data analytics, research and population health management projects within the over-arching governance of the Kent and Medway ICS.

The SHCAB JCA establishes the collaborative governance needed to provide a fair, lawful and transparent framework for the co-ordination of joint processing of health and social care data (The Jointly Controlled Data) for the following agreed joint purposes:

(a) Planning, implementing and evaluating population health strategy

(b) Managing finances, quality and outcomes

(c) Risk stratification for early intervention and prevention

(d) Co-ordinating and optimising patient or service user flows

(e) Undertaking research

(f) Public Health

The KID is a person level data linking routinely collected administrative activity and cost data from almost all NHS providers across Kent and many non NHS organisations from April 2014 onwards. The KID stopped receiving regular data flows from local providers as of April 2019. It is now currently a static pseudonymised dataset only capable for historical analyses and no RE-ID function. However, this remains a valuable information asset that has potential to generate much more insights into our population health.

The KERNEL is the new linked health and care population dataset for Kent & Medway developed by the HISBi Data Warehouse team, building on the success of the Kent Integrated Dataset. The KERNEL encompasses pseudonymised linked data from health & social care organisations in Kent. RE-ID function is available but only for exceptional purposes.

Pseudonymised data will always be the output. Re-identification will only take place in very exceptional cases on an individual basis where there is duty of care to do so e.g. detection of previously undiagnosed disease or adverse outcome in patients undergoing clinical trials. Applications for access to KID and KERNEL data individually or jointly on this basis will be assessed by the Database Access Committee and SHcAB.

The IGDA Sub Group is a sub-committee of the SHCAB. The purpose of the IGDA sub group will oversee, support and maintain the secure sharing of information under the SHcAB JCA. The group will oversee, advise and guide the use of the datasets within the KID and Kernel for projects which meet the SHcAB JCA joint purposes and benefit the local health economy.

1. **Membership:**

The membership of the group will include:

* Caldicott Guardian (Chair)
* Data Security and Protection Leads
  + Data Protection Officer
  + IG lead – Primary Care
  + IG lead – Provider Trust
* Clinicians
* Consultants in Public Health;
* Analytics/BI Representatives
* Kent and Medway R&I Manager or equivalent
* Academic Representative
* Appropriate CCG representatives and/or commissioning representative
* Patient representative(s)
* SHCAB IG and Project Manager Lead

Current membership is as follows:

* Dr Abraham George, Consultant in Public Health and SHCAB Caldicott Guardian (Chair)
* Prof Chris Farmer, Renal Physician, East Kent Hospitals NHS Foundation Trust & Academic Representative, Kent University
* Martine Saker, Information Governance Assurance Lead, , Kent Community Health NHS Foundation Trust
* Latifa Aina, GP Data Protection Officer, NHS Kent and Medway CCG
* Simon Bailey, Director of Business Intelligence, Planning & Performance, Medway NHS Foundation Trust
* Dr Marc Farr, Chief Analytics Officer, East Kent Hospitals NHSFT and SHXAB Chair
* Peter Gough, HISbi Head of Service, Maidstone & Tunbridge Wells NHS Trust
* Helen O’Neil, Data Protection Officer, Kent and Medway CCG
* Morfydd Williams, Director of Digital Transformation, Kent and Medway CCG
* Bob Bowes, GP Governing Body member, Kent & Medway CCG
* Chris Morley, Associate member for patient and Public Involvement, Kent and Medway CCG

The following members of the group will complete the triage of any request for access to data on the groups behalf, before the request is bought to a full panel meeting for review:

* Caldicott Guardian (Chair)
* Data Protection Officer
* SHCAB IG Lead

Observers from projects, or patient/public representatives may also attend.  Observers may provide information to the group regarding the use of the data, application for use in new studies and progress of existing studies utilising data processed under the SHcAB JCA.

1. **Role of the group**
   1. To monitor each Partner’s compliance with the SHCAB JCA or data processing agreement. The Group may request evidence of compliance on written request to any Partner.
   2. To oversee the governance and management of requests to access data from the KERNEL and KID to ensure these meet the agreed joint purpose of the SHcAB JCA, are beneficial to the local health economy and relevant legislation is adhered to and the safety, rights and wellbeing of data subjects are safeguarded.

* The group is responsible for ensuring the completion of DPIAs prior to commencement of each project or activity undertaken in support of one or more of the agreed joint purposes. Each project DPIA must include at least the following:
  + Description of Project.
  + Description of proposed processing operations and data flows.
  + Controllers involved.
  + Proposed Data.
  + Statement of Purpose.
  + Legal basis.
  + Assessment of the necessity and proportionality of processing.
  + Assessment of the risks to the rights and freedoms of data subjects.
  + Proposed measures to control the risks and establish any additional technical and organisational measures necessary to secure data in transit and at rest for each purpose, project and activity.
  + Assessment of whether any proposed use of confidential information is within the ‘reasonable expectations’ of a ‘reasonable person’.
* The group will be ensure that access to Jointly Controlled Data is restricted to authorised individuals on a ‘need to know’ basis only and subject to appropriate technical and organisation controls and sanctions.
* Ensure data flows are appropriately managed and documented in accordance with UK GDPR Art. 30. In keeping with this requirement, the SHcAB ROPA will be updated to reflect each use of the KID and/or KERNEL data.
* Patient and Public Involvement (PPI) members of the group will ensure the interest of patients/carers and the public are considered at all times and that projects include PPI activity where appropriate.
* Ensure that decisions of the group are reported to SHcAB at the next available meeting to note and for any objections to be raised and discussed.
* Ensure that prior to a Party’s data being brought ‘into play’ for a candidate project or activity, their named contact shall be informed of the intent by email and provided with a DPIA, project proposal and the name of the project or activity sponsor, in line with the operating framework. Parties have a right to object to the processing of data they provide into Joint Control for any candidate project or activity. Where they do so, they should provide an explanation or reason.
* Consider and approve charges (to the applicant) for data extraction / access and relevant IG / administration paperwork for each project / application
  1. Subject to satisfactory due diligence and assurance as detailed within the SHCAB IG operating framework:
* To approve additional Partners to the SHcAB JCA
* To determine whether a Partner shall cease to be a party to the SHcAB JCA for a specific period of time or permanently for non-compliance.
* To determine whether a Partner may derogate from or amend any requirement under the SHcAB JCA
* To approve any proposed amendment to the information sharing arrangements
  1. Maintain an information conduit between the Partners; information sharing initiatives and relevant NHS and local authority national initiatives.

* 1. Investigate (or commission the investigation of) breaches of the SHcAB JCA or related data sharing or processing agreements and require partners to take remedial actions.
  2. Approve common patient and public communication materials and take a proactive role in ensuring effective communication about information sharing under the SHcAB JCA.
  3. Develop, review and maintain the SHcAB JCA and associated schedules and data processing agreements to ensure they reflects any legal and statutory obligations and any other related best practice guidance in relation to information governance;

1. **Organisation and Procedures**

* Meetings will be arranged and minuted by the Project Manager or administrator, or by a designated member of the group in their absence.
* Minutes of meeting; outcome and rationale written up within 5 working days of meeting.
* Group decisions shall be taken by consensus. If consensus on any decision cannot be reached, and unless the Group decides otherwise, its decisions shall be taken by a simple majority, or where there is no majority the Chair of the group (or in their absence the co-Chair) has a casting vote
* The group will meet as a panel each month. Virtual meetings of the triage group will take place as needed.
* There will a be a quorum and meetings will go ahead as long as the following members can attend
* Chair
* DPO and 1 IG lead
* At least 1 PPI member
* At least 1 Clinician
* At least 1 BI/Analytics lead
* The following standard agenda will be used for all meetings:

**Standard agenda:**

Attendance

Conflicts of Interest

Minutes of last meeting

Matters arising

Governance, updates or issues

Finance

New applications for access to data

Update from ongoing projects

Publications/outputs

Communications & engagement

AOB

# Appendix C - Application form and checklist for new organisations (On-Boarding Process for the SHcAB Joint Controllers Agreement)

|  |  |
| --- | --- |
| Date: [ ] |  |
| **To:** | The Members of the SHcAB |
| **From:** | [Name and address of entity applying] |

We are a Data Controller operating within Kent and/or Medway and wish to join the above Agreement, a template copy of which has been supplied to us.

We acknowledge and understand the aim of the Agreement is to provide a lawful framework for the joint processing of health or social care data for analytical and research purposes.

It serves to benefit society by:

* Preventing illness and improving population health;
* Improving the effectiveness and efficiency of health and social care services;
* Meeting public health obligations; and
* Undertaking scientific and medical research.

