

# Risk Stratification

Leicester, Leicestershire and Rutland

## Information Sharing and Data Processing Agreement

for the use of GP Practice data  
and Secondary Uses Service (SUS) data  
for risk stratification for case finding, public health  
and commissioning purposes

**July 2015**

This Agreement will be executed in counterparts – it will be signed separately by each participating organisation and returned to Arden and GEM CSU via the relevant CCG. Each counterpart shall be deemed to be an original document and all of the counterparts taken together shall constitute one single agreement between the participating organisations. A full list of participating organisations will be maintained by the Arden and GEM CSU.

## 1 Introduction

- 1.1 The overall purpose of risk stratification is to improve the quality of care and clinical outcomes for patients. Whilst risk stratification supports case finding of high risk patients it can also be used to support commissioning through the use of aggregated data.
- 1.2 Risk stratification can help determine which people in a population are at high risk of experiencing outcomes such as unplanned hospital admissions that are simultaneously undesirable for patients; costly to the health service; and potential markers of low-quality care.
- 1.3 **Risk Stratification for Case Finding:** Risk stratification tools can assist clinicians in identifying which patients should be offered targeted preventative support (this is known as “risk stratification for case finding”).
- 1.4 Once the population has been stratified using a predictive modelling tool, high-risk individuals can then be re-identified by GP Practice staff who have a direct care relationship with the patient (as determined by the GP Practice), so that their GP can offer them additional preventative services.
- 1.5 **Risk Stratification for Commissioning:** Risk stratification tools can also be used for analysing the health and the variations in health outcomes within the population to help understand local population characteristics. The aggregated information produced provides information about disease and risk prevalence and distributions across wider populations. It can be used to partly inform such activities as planning, service redesign, quality assessment, resource allocation and commissioning wider preventative services, for example. This is known as “risk stratification for commissioning”. Risk stratification for commissioning could include services commissioned by:
  1. the respective Clinical Commissioning Group (CCG) individually or collaboratively, for example, for “Better Care Together” planning
  2. the respective Public Health Department
  3. General Practices that commission services.
- 1.6 It is important to note that risk stratification for commissioning purposes involves only the use of pseudonymised or aggregated data, i.e. NO personal confidential level data (PCD)<sup>1</sup> is seen by commissioners. All data will be processed in a secure and confidential manner and in strict accordance with legal obligations and NHS guidelines.
- 1.7 All signatories of this Agreement will ensure that re-identification is solely for the purpose of direct care and is available only to those with a direct care relationship with the patient.
- 1.8 Commissioners will only receive aggregated or pseudonymised reports which will be produced in strict accordance with the Information Standards Board for Health and Social Care publication – “Anonymisation Standard for Publishing Health and Social Care Data Specification”<sup>2</sup>. Where necessary small number suppression will be applied to avoid any unintentional possibility of re-identification.
- 1.9 To facilitate this risk stratification implementation Arden and Greater East Midlands Commissioning Support Unit (Arden and GEM CSU) will provide a number of support services within the approved legal framework to process data in their Accredited Safe Haven (ASH). An

---

<sup>1</sup> **Personal Confidential Data (PCD)** - As per Caldicott 2, ‘Personal’ includes the Data Protection Act definition of personal data, plus data relating to the deceased. ‘Confidential’ includes both information ‘given in confidence’ and ‘that which is owed a duty of confidence’ and is adapted to include ‘sensitive’ as defined in the Data Protection Act.

<sup>2</sup> The ISB standard - Anonymisation Standard for Publishing Health and Social Care Data Specification (Process Standard) is available to view on <http://www.isb.nhs.uk/documents/isb-1523/amd-20-2010/1523202010spec.pdf>

ASH is an NHS accredited organisation which is contractually and legally bound to process data in a secure and confidential manner. Technical and operational security measures are in place to ensure that there is robust segregation of data and strict access control within the ASH.

- 1.10 This implementation will enable both risk stratification for case finding and risk stratification for commissioning.
- 1.11 For the purposes of this Agreement the words “data” and “information” are synonymous.