We understand the parties agree to only process Personal Data, Special Categories of Personal Data, and Personal Confidential Information as respectively described in clause 4 .1 and clause 4.2 and clause 4.3 and within the constraints set out in Schedule 3 of the Agreement, for the following joint purposes:

* Planning, implementing and evaluating population health strategy
* Managing finances, quality and outcomes
* Risk stratification for early intervention and prevention
* Co-ordinating and optimising patient or service user flows
* Undertaking research
* Public Health

We acknowledge that we will become a party to the Agreement subject always to the prior approval of all other parties to it in accordance with the Agreement and our signature of the Agreement by which we agree to be bound.

We confirm we have authority to apply to enter into the Agreement and the undersigned is duly authorised to sign.

|  |  |
| --- | --- |
| Signed: |  |
| Name: |  |
| Appointment: |  |
| Date: |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Check List | | Achieved (Yes/No) | Evidence (embedded docs / file references / registration number etc) | Verified by IGDA Group |
| **SECTION 1 - PRIOR TO REVIEW BY IGDA GROUP** | | | | |
| 1. The organisation has reviewed and signed the SHcAB Data Protection Impact Assessment, ensuring it has:  * added their organisation and DSP Toolkit details, * identified any risks to the data sharing, * updated the schedule of data items to be shared, * updated the description of data flows, * ensured any changes to the DPIA have been reviewed by your IG lead and received appropriate organisational sign off. | |  |  |  |
| 1. The organisation must be registered with the Information Commissioners Office (ICO) and have a current Data Protection Registration Number | |  |  |  |
| 1. The organisation must have published a Data Security and Protection (DSP) Toolkit self-assessment to provide assurance that they are practicing good data security and that personal information is handled correctly. | |  |  |  |
| 1. The organisation has an up to date, publicly available Privacy Notice covering all the data processing relevant to the service. | |  |  |  |
| 1. The organisation will be connected to the Health and Social Care Network | |  |  |  |
| 1. The organisation will ensure compliance at all times with obligations for NHS Information Security requirements to identify risks and incidents they have a responsibility to manage. | |  |  |  |
| 1. The organisation must have implemented measures to ensure all IG incidents are reported in accordance with the NHS Digital Guide to the Notification of Data Security and Protection Incidents for reporting, managing and investigating Information Governance Serious Incidents | |  |  |  |
| 1. The organisation must be compliant with the Data Protection Act 2018. If not already compliant with the Data Protection Act 2018, the organisation must have in place an implementation plan to be compliant and provide a statement of assurance that they will be complete during financial year 2019-20 | |  |  |  |
| **SECTION 2: REVIEW AND DECISION OF IGDA GROUP** | | | | |
| Date received: |  | | | |
| Meeting date: |  | | | |
| Initial review comments: |  | | | |
| Final decision | 1. Decline application (please state reason) 2. Refer to SHCAB for approval | | | |
| **SECTION 3: REVIEW AND DECISION BY SHCAB** | | | | |
| Date received: |  | | | |
| Meeting date: |  | | | |
| Initial review comments: |  | | | |
| Final decision | 1. Decline application (please state reason) 2. Approve application and move to section 4 | | | |
| **SECTION 3: NOTIFICATION OF PARTIES AND COMPLETION OF DOCUMENTS** | | | | |
| There has been a notification to all Controllers of the SHcAB Data Sharing Agreement to make them aware of the proposal (at DPO/IG lead/Caldicott Guardian level) and given opportunity to consider, comment upon and object to the proposal. Following notification, there will be a two week standstill. | |  |  |  |
| The organisation has reviewed and signed the SHCAB JCA, ensuring it has:   * added their organisation and contact details, * Been signed by a Senior Responsible Officer, | |  |  |  |
| Actions to be completed by SHCAB IG Lead:   * Uprate schedule with Joint Controllers details * Issue a confirmation of joining letter | |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| On-boarding organisation signatory details | | | |
| Signatory Name (Printed) |  | **Signed** |  |
| Role: |  | **Organisation Name:** |  |
| Date: |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| Information governance validation signatory details | | | |
| Signatory Name (Printed) |  | **Signed** |  |
| Role: |  | **Organisation Name:** |  |
| Date: |  |  |  |

# Appendix D – Confirmation of Joining letter

1. An application form was submitted by [name of entity] on [date] to become a party to the Agreement.
2. A copy of the application submitted by [name of entity] is attached and has been submitted to the parties to the Agreement by the Agreement Administrator.
3. The SHCAB collectively agree that [name of applicant] be permitted to become a party to the Agreement subject always to its terms and the application process detailed therein and that the signatory hereunder is duly authorised to execute this decision-making document on our behalf.

For and on behalf of the SHCAB

Signed:

Name:

Appointment:

Date:

# Appendix E – Schedule of Joint Controllers (The Parties)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Organisation name | Address | Contact | Email | Tel |
| Dartford and Gravesham NHS Trust | Darent Valley Hospital, Darenth Wood Road, Dartford, Kent DA2 8DA | Named Contact for the Agreement is BASIRAT SADIQ  Data Protection Officer is JANICE GUNN  Caldicott (Privacy) Guardian is STEPHEN FENLON | BASIRAT.SADIQ@NHS.NET  JANICE.GUNN@NHS.NET  STEPHENFENLON@NHS.NET | 01322 428431  01322 428375  01322 428653 |
| East Kent Hospitals Trust | Kent and Canterbury Hospital Ethelbert Road Canterbury Kent, CT1 3NG | Named contact for the agreement: Marc Farr  Data Protection Officer: Phil Elliott  Caldicott (Privacy Guardian): Paul Stevens | [marc.farr@nhs.net](mailto:marc.farr@nhs.net)  ekhuft.dataprotectionofficer@nhs.net | 07917 436289 |
| Kent and Medway CCG | Kent House 81 Station Road Ashford TN23 1PP | Named Contact for the Agreement is Helen O’Neil,  Data Protection Officer is Helen O’Neil  Caldicott (Privacy) Guardian is Paula Wilkins | [Helen.oneil3@nhs.net](mailto:Helen.oneil3@nhs.net)  [Helen.oneil3@nhs.net](mailto:Helen.oneil3@nhs.net)  p.wilkins@nhs.net | 07885 243854  07885 243854  01634 335069 |
| Kent and Medway NHS and Social Care Partnership Trust | Farm Villa Hermitage Lane Maidstone Kent ME16 9PH | Our Named Contact for the Agreement is Leanne McDougall  Our Data Protection Officer is Leanne McDougall,  Our Caldicott (Privacy) Guardian is Dr Afifa Qazi | [leanne.mcdougall@nhs.net](mailto:leanne.mcdougall@nhs.net)  [leanne.mcdougall@nhs.net](mailto:leanne.mcdougall@nhs.net)  [Afifa.Qazi@nhs.net](mailto:Afifa.Qazi@nhs.net), | 01795 514507  01795 514507  01622 724133 |
| Kent Community Health NHS Foundation Trust | Trust Headquarters The Oast, Unit D Hermitage Lane, Barming Maidstone Kent ME16 9NT | Named Contact for the Agreement is Natalie Davies  Data Protection Officer is Natalie Davies  Caldicott (Privacy) Guardian is Mercia Spare | [Natalie.davies1@nhs.net](mailto:Natalie.davies1@nhs.net)  [Natalie.davies1@nhs.net](mailto:Natalie.davies1@nhs.net)  m.spare@nhs.net | 01622 211904  01622 211904  01622 211936 |
| Maidstone and Tunbridge Wells NHS Trust | **Maidstone Hospital** Hermitage Lane Maidstone Kent, ME16 9QQ | Named contact for the agreement: James Jarvis  Data Protection Officer: Kevin Rowan  Caldicott (Privacy Guardian) Peter Maskell | [James.jarvis@nhs.net](mailto:James.jarvis@nhs.net)  [kevinrowan@nhs.net](mailto:kevinrowan@nhs.net)  peter.maskell@nhs.net | 01622 227432  01622 228 698  01622 228 574 |
| Medway Community Healthcare CIC | MCH House 21 Bailey Drive Gillingham Businees Park Gillingham Kent ME8 0PZ | Named contact for the agreement: Penny Smith  Data Protection Officer: Natasha Glover-Jones  Caldicott (Privacy) Guardian: Tracy Webb | penny.smith9@nhs.net  natasha.glover-jones@nhs.net  tracy.webb2@nhs.net | 01634 334622  01634 334623  01634 334631 |
| Medway NHS Foundation Trust | **Medway Maritime Hospital** Windmill Road Gillingham Kent ME7 5NY | Named contact for the agreement: Paul Mullane  Data Protection Officer: Paul Mullane  Caldicott (Privacy Guardian) David Sulch | [p.mullane@nhs.net](mailto:p.mullane@nhs.net)  [p.mullane@nhs.net](mailto:p.mullane@nhs.net)  david.sulch@nhs.net | 07843 444508  07843 444508  07889 525333 |

# Appendix F – THE PROCESSORS.

The listed Processors shall comply with the written instructions of their Contracting Authority with respect to the activities and projects of the SHCAB. They are not permitted in law to act beyond the instructions of their Contracting Authority. Instructions relating to Joint Controller activities must therefore be directed through the relevant Contracting Authority.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Processor | Address | Processor Contact | Contracting Authority | Authority Contact(s) |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

# Appendix G - Pseudonymised Data Access Request Form

You must check if your proposed use of data amounts to ‘research’ as defined by UK Policy Framework for Health and Social Care Research and this must be carried out in the public interest. You can check if your proposed use of data amounts to ‘research’ by using the online decision tool: <http://www.hra-decisiontools.org.uk/research/>

Please attached the resulting PDF to the application email

|  |  |  |  |
| --- | --- | --- | --- |
| SECTION 1: TO BE COMPLETED BY REQUESTOR | | | |
| **Requestor Name** |  | **Requestors Contact Number** |  |
| **Requester's Organisation** |  | **Requestors Email Address** |  |
| **Clinical Sponsor and Organisation:** *(Data controller and signatory to the Shared Healthcare Analytics Board (SHcAB) Joint Controller Agreement)* | Clinical Sponsor:  Organisation: | | |
| **Analysts(s) who are required to have access**  *Please list all users who you wish to access the data set - all analysts must have* [*Safe Researcher Training*](https://www.ukdataservice.ac.uk/get-data/how-to-access/accesssecurelab/train.aspx) *(attach certificate to the application email)* | Analyst Name(s) and Job Title(s): | | |
| **The pseudonymised data will be made available in a secure SQL data warehouse, analysts will need SQL skills to extract the data. Can you confirm if the analysts(s) have the necessary skills?** | ☒Yes ☐No  **Users SQL Skill Level** *(Skills level as listed in Annex A):* | | |
| **Software currently available in the pseudonymised. Please mark software required** | * *Excel* * *SQL* * *Tableau* * *R* * *Python* | | |
| **Period of Access** | *Note that access will be provided for 6 months maximum, if access required for longer than an extension application needs to be made a month before the data access is due to expire* | | |
| **Request Date/Time Period for use** | Start :  End : | | |

|  |  |
| --- | --- |
| SECTION 2: TO BE COMPLETED BY REQUESTOR – Projects | |
| **Description of project including background, aims, methods and impact** | *BACKGROUND:*  *AIMS:*  *METHODS:*  *IMPACT:* |
| **State exactly why you require the pseudonymised for**  (tick all that apply) | * Translational Research * Healthcare Delivery * Healthcare Planning * Evaluation * **Other** (please specify) |

|  |  |
| --- | --- |
| Description of Information Required *(Please include dates/timeframes for any analysis, and other specific indicators/categories required in the data such as specific codes/metrics)* | Reference data |
| Other data? (please provide details)  *(for access to KID data please refer to the excel spreadsheet embedded below for available fields)* |

|  |  |
| --- | --- |
| SECTION 3: Details of Controlled Environment (In line with the current ICO Anonymisation Guidance completed by requesting organisation and assessed by the SHCAB Information Governance Group) | |
| *This section serves to document the consistent assessment of data requests to ensure compliance with the ISS requirements* | |
| Is your organisation compliant with the Data Security and Protection Toolkit? |  |
| Is there any intention to link with other data sets? |  |
| How are staff appropriately vetted and confirmation that they have confidentiality clauses in their contracts? |  |
| Have your staff undergone relevant mandatory IG Training? Please detail compliance. |  |
| Will data will be deleted once project has been completed? How will data be deleted? |  |
| If above answer is ‘no’, please explain why and how long you intend to keep the data |  |
| Do you have sufficient resources or funding to support your request? |  |

In order to qualify for approval to pseudonymised data, you must check all the boxes below:

* the terms and conditions of the ‘SHcAB Data Access Contract’ set out below and sign it;
* You agree to report any data quality issue found during analysis to the SHcAB mailbox at:
* You will report back on any benefits of using the pseudonymised dataset and the outcome of analysis to the SHcAB which meets every 2 months. A summary of the benefits will also be presented back to the SHcAB.
* Attend the bi monthly SHcAB to remain updated on data structure changes and the on-going work on data quality.
* Participate in prioritisation exercises to help the SHcAB team in prioritising the issues that are reported.
* Acknowledge the Kent & Medway SHcAB in any papers or publications as a result of the work done with SHcAB, providing evidence of such.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| SECTION 4: To be completed by SHcAB Information Governance G Sub-Group | | | | | |
| **Request Number** |  | **Date Received** | |  | |
| Received by |  | Assigned to | |  | |
| **Initial review by comments** *(Discussion with client – revisions required?*  *Agreement to proceed?* |  | | | | |
| **Any additional conditions attached to disclosure?**  *Other than those set out in the SHcAB Data Access Contract* |  | | | | |
| **Final Decision** |  | | | | |
| **SECTION 5: Completion Details** | | | | | |
| **Date Completed** |  | | **Date Provided** | |  |
| **Revisions Required** |  | | | | |
| **Feedback from Client** *(if applicable)* |  | | | | |
|  |  | | | | |

**Annex A -** SQL levels and expected mastery items

Beginner

* Where clauses (in, between, etc)
* Update syntax
* Inner vs left vs right join understanding and usage
* Syntax for altering and creating structures
* Temp tables and their usage
* Basic idea what indexes are for, though not how they work
* Understanding of what foreign keys are for and how to work around them (cascading deletes, etc)
* Understands basics of transactions
* Understands constraints

Intermediate

* How indexes work, difference between clustered, non-clustered, ETC’s, what a page is and how they layout
* Understanding of sub queries, and can think through using them in joins and where’s
* Pivots, Cursors
* Can think through joining a table on itself when relevant
* Can generate complex data reports via group bys with aggregate functions
* Can do basic profiling just in a monitoring/debugging capacity like reading a log
* Understands the difference between OLAP and OLTP and when/where to use OLAP structures
* Knows how to use triggers and not to use them
* Understands transactions and can layer them handling failures up the stack

Advanced

* Can read an execution plan, and understand how the different parts of the query effect it
* Can tune queries with execution hints (parallelism hints, index hints, loop hints, et al)
* Can profile and use traces for identifying and understanding statistics of executions under real-world load
* Can implement indexes, column store indexes, nested queries efficiently, optimise performance
* Knows what the data structures are on the disk
* Can use performance counters and understand what the database load and behaviour is from monitoring them
* Knows how to use triggers and how to use them safely, with minimal risk
* Knows how to use distributed transactions even with layers

# 

# Appendix H - SHcAB Data Protection Impact Assessment

|  |  |
| --- | --- |
| Name of Project: |  |

# ­­­

# Revision History

|  |  |  |
| --- | --- | --- |
| Version | Date | Summary of Changes |
| 0.1 | 17/12/2018 | Initial Draft |
|  |  |  |
|  |  |  |
|  |  |  |

# Reviewers

|  |  |  |
| --- | --- | --- |
| Name | Date | Title/Role |
|  |  |  |
|  |  |  |
|  |  |  |