## **2 Purpose of this Agreement**

- 2.1 This Agreement outlines the framework that enables lawful processing of GP Practice data and commissioning data sets from the Secondary Users Service (SUS) for:
  - (a) risk stratification for case finding, **and**
  - (b) risk stratification for commissioning purposes.
- 2.2 The Agreement outlines the procedures and controls necessary to comply with NHS guidance on risk stratification, the Data Protection Act 1998, the common law duty of confidence and other applicable legislation.
- 2.3 This Agreement describes how information will be processed securely and confidentially and documents the responsibilities of all parties involved. It will provide reassurance that only pseudonymised and aggregated data is used for commissioning purposes.
- 2.4 This implementation will ensure compliance with the NHS England guidance, “Information Governance and Risk Stratification: Advice and Options for CCGs and GPs”, (July 2013) – see Appendix A.
- 2.5 An organisation will only be included in this risk stratification for case finding and commissioning activity when they have signed this Agreement. In addition to this Agreement, the relevant CCG must sign the NHS England Risk Stratification Assurance Statement and submit it to NHS England for approval (see Appendix B).
- 2.6 **This Agreement relates to the extraction, analysis and secure storage of data for risk stratification for case finding and commissioning purposes only. The use of risk stratification PCD for any other purpose is not permitted under this Agreement and would require a separate Agreement to be signed again by the GP Practice.**
- 2.7 Adjusted Clinical Groups (ACGs; the tools used for risk stratification) is widely used nationally and internationally to support clinical research. A number of local academics have expressed an interest in using some of the Leicester, Leicestershire and Rutland non-PCD outputs of the ACG system to support their work. Such clinical research is outside the scope of this Agreement. In the event that clinical research using the ACG system outputs is to be pursued, a separate Agreement outlining the legal gateway will be offered.

## **3 Lawful Basis for Data Processing**

- 3.1 The second Caldicott review of information governance (Caldicott 2), published in April 2013, reaffirmed that risk stratification is not a form of direct care and that organisations need to identify a legal basis to process confidential patient information for this purpose.
- 3.2 The legal basis for this risk stratification processing for case finding and for commissioning purposes, was established by NHS England through specific approval under Section 251 of the NHS Act 2006 – CAG7-04(a)/2013. This approval allows disclosure of commissioning data sets

(SUS) from the Health and Social Care Information Centre (HSCIC) and the disclosure of data from GP systems to data processors working under the instruction of GPs as data controllers, to enable the preliminary processing and linkage of the data for risk stratification. This approval **does not** currently cover additional linking of identifiable social care data for risk stratification.

- 3.3 The Section 251 approval is a temporary measure. When new regulations are approved this Agreement will be reviewed and updated as appropriate.

## **4 Fair Processing Notices (Privacy Notices)**

- 4.1 GP Practices (as Data Controllers) are already required to inform patients about how their information will be used, who it will be shared with, the purpose of sharing and about the provision for opting-out. GP Practices are required to ensure that their Fair Processing Notices (sometimes referred to as privacy notices) are updated to cover risk stratification data processing and must take reasonable steps to ensure that all patients have access to this.
- 4.2 Patients should also be informed that this is a local risk stratification implementation and is different from national initiatives, such as "care.data".
- 4.3 Commissioners (CCGs and Public Health) must also ensure that their Fair Processing Notices reflect their use of non-PCD risk stratification data outputs.

## **5 Patient Objections – Opt-out**

- 5.1 GP Practices are required to have a process in place to enable patient requests for exclusion (opting-out) from risk stratification data processing to be respected.
- 5.2 A specific opt-out code (see 5.3. below) has been created for risk stratification. As recommended by NHS England, the "care.data" opt-out code should not be used to record dissent from this local risk stratification programme.
- 5.3 Where a patient objects to their data being processed for local risk stratification activities (opting-out), the GP Practice should add the appropriate code to the patient record, as follows:
- TPP SystmOne (CTV3) opt out code – XaJDp (multi-professional risk assessment declined).
  - EMIS (Read2) opt out code – 9Oh5 (multi-professional risk assessment declined).

## **6 Risk Stratification Data Flow**

- 6.1 Risk stratification will involve the extraction of patient identifiable data (as listed in Appendix C) from each participating GP Practice via Secure File Transfer Protocol (SFTP) by their system suppliers, and submission to a safe haven within the Arden and GEM CSU. The system

suppliers will not extract any data relating to a record which bears an opt-out code indicating that the patient does not wish to be included in risk stratification, namely:

- TPP SystmOne (CTV3) opt out code – XaJDp (multi-professional risk assessment declined).
- EMIS (Read2) opt out code – 9Oh5 (multi-professional risk assessment declined).