# Approved by

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Date | Title/Role | Organisation |
|  |  | DPO |  |
|  |  | SIRO |  |
|  |  |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **PROJECT / ACTIVITY DESCRIPTION** | | | | | |
| This is a SHcAB project. An over-arching Data Protection Impact Assessment (DPIA) which describes the general lawful purposes and activities of the SHcAB can be found here [INSERT LINK]. This is an additional DPIA specific to this project or activity. | | | | | |
| [BRIEF (PLAIN ENGLISH) DESCRIPTION OF PROJECT] | | | | | |
| 1. DATA CONTROLLER(S) | | | | | |
| Subject to the purpose and approach being agreed as necessary and proportionate, and data security and protection controls being appropriate and sufficient, the following controllers intend to provide, or allow the use, of their pseudonymised personal data for the stated purpose.  [Acute Provider(s)]  [Community Providers]  [Mental Health Provider(s)]  [General Practices in [geographic area]]  [Ambulance Trusts]  Medway Council (Social Care and Public Health)  Kent County Council (Social Care and Public Health)  Public Services  [Kent Police]  [Kent Fire and Rescue]  [HM Prisons Service]  [Local Government [Specify department]] | | | | | |
| **INFORMATION ASSETS** | | | | | |
| An information asset is a body of records or information, defined and managed as a single unit so it can be understood, shared and protected. Information Assets used by the SHcAB include pseudonymised datasets held for and on behalf of controllers by one or more contracted data processors (Trusted Third-Party’s). Information Asset Owners (IAOs) are named individuals who are responsible for protecting these assets (i.e. ensuring their confidentiality, integrity and availability) during their life-cycle. | | | | | |
| Subject to the purpose and approach being agreed as necessary and proportionate, and data security and protection controls being appropriate and sufficient, it is proposed to use data held in the following Information Assets.  Trusted Third-Party Processors  [Optum PLC (Contracted to Canterbury Coastal CCG)]  [Maidstone Tunbridge Wells NHS Foundation Trust HISBi (Contracted to East Kent Hospitals University Foundation NHS Trust}]  Providers  [NAME OF INFORMATION ASSET + OWNER]  Public Services  [NAME OF INFORMATION ASSET + OWNER] | | | | | |
| **DESCRIPTION OF THE PROCESSING** | | | | | |
| Data will be pseudonymised in accordance with the ICO Anonymisation: managing data protection risk code of practice. Chapter 7 permits Limited Access to row-level data for the purposes of performing the processing necessary to produce anonymous outputs.  Each participating controller has agreed and documented a schedule of pseudonymised data (dataset) for the purpose stated.  [[NAME OF CONTRACTED DATA MART / WAREHOUSE] already holds data needed for the stated purpose and subject to information governance and security controls, are available for processing.] [Additional data items needed for the purpose will be agreed with the controller and scheduled for extraction.]  [Extraction of data items held in [NAME OF INFORMATION ASSET] and under the control of [NAME OF CONTROLLER] are not currently held in a contracted Data Mart or Data Warehouse. Subject to agreement of the relevant controller(s), arrangements will be made for their secure extraction and transfer to the Trusted Third-Party facility using an approved method.]  Data are either pseudonymised at source (i.e. before extraction) or on-landing in a controlled environment (quarantine).  In the [NAME OF TRUSTED THIRD PARTY] facility, data are linked to perform the required analytics. Linking uses a machine-generated pseudonym designed to prevent re-identification. Role-based access controls restrict access to the resultant anonymised row-level to named individuals who are accountable for their actions during processing.  [This project involves re-identification of data to identify ‘individuals at risk‘ (i.e. risk stratification) and is necessary for ethical approval of the project; however controls ensure that these individuals are identified only back to their GP practice.]  [This project identifies potential candidates for a research purpose and operates in accordance with Health Research Authority (HRA) guidance.]  In accordance with UK GDPR Art. 89(1), technical and organisational measures are in place to ensure data minimisation and de-identification (pseudonymisation) techniques used where the purposes can be fulfilled without identifying data subjects. | | | | | |
| 1. AUDIENCE | | | | | |
| This DPIA informs each controllers’ Data Protection Officer (DPO), Caldicott (Privacy) Guardian, Senior Information Risk Owner and IG lead of the purpose of the processing and the likely impact on individual rights and freedoms. For the avoidance of doubt, it is the Caldicott (Privacy) Guardian’s responsibility to evaluate the ‘necessity and proportionality’ of the proposed processing and the SIROs responsibility to be assured of the technical and organisational controls for data security | | | | | |
| 1. REVIEW | | | | | |
| In accordance with UK GDPR this draft Data Protection Impact Assessment is an opportunity to consult Data Protection Officers of each of the organisations listed in 7.1 for review and comment. This document will be circulated to their IG leads Caldicott Guardians and SIROs, whose review and comments are invited and warmly welcomed. | | | | | |
| **DATA PROTECTION IMPACT ASSESSMENT QUESTIONS** | | | | | |
| This project will process UK GDPR Art. 9 ‘special category personal data’ (e.g. health) listed[[2]](#footnote-2) by the ICO as ‘likely to result in high risk’. This means that a full Data Protection Impact Assessment is mandatory. | | | | | |
| 7.1 STAKEHOLDERS | | | | | |
| A full list of members of the SHcAB and the organisations they represent can be found at: [INSERT LINK TO RELEVANT SHcAB PAGE]  The following controllers intend to permit (subject to appropriate technical and organisational controls) the use of their data for the stated purpose.  SHcAB Joint Controller  [Acute Trusts]  [Mental Health Trusts]  [Community Providers]  [Commissioners]  [Public Services]   * [Kent Fire and Rescue] * [Kent Police] * [Xx District Council] | | | | | |
| 7.2 Purpose(s) of Processing | | | | | |
| [Pseudonymised] Art. 9 ‘special category personal data’ will be processed for the following general purpose(s) *(delete as necessary)*:   * [Informing the planning, implementation and evaluation of population health strategy.] * [Providing analytics services to support the delivery and evaluation of STP projects.] * [Public Health as defined by Regulation (EC) No. 1338/2008 and interpreted in UK GDPR Recital 54.] * [Undertaking Scientific and Medical Research as interpreted in UK GDPR Recital 159.]   It is important to read the over-arching DPIA relating to the general purposes of the SHcAB and their Terms of Reference.  The specific purposes of this project are *(Use NHSE PHM Reference Tables)*:  [E.G. F. PLANNING, IMPLEMENTING AND EVALUATING POPULATION HEALTH STRATEGY  39 Understanding how [NAME OF HEALTH AND CARE SERVICE] impacts on the health of populations in [GEOGRAPHICAL OR ADMINISTRATIVE AREA] | | | | | |
| **Legal Basis of Processing** | | | | | |
|  | | | | | |
| **How will individuals be informed about how their personal data is used?** | | | | | |
| Data Controllers inform their data subjects about the activities and general purposes of the SHcAB in their Privacy (Fair Processing) Notices. This includes the stated lawful purposes and legal basis.  Further information about this specific project can be found on the SHcAB website at the following link:  [INSERT PROJECT LINK]  Accessible versions are available online or on request.  Project progress is communicated through direct campaigns and social media.  Support for Data Controllers will include [a point of contact] for those requiring more detailed information alongside information leaflets and online information. | | | | | |
| * 1. What controls are proposed to ensure only the personal data necessary for the purpose is collected and processed? | | | | | |
| An extraction schedule will be agreed with each controller and signed-off by the relevant Caldicott (Privacy) Guardian or registered professional as ‘necessary and proportionate’ before processing commences. Personal identifiers are removed from the data (e.g. prior to extraction) by the TTP data processor both in transit and in storage and strong access controls are in place, therefore risks are minimised. | | | | | |
| * 1. Briefly explain why the processing is ‘necessary’. | | | | | |
| Processing is necessary to: *(delete if not applicable)*  [Develop new ways of predicting or diagnosing illness]  [Identify ways to improve clinical care]  [Understand more about disease risks and causes]  [Improve diagnosis]  [Develop new treatments and prevent disease]  [Plan NHS and social care services].  The project delivers the following direct and tangible benefits to patients/service users:   * [Improved health, wellbeing and safety]. * [Improved quality of care and clinical outcomes]. * [Improved diagnosis and treatment]. * [Evidence-based preventative measures to reduce individual harm].   The project delivers the following direct and tangible benefits to health and social care professionals:   * [Better understanding of disease and risk factors]. * [Improved patient management and flow]. * [Reducing the overhead of local analytics]. * [Strategies for prevention].   [The [project improves community health and social care and] minimises the following negative effects:   * [Poorly coordinated care and support].   [Risks associated with harmful behaviours]. | | | | | |
| * 1. Will personal data be shared and/or merged with other datasets? | | | | | |
| Personal data is pseudonymisedbefore being linked. Datasets are separated and attributed to each participating data controller. Datasets resulting from linking can be reversed or destroyed without affecting the data from which they were derived. All published outputs are anonymous and are subject to a formal re-identification risk assessment. | | | | | |
| * 1. How long will personal data be retained? | | | | | |
|  | | | | | |
| * 1. How will data quality standards be achieved and maintained? | | | | | |
| NAME OF TRUSTED THIRD-PARTY DATA PROCESSOR] is contracted to:   * Ensure the integrity of data collected, processed and stored. It applies its collective expertise and implements business processes to ensure data are informative and of good provenance, structure and meaning. * Professional analysts profile data to ensure its correct and consistent interpretation, structure and definition. * Processes are designed to ensure the quality of data collected are sufficient for the intended purpose(s). * Information standards and data collection specifications ensure optimal data quality. * Where data quality concerns are identified they will be reported to the relevant controller with advice and guidance on how to improve future collections. * Quality will be monitored, assured and reported on, taking account of internationally agreed practices, for example the European Statistical System dimensions of quality. * Analyses, findings, statistics and conclusions will be produced according to scientific principles and will include details of methods used. Quality assurance procedures will consider each product against users’ requirements. * Skilled staff seek to achieve continuous improvement in analysis and statistical processes. * To promote comparability processing standards, concepts, sampling frames, questions, definitions, statistical units and classifications (including common geographic referencing and coding standards) are applied. | | | | | |
| **How will individuals be made aware of their rights?** | | | | | |
| Controllers are individually responsible for ensuring their Privacy (Fair Processing) Notices include an explanation of subject rights. Given that the data processed are pseudonymised data subjects may be unable to exercise their Art. 15 right of access or Art. 20 right to portability as to do so would require re-identifying data just for that request (in accordance with UK GDPR article 89). They will however be assisted by their respective controllers in understanding the processing and the reasons why these particular rights may be excluded.  Data subject rights are not affected by processing prior to completion of the anonymisation process and should be directed in the usual way to the relevant data controller.  The ‘right to object’ must be exercised with the relevant controller and will be respected and removed from analysis. Where data are linked to national datasets, individuals who have exercised their National Data Opt-out will be removed from processing. | | | | | |
| **What technical and organisational controls have been considered?** | | | | | |
| [NAME OF TRUSTED THIRD-PARTY DATA PROCESSOR(S)] comply with NHS Data Security Standards and demonstrate this compliance through annual completion of the NHS Data Security and Protection Toolkit.  The named data processors comply with the terms of their written contract or agreement (UK GDPR Art. 28) and have provided ‘sufficient guarantees’ of their technical and organisational measures. They must operate and maintain an Information Security Management System to ISO27001:2013 standards as evidenced by a completed Statement of Applicability (SoA).  [NAME OF CONTRACTING AUTHORITY] is responsible for management of the Trusted Third-Party and for ensuring robust operational procedures to protect the security of patient data and respect the rights and freedoms of individuals and for liaising with the Contractor on matters of data security. An ISO27005 compliant Information Risk Assessment has been completed. Data Protection Officers (DPOs) will be consulted to assure controllers that the rights and freedoms of data subjects are protected and respected. | | | | | |
| **Will personal data be transferred outside the EEA?** | | | | | |
| This project does not export or process patient data outside of the EEA. | | | | | |
| 1. Assessment of Impact of Data Security and Protection Risks | | | | | |
| Risk | Description | | Proposed Control | | H/M/L |
| Governance | | | | | |
| Data Control | Lack of clarity over apportionment of data control responsibilities and accountabilities resulting in poor transparency and uncertainty over liabilities, risk ownership, indemnities. | | Project is under SHcAB Joint Control. Operating procedures ensure responsibility and accountability by design. | | L |
| Unlawful Processing | An ‘instruction to process’ issued directly by a contracting authority to a Trusted Third-Party (TTP) data processor without the prior knowledge or agreement of one or more controllers. | | The Joint Control arrangement has robust on-boarding procedure and audit trails to ensure all data held is attributed to a controller or data owner. TTPs are held to contracts, which if found in breach can be terminated. | | L |
| Limited Access | The ‘Limited Access’ controls needed to comply with the ICO Anonymisation code of practice are not adequately supervised and monitored, leading to users retaining access rights beyond their involvement in a project. | | SHcAB administrative functions authorise users and managing access rights for project roles and permissions. | | M |
| Contract Management | Failure to comply with UK GDPR Art. 28 provisions for issuing or revoking instructions to process (Art. 28). | | Contract includes relevant schedules that set out purposes and lawful basis together with a contractual process for new / change ‘instructions to process’. | | L |
| Project or Mission Creep | Projects that extend processing activities beyond its mandate or stated purpose(s). | | Each new project is subject to mandatory DPIA, is notified to relevant data-providers, and signed-off by relevant health professionals (e.g. Caldicott Guardian) as ‘necessary and proportionate’ and by relevant SIROs as within documented information risk appetite. | | L |
| Reputational Damage | A reported loss or breach incident, or poor data protection practices questioned by press, pressure or interest group, or made public following audit. | | Annual external ethical and privacy audits and action plans. | | M |
| Technical | | | | | |
|  |  | |  | |  |
|  |  | |  | |  |
| Transparency | | | | | |
| Individual’s unaware of the purpose and legal basis for the processing of data by SHcAB or who to contact. | Data controllers fail to include TTP/SHcAB model clauses in their Privacy (Fair Processing) Notices **or** people fail to read them. Where included they may not express the purpose and legal basis in ways that are concise, transparent, intelligible and easily accessible, using clear and plain language, e.g. for children. | | Model clauses are provided with supporting guidance. Effective communications campaign targets data controllers and includes checks to ensure they have been included. It is the responsibility of each TTP and their contracting authority to ensure data they hold is lawfully obtained. Processing is unlawful if purpose and legal basis are not included in DC PNs.  SHcAB projects are open and transparent and engage directly with stakeholders and interest groups such as Healthwatch. | | L |
| Individual rights and freedoms | | | | | |
| Objections and Opt-Outs. | Individuals have the right to object the use of their health data for analytics or research purposes. Data Controllers must consider objections and make a decision as to whether they are able to comply under the circumstances. | | Processes are in place to restrict or prevent processing where an individual objects. | | M |
| Individuals don’t understand how data is anonymised and why their rights of access and portability are not available. | UK GDPR Art.11(2) recognises that anonymised data would need to be re-identified if it were to be searchable for subject access requests, or portable, negating the protection anonymisation offers. | | Model PN clauses must explain in plain English the reasons why these rights are removed. | | H |
| **Information Risk** | | | | | |
| The information risks identified below are indicative and subject to review. Trusted Third Party data processors are required to offer ‘sufficient guarantees’ to their contracting authorities. These requirements include TTPs operating an appropriately scoped Information Security Management System (ISMS) to ISO27001 evidenced by a corresponding Statement of Applicability (SoA). All TTPs must have in place, and actively manage, a Data Security Plan for the duration of their contract. It is the responsibility of the contracting authority to ensure ISO27005 compliant Information Risk Assessments are carried out by an appropriately ‘competent person’. | | | | | |
| Risk | Description | Control | | H/M/L | |
| Confidentiality | | | | | |
| Row-level data downloaded to a portable storage device or computer for local processing (e.g. spreadsheet). | Individuals motivated to act beyond their authorisation. This may be out of enthusiasm, with malicious intent or for personal gain. | | All row-level data are processed by the TTP under written instruction. Controls are in place to prevent data from being downloaded or ‘screen-scraped’, such as VPN remote access, or use of TTP proprietary analysis tools. | | M |
| Row-level data moved to an unapproved cloud service for processing (e.g. to produce infographics or perform ‘big data’ analytics). | Individuals motivated to act beyond their authorisation. This may be out of enthusiasm, with malicious intent or for personal gain. | | All row-level data are processed by the TTP under written instruction. Controls are in place to prevent data from being downloaded, ‘screen-scraped’ or moved to sub-contractors. | | M |
| Incident / Breach Management | Any loss, disclosure or breach of personal data from point of extraction will be considered and treated as an incident with consequential statutory reporting and notification obligations. | | Contracting authorities are responsible for managing interdependent loss/breach incident protocols. This includes ‘near-miss’ reporting. Responses to incidents will be coordinated by their SIRO and Data Protection Officer, who will liaise with parties. | | L |
| Cyber attack | Loss or disclosure of any volume of personal data resulting from cyber-attack will be treated as an incident. | | Contracting authorities are responsible for managing interdependent loss/breach incident protocols. This includes ‘near-miss’ reporting. Responses to incidents will be coordinated by their SIRO and Data Protection Officer, who will liaise with parties. All parties must to observe the Data Security Principles to ensure their protection is up to date, including annual penetration testing. | | L |
| Integrity (Data Quality) | | | | | |
|  |  | |  | |  |
| Availability | | | | | |
| Commercial Failure | A TTP data processor fails or terminates a contract reducing capacity with potential loss of assets. | | Contingency plan in place to ‘white-horse’ data held in TTP data-stores. | | M |
| Unavailability of TTP Assets or services. | Processing is delayed. | | TTP Business Continuity Planning audited and monitored by contracting authorities. | | M |

# APPENDIX I – Triage checklist

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Date: |  | | | |
| Reference number: |  | | | |
| Project name: |  | | | |
| Project description including data in scope: |  | | | |
| Triaged by: |  | | | |
| **Check List** | | **Achieved (Yes/No)** | **Evidence (embedded docs / file references / registration number etc)** | **Verified by IGDA triage group** |
| 1. Is the requestor a signatory to the SHCAB Joint Controller or signatory to any existing DSA or DPA within Kent & Medway? | |  |  |  |
| 1. Is the project feasible, e.g. is the data held, would it need to be acquired etc? | |  |  |  |
| 1. Does the sharing involve any sub processors or sub-contractors? | |  |  |  |
| **SECTION 1: AIMS & PURPOSES OF THE SHCAB JCA** | | | | |
| 1. Is the request for a research study/clinical trials (particularly where DEIF/REID of trial participants is required) *All such requests will be sent to the Database Access Committee for consideration* | |  |  |  |
| 1. Does the request have a clear legal basis and meet with the principles of UK GDPR/DPA 2018 | |  |  |  |
| 1. Does the request provide details on how the project serves to benefit society for discussion by panel. | |  |  |  |

| **Section 2 :General UK GDPR/DPA Assurance checklist** | | |
| --- | --- | --- |
| **Requirement** | **Assurance** | **Guidance** |
| **ICO registration -** the organisation is registered with the Information Commissioner’s Office (ICO) | **Registration Number:**  **Expiry Date:** | *Confirm your ICO registration number and expiry date – see* [*link*](https://ico.org.uk/about-the-ico/what-we-do/register-of-fee-payers/) |
| **ICO investigation –** the organisationis not currently under ICO investigation, nor has it been subject to previous ICO enforcement action | *Enter confirmation here* | *Please provide:*   * *Statement confirming the organisation has not been subject to ICO enforcement action or is currently under investigation’* * *Details of any current investigations* * *Details of any previous enforcement action* |
| **NHS Data Security & Protection Toolkit (DSPT) Compliance -** the organisation has submitted a NHS Data Security & Protection Toolkit (DSPT) with status of standards met or exceeded. | **ODS Code:**  **Latest Status:** | *Please see* [*link*](https://www.dsptoolkit.nhs.uk/OrganisationSearch?searchValue=) *and provide:*   * *Details of last DSPT submission include date and achievement level; OR* * *Copy of DSPT Action Plan and confirmation of whether approved by NHS Digital* |
| **Roles & Responsibilities – Caldicott Guardian** | **Name:**  **Job Title:**  **Email address:** |  |
| **Roles & Responsibilities – Senior Information Risk Owner (if applicable)** | **Name:**  **Job Title:**  **Email address:** |  |
| **Roles & Responsibilities – Data Protection Officer (if applicable)** | **Name:**  **Job Title:**  **Email address:** |  |
| **Roles & Responsibilities – Assigned local Information Asset Owner for data processed under this project** | **Name:**  **Job Title:**  **Email address:** | *Please provide confirmation of name, job title, and contact details of assigned Information Asset Owner (who should be a senior staff member)* |

|  |  |
| --- | --- |
| SECTION 3: REVIEW AND DECISION OF TRIAGE | |
| Date received: |  |
| Meeting date: |  |
| Initial review comments: |  |
| Decision | Decline application (please state reason) |
| Request completion of full data access form and refer to the IGDA Group |

# Appendix J – Data Access Contract (Data Processing Agreement)

**TERMS AND CONDITIONS FOR USE OF KID and/or KERNEL data**

The Kent and Medway CCG is appointed by Joint data Controllers as the “lead controller” within the SHcAB Joint Controllers Agreement. As such, the CCG is authorised to enter into a data processing agreement with the named recipient.

*Each party referred to singly as “a Party” or together as “the Parties”*

|  |  |
| --- | --- |
| Recipients details | Name  Address  ICO Registration |

# The Agreement

## This Agreement incorporates the following documents by reference: The Data Request Form and the Data Access Contract and any other terms referenced within them (collectively, the "Agreement"). The Agreement is effective from the Effective Date.

# Interpretation

## In this Agreement, unless the context otherwise requires, the following words and expressions shall have the following meanings:

|  |  |
| --- | --- |
| Agreement | has the meaning given in Clause 1.1; |
| **Applicable Law** | means any court order or any common law, statute, statutory instrument, order or regulation issued by a governmental body with authority over any relevant Party, applicable to any relevant Party from time to time in the context of its relevant rights and obligations under this Agreement; |
| **Background Intellectual Property** | means any Intellectual Property created, devised, generated, owned or licensed by a Party or to which a Party has rights to, prior to the Effective Date; |
| **Data Privacy Law** | means the UK GDPR, DPA 2018, the Privacy and Electronic Communications (EC Directive) Regulations 2003 (21 2003/2426) and all other applicable laws and regulations relating to processing of Personal Data and privacy in effect in any relevant territory from time to time, including where applicable the guidance and codes of practice issued by the Information Commissioner’s Office (ICO), Information Governance Alliance; |
| **Data Protection Legislation** | means Regulation (EU) 2016/679 (General Data Protection Regulation) (UK GDPR) and Data Protection Act 2018 (DPA 2018); |
| **Data Subject** | shall have the meaning given to it under section 3(5) of the DPA 2018; |
| **Effective Date** | means the date this Agreement was signed by the when the Parties’ respective rights and obligations hereunder shall be deemed binding; |
| **FOIA** | means the Freedom of Information Act 2000; |
| **FOIA Request** | means a request for information or an apparent request under FOIA; |
| **IGDA** | shall mean the Information Governance and Data Access Group; |
| **Intellectual Property** | means (i) patents, designs, trade marks and trade names (whether registered or unregistered), copyright and related rights, database rights, Know-How and confidential information, (ii) all other intellectual property rights, in each case whether registered or unregistered and similar or equivalent rights anywhere in the world which currently exist or are recognised in the future; and (iii) all applications, renewals or extensions (including supplementary protection certificates) in relation to any such rights; |
| **KERNEL** | Shall mean the Kent Research Network for Education and Learning linked health and care population dataset for Kent & Medway |
| **KID** | Shall mean the Kent Integrated Dataset |
| **Know-How** | shall mean any technical and other information which is not in the public domain, including information comprising or relating to concepts, discoveries, data, designs, formulae, ideas, inventions, methods, models, assays, research plans, procedures, designs for experiments and tests and results of experimentation and testing (including results of research or development), processes (including manufacturing processes, specifications and techniques), laboratory records, chemical, pharmacological, toxicological, clinical, analytical and quality control data, trial data, case report forms, data analyses, reports, manufacturing data or summaries and information contained in submissions to and information from ethical committees and regulatory authorities and computer programs or algorithms. Know-How includes documents containing Know-How, including but not limited to any rights including trade secrets, copyright, database or design rights protecting such Know-How. The fact that an item is known to the public shall not be taken to preclude the possibility that a compilation including the item, and/or a development relating to the item, is not known to the public; |
| **Lead controller** | means an organisation which is a signatory to the SHCAB JCA Service Specification, named in section 1 of the SHCAB Pseudonymised Data Request Form; who is permitted to disclose the KID and/or KERNEL Pseudonymised pursuant to the terms set out in this Agreement; |
| **Non-Commercial** | Shall mean anything which does not have a commercial objective and is not intended to make a profit; |
| **Overall Purpose** | shall have the same meaning as set out in section 2 of the SHCAB pseudonymised Data Request Form; |
| **Party** or **Parties** | meaning the Relevant Partner and/or the Recipient individually being the two parties to this Agreement; |
| **Permitted Period of Retention** | shall initially mean the period set out in clause 4.1 and any extension granted per clause 4.2; |
| **Personal Data** | shall have the meaning given to it under section 3(2) of the DPA 2018; |
| **Project Intellectual Property** | means any Intellectual Property created, devised, or arising out of the Purpose which has relied on or any part of the KID and/or KERNEL Pseudonymised Data, including but not limited to the Requested Data; |
| **Purpose** | means the purposes the Recipient will use the KID and/or KERNEL Pseudonymised Data for, as expressly set out in the SHCAB Pseudonymised Data Request Form, such purpose must be permitted by the IGDA and SHCAB applicable to the Relevant Partner's organisation type and aligned to the Overall Purpose; |
| **Recipient** | means the organisation identified in the SHCAB Pseudonymised Data Request Form as the one requesting access to the KID and/or KERNEL Pseudonymised Data; |
| **SHCAB** | Shall means the Shared Healthcare Analytics Board |
| **SHCAB Pseudonymised Data Request Form** | means the form setting out the Recipient’s request for access of the Pseudonymised Data within KID and/or KERNEL and details of disclosure of the Pseudonymised Data to the Recipient; |
| **SHCAB JCA** | Shall means the Shared Healthcare Analytics Board Joint Controllers Agreement |
| **Terms and Conditions** | means the terms and conditions contained in this document comprising the terms and conditions applicable to the use and disclosure of the KID and/or KERNEL Pseudonymised Data; and |

## Interpretation

* + 1. A reference to a statute or statutory provision is a reference to it as amended or re-enacted. A reference to a statute or statutory provision includes any subordinate legislation made under that statute or statutory provision, as amended or re-enacted.
    2. Any words following the terms **including**, **include**, **in particular**, **for example** or any similar expression shall be construed as illustrative and shall not limit the sense of the words, description, definition, phrase or term preceding those terms.
    3. A reference to **writing** or **written** includes email.
    4. A reference to a **company** shall include any company, corporation or other body corporate, wherever and however incorporated or established.
    5. Any obligation on a party not to do something includes an obligation not to allow that thing to be done.

# Information to be Accessed

## The SHcAB in conjunction with the Relevant Partner is disclosing the KID and/or KERNEL Pseudonymised Data to the Recipient.

|  |  |  |
| --- | --- | --- |
| Details of data to be disclosed: | KID | XXXXXXXXXXXXXXXX |
| KERNEL | XXXXXXXXXXXXXXXX |

## The Relevant Partner hereby agrees to provide the Recipient with access to the specific part of the KID and/or KERNEL Pseudonymised Data set out in section 2 of the Pseudonymised Data Request Form (the “Requested Data”) and as detailed in 3.1 above.

## The Recipient acknowledges that the Requested Data is derived from the KID and/or KERNEL Pseudonymised Dataset and that the Relevant Partner is a signatory to the SHcAB JCA under which the Relevant Partner agrees to only disclose data contained within the KID and/or KERNEL Pseudonymised Dataset to a third party engaged to act on behalf of the Relevant Partner, for the sole purpose of that third party acting on behalf or in collaboration with the Relevant Partner, and only where that third party is subject to contractual terms no less onerous than those imposed on the Relevant Partner by the SHCAB.

## The Recipient hereby acknowledges and agrees that it shall not perform its obligations under this Agreement in such a way as to cause the Relevant Partner to breach any of its obligations under the SHCAB JCA.

## The Parties agree and acknowledge it is not intended for any Personal Data to be shared under this Agreement. If the Recipient receives any data from the Relevant Partner which it considers may constitute Personal Data or it could be used, couple with other information, to identify a patient or any person then, the Recipient will:

### immediately notify the Relevant Partner; and

### at the request of the Relevant Partner, destroy any information the Relevant Partner requests, including but not limited to, patient identifiable data and/or Personal Data.

## Prior to disclosure of the Requested Data, the Relevant Partner will inform the Recipient if there are any additional terms and conditions of use over and above those set out in this Agreement. If there are any additional terms and conditions of use, the Recipient must agree to them in writing in the final SHCAB Pseudonymised Data Request Form before the Requested Data is shared and such terms shall be incorporated into this Agreement.

## No term of this Agreement shall oblige the Relevant Partner to disclose any KID and/or KERNEL Pseudonymised Data to the Recipient.

## While data quality is an important priority under the SHCAB JCA, the Relevant Partner does not warrant and shall have no liability for the quality, accuracy, completeness and validity of the Requested Data.

# Retention of information

## The Requested Data may only be accessed for XX months. Note that all data will be retained within the safe haven and requests will need to be made to the IGDA for record level data extraction.

## If the Recipient requires an extension to the retention period, the Recipient will request an extension in writing no less than XX prior to the expiry of the retention period.

## No term of this Agreement shall oblige the Relevant Partner to extend the Permitted Period of Retention and the Relevant Partner will determine solely at its own discretion whether to grant such a request and shall notify the Recipient of its decision as soon as reasonably practicable.

# Conditions of disclosure

## Subject to Clause 5.2, the Parties acknowledge and agree that the Requested Data shall only be used for a Purpose permitted by the SHCAB and set out in Section 2 of the SHcAB Pseudonymised Data Access Request Form as applicable to the Relevant Partner's organisation type, these are as follows:

### a partner to the SHCAB JCA which is a Clinical Commissioning Group may only use or allow any data contained within the KID and/or KERNEL Pseudonymised Dataset to be used in connection with that CCG Partners' statutory functions as a commissioner of health care;

### a partner to the SHCAB JCA which is a local authority may only use or allow any data contained within the KID and/or KERNEL Pseudonymised Dataset to be used in connection with that Partner's statutory functions as a provider or commissioner of health and/or social care;

### a partner to the SHCAB JCA who provides health or social care (other than a local authority) may only use or allow any data contained within the KID and/or Kernel Pseudonymised Dataset to be used in connection with that Partner's statutory functions as a provider of health and/or social care; and

### any partner, signatory to the SHCAB JCA, may use the KID and/or KERNEL Pseudonymised Data for the purposes of research which must be considered as:

#### translational research;

#### healthcare delivery;

#### healthcare planning; or

#### evaluation

## In return for the Relevant Partner making the Requested Data available to the Recipient, the Recipient warrants, represents and undertakes to the Relevant Partner that it:

#### will only use the Requested Data for the Purpose and will ensure and prevent the Requested Data being used or exploited for any other purpose. For the avoidance of doubt, the Recipient warrants, represents and undertakes that it will not sell or otherwise exploit for commercial gain or reward any data contained in the Requested Data unless it brings benefits to service users/patients/NHS;

#### will not directly or indirectly disclose or make available any of the Requested Data in whole or in part to any person, except where expressly permitted by, and in accordance with, this Agreement;

#### will not seek to attempt to re-identify any Data Subject contained within the Requested Data or combine the Requested Data with other data in an attempt to identify any individual;

#### shall not use any of the Requested Data to take a decision about any specified individual or individuals;

#### shall not link data in the Requested Data with any other dataset containing Personal Data;

#### shall comply with all Applicable Law in its use of the Requested Data and shall not perform its obligations under this Agreement in such a way as to cause the Relevant Partner to breach any of its legal obligations under Data Privacy Law;

#### shall ensure that any derived materials using the Requested Data attribute is attributed to the Relevant Partner and highlight the source of the information you have used; and

#### will fully co-operate with the Relevant Partner and/or the IGDA and SHCAB to ensure the Relevant Partner's compliance with its obligations under Data Privacy Law.

#### will ensure there is no forward transfer of data

### For the avoidance of doubt, references in this Agreement to the use of the KID and/or KERNEL Pseudonymised Data or Requested Data includes use and/or reproduction of any part of the KID and/or KERNEL Pseudonymised Data or Requested Data. "Use" includes any action which would constitute "Processing" as per section 3(4) of DPA 2018.

# Security

## The Recipient shall only access, store and make use the Requested Data on the VDI and shall not attempt to extract any of the Requested Data, whether in whole or in part, outside of the VDI unless as expressly permitted by clause 6.2.

## Where the Recipient does not wish to utilise the VDI and seeks to access, store or make use of the Requested Data outside of the VDI, he/she must first seek written permission from the data access sub-group in order to do so. If granted written permission, by the data access sub-group; then the Recipient shall ensure and guarantee and implement the following:

### appropriate technical and organisation controls are put into place to ensure full compliance with Article 32 of UK GDPR;

### any storage the Requested Data will be on a secure system and apply the same security measures and degree of care to the Information as the Recipient applies to its own confidential information, which the Recipient warrants as providing adequate protection from unauthorised disclosure, copying or misuse;

### safe destruction of the Requested Data, after the Permitted Period of Retention in in accordance with the NCSC guidance: <https://www.ncsc.gov.uk/guidance/secure-sanitisation-storage-media>

### if applicable, for any hard copies to be safe and secure shredded and disposed of; and

### must provide the Relevant Partner with confirmation in writing that the provisions of Clause 6.2 have been complied with.

### must complete a data processing agreement with XXX

### must maintain records of processing and provide audits of data access

# Audits

## The Recipient agrees to the following:

### During the Agreement period, the Relevant Partner reserves the right at any time to undertake an audit in respect of the Recipient's use and storage of the Requested Data is in compliance with the terms of the Agreement.

# RETURN OF THE DATA and additional obligations

## The Recipient shall comply, in respect to the Requested Data, with any request from the Relevant Partner and/or the IGDA or SHCAB requiring the Recipient to:

#### securely return all or part of the Requested Data to the Relevant Partner and/or IGDA or SHCAB Information Governance Board (as applicable); and/or

#### securely destroy all or part of the Requested Data;

within a timeframe specified by the Relevant Partner and/or IGDA or SHCAB in accordance with any specified security measures.

## The Recipient shall not do anything that may materially damage the reputation of the Relevant Partner, any signatories to the SHCAB JCA or the SHCAB.

## The Recipient shall not make, or permit any person, company or other body to make, any public announcement concerning this Agreement without the Relevant Partner's prior written consent.

# FREEDOM OF INFORMATION

## The Recipient acknowledges that the Relevant Partner is subject to the requirements of FOIA and shall assist and co-operate with the Relevant Partner to enable the Relevant Partner to comply with the FOIA disclosure requirements.

## The Recipient shall:

### transfer any FOIA Request to the Relevant Partner as soon as practicable after receipt and in any event within three (3) days of receiving a FOIA Request;

### provide the Relevant Partner with a copy of all Requested Data in its possession or power in the form that the Relevant Partner requires within seven (7) days (or such other period as the Relevant Partner may specify) of the Relevant Partner requesting the Requested Data; and

### provide all necessary assistance as reasonably requested by the Relevant Partner to enable the Relevant Partner to respond to a FOIA Request within the time for compliance set out in section 10 of FOIA.

## The Relevant Partner shall be responsible for determining at its absolute discretion whether the Requested Data:

### is exempt from disclosure in accordance with the provisions of FOIA; or

### is to be disclosed in response to a FOIA Request.

## The Recipient is prevented, under any circumstances, from responding directly to a FOIA Request, made in respect of the Requested Data, unless expressly authorised to do so by the Relevant Partner.

## If the Relevant Partner takes a decision to comply with the FOIA Request, it shall notify the Recipient of this decision not less than three (3) days in advance of the disclosure being made and provide the Recipient with a copy of the information that it intends to disclose.

## The terms of the Agreement shall not be deemed as confidential, but neither Party shall make any announcement which is calculated to or which does harm the reputation or legitimate interest of the other. This clause shall not prevent either Party from making comments in good faith on a matter of public interest, or from making disclosures required by the FOIA or any other legislative or regulatory requirement.

## For any other requests to release the Requested Data, the Recipient must obtain the written permission of the Relevant Partner prior to its release.

# Breach of conditions

## Notification of breach

The Recipient must report any known or suspected breach of this Agreement to the IGDA and Relevant Partner within twenty-four (24) hours.

## Consequences of breach

The breach of any term of this Agreement may, at the absolute discretion of the Relevant Partner, result in one or more of the following:

### the requirement for the Recipient to return all the Requested Data supplied under this Agreement; and/or

### immediate termination of this Agreement.

# Proprietary Rights in the Data

## Nothing in this Agreement shall affect the ownership of any Background Intellectual Property owned by either Party.

## The Recipient acknowledges and agrees that nothing in this Agreement grants or shall be deemed to grant to the Recipient any right, title, or interest whatsoever (including any Intellectual Property right whatsoever) in or to the Requested Data or any part thereof, except the limited right to use the Requested Data for the Purpose and performance of its obligations under, and in accordance with, the Agreement.

## All Project Intellectual Property created by the Recipient shall, subject to the terms set out in clauses 11.4, 11.5 and 11.6, be jointly owned by the Parties.

## The Parties hereby agree that each Party may use the Project Intellectual Property for any research, academic and Non-Commercial purpose.

## The Relevant Partner, subject to the profits being shared equally (50/50) between the Parties, hereby agrees to allow the Recipient to use the Project Intellectual Property for their own commercial purpose(s).

## Any decision on disposal of the Project Intellectual Property shall be jointly made and agreed by the Parties.

# Term and Termination

## This Contract shall commence on the Effective Date and shall continue until the Recipient has ceased:

### to use the Requested Data for the Purpose; and

### to have any of the Requested Data in possession or control.

## The Agreement may be terminated by the Relevant Partner with immediate effect in the event that any changes in legislation or guidance are made which would result in the terms of the Agreement to not be in compliance and/or at the request of the IGDA or SHCAB.

## This Agreement may be terminated by the Relevant Partner with immediate effect if the Recipient:

### is in breach of any obligation under this Agreement;

### is made the subject of a winding up order or an administrator or receiver is appointed;

### ceases to trade in the UK; or

### is subject to a change of control.

## Termination of the Agreement, for any reason, shall not affect any rights, remedies, obligations or liabilities of either Party that have accrued up to the date of termination, including the right to claim damages in respect of any breach of the Agreement which existed at or before the date of termination.

# Indemnity

## The Recipient shall indemnify the Relevant Partner and all parties to the SHCAB agreement fully and keep the Relevant Partner and signatories to the SHCAB JCA indemnified against all costs, regulatory fines, losses, charges, claims, proceedings, actions, damages, legal costs, expenses and any other liabilities which the Relevant Partner or SHCAB JCA signatories suffers or for which the Relevant Partner or SHCAB JCA signatories may become liable which are caused directly or indirectly by any breach of this Agreement by the Recipient.

# Assignment

## Neither Party may assign, transfer, or otherwise dispose of its rights or obligations under this Agreement without the prior written consent of the other Party.

# No waiver

## No failure or delay by either Party to exercise any right or remedy provided under the Agreement or by law, shall constitute a waiver of that or any other right or remedy, nor shall it prevent or restrict the further exercise of that or any other right or remedy. No single or partial exercise of such a right or remedy shall prevent or restrict the further exercise of that or any other right or remedy.

# Severability

## If any provision or part-provision of the Agreement is or becomes invalid, illegal or unenforceable, it shall be deemed modified to the minimum extent necessary to make it valid, legal and enforceable. If such modification to or deletion of a provision or part-provision shall be deemed deleted. Any modification to or deletion of a provision or part-provision under this clause shall not affect the validity and enforceability of the rest of the Agreement.

## If any provision or part-provision of the Agreement is deemed deleted under clause 16.1, the Parties shall negotiate in good faith to agree a replacement provision that, to the greatest extent possible, achieves the intended result of the original provision.

# Status of the Parties

## Nothing in this Agreement is intended to or shall operate to create a partnership or joint venture of any kind between the Parties or to authorise either Party to act as agent for the other and neither Party shall have authority to act in the name or on behalf of or otherwise bind the other in any way.

# Third parties

## Nothing in this Agreement will be construed as conferring any rights or benefits on any person or legal entity who or which is not a Party to this Agreement. The Contracts (Rights of Third Parties) Act 1999 and any other legislation applicable to this Agreement that confers contractual rights on third parties, is hereby excluded to the fullest extent permitted by law.

# Variation

## No variation or modification of this Agreement shall be valid unless in writing and signed by both Parties.

# Entire agreement

## This Agreement constitutes the entire agreement and supersedes all previous verbal or written proposals and agreements between the Parties. Except as expressly stated in writing in this Agreement, neither Party has relied upon any statement or representation made by the other in agreeing to enter into this Agreement.

# Counterparts

## This Contract may be executed in any number of counterparts, each of which will be regarded as an original, but all of which together will constitute one agreement binding on all of the Parties, notwithstanding that all of the Parties are not signatories to the same counterpart.

# Governing law

## This Agreement, all matters regarding the interpretation or enforcement of it, and any other matters or disputes arising in connection with it or its subject matter shall be governed by the laws of England and Wales and the Parties hereby submit to the exclusive jurisdiction of the courts of England and Wales.

|  |  |
| --- | --- |
| **SIGNED** for and on behalf of **[INSERT PARTNER DETAILS]** (the “**Recipient**”) |  |
| Name: |  |
| Position: |  |
| Date: |  |

|  |  |
| --- | --- |
| **SIGNED** for and on behalf of  The “Relevant partner”  [insert here] |  |
| Name: |  |
| Position: |  |
| Date: |  |

# Appendix K – Template Privacy Notice

1. Steps 3 and 4 may happen simultaneously, dependent on the timing of the application and the next meeting of the SHCAB. [↑](#footnote-ref-1)
2. [https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-UK GDPR/data-protection-impact-assessments-dpias/examples-of-processing-likely-to-result-in-high-risk/](https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/examples-of-processing-likely-to-result-in-high-risk/) [↑](#footnote-ref-2)