- 6.2 The data will be pseudonymised<sup>3</sup> upon receipt in the Arden and GEM CSU (known as pseudonymisation on landing). This will be done in a secure automated environment, separate from other data processing activities.
- 6.3 Automated validation checks will be run by Arden and GEM CSU to ensure that there is no data relating to records which bear an opt-out code indicating that a patient has opted-out of risk stratification processing.
- 6.4 GP Practice data which is coded to indicate that it contains legally protected or highly sensitive data (see paragraph 7.1.5) will be excluded from risk stratification analysis in an automated routine. Arden and GEM CSU will run automated validation checks to ensure that all such data is excluded.
- 6.5 The data fields that are required for risk stratification analysis will be extracted in an automated routine. Any data not required for risk stratification analysis or for re-identification by a GP Practice will be securely deleted in an automated routine.
- 6.6 The remaining pseudonymised GP Practice data will then be linked with pseudonymised SUS data and securely transmitted to the risk stratification tool in an automated routine.
- 6.7 The risk stratification tool currently used is the Johns Hopkins Adjusted Clinical Groups (ACG) system. Reports on the stratified data will be available to approved users through the Arden and GEM CSU's secure portal reporting system, in either aggregated or pseudonymised format, depending upon the user's approved level of access. Access will be strictly controlled to ensure that only authorised users of the originating GP Practice will be able to re-identify appropriate patients when it is necessary to do so for direct patient care purposes.
- 6.8 Pseudonymised or aggregated reports (non-PCD) will be available to the respective commissioner (CCGs, Public Health Departments or commissioning GP Practices).
- 6.9 The GP Practice remains the Data Controller of their data at all times. Arden and GEM CSU are acting as data processors on behalf of the GP Practice and are only able to undertake any activity with the express permission of the GP Practice. (See Appendix D for further explanation about Data Controllers and Data Processors and their responsibilities).
- 6.10 The GP Practice will become Data Controller in Common with the HSCIC for any SUS data made available to the Practice through the risk stratification process.

## **7 Information**

### **7.1 What information is necessary to process?**

- 7.1.1 The GP clinical system suppliers will provide data extracts on a monthly basis for all patients registered in the GP Practice, with the exception of records which contain an opt-out code indicating that the patient has opted-out of inclusion in risk stratification (also referred to as multi-professional risk assessment declined).<sup>4</sup>
- 7.1.2 The extraction from the GP systems (by their system suppliers) provides a full patient identifiable data set as defined in the extract specification in Appendix C of this Agreement.

---

<sup>3</sup> **Pseudonymised data** - data with no identifiers except unique pseudonyms that do not reveal patients' 'real world' identities.

<sup>4</sup> A separate Agreement is in place between the System Suppliers and the Arden and GEM CSU for the supply of the data extracts.



7.1.3 Arden and GEM CSU will pseudonymise the GP data upon receipt. Information to enable the GP Practices to re-identify the patient will be segregated and stored in a separate safe haven environment with strict access controls.

7.1.4 Arden and GEM CSU will extract the pseudonymised data items required for risk stratification analysis and securely delete the remainder.

7.1.5 The Arden and GEM CSU will ensure that the data to be processed for risk stratification analysis does not contain any highly sensitive or legally protected data and will run validation checks to ensure that no data relating to patients who have opted-out is included.

An indicative list of excluded codes is available in Appendix C. (This list has been subject to clinical review by a Risk Stratification Project Steering Group.)

7.1.6 Only the minimum amount of pseudonymised data necessary will be processed through the risk stratification tool.

7.1.7 The remaining pseudonymised GP Practice data will be linked with pseudonymised secondary care data using the standard Secondary Users Service (SUS) Data Services for Accident and Emergency (A&E), In-Patient (IP) and Out-Patient (OP).

## **7.2 Who is responsible for data quality and accuracy?**

7.2.1 Under the provisions of the Data Protection Act 1998, the GP Practice (as Data Controller) is responsible for ensuring the accuracy of the data extracted from their system. Responsibility for the accuracy of the commissioning data sets from SUS lies with the originating provider, subject to quality checks within the GEM Data Services for Commissioners Regional Office (DSCRO).

7.2.2 The GP Practice is also responsible for ensuring that the correct opt-out code is applied to their record where a patient has declined participation in risk stratification:

- TPP SystmOne (CTV3) opt out code – XaJDp (multi-professional risk assessment declined).
- EMIS (Read2) opt out code – 9Oh5 (multi-professional risk assessment declined).

## **7.3 How will a record be kept of what information has been shared?**

Arden and GEM CSU will maintain an audit log of all data flows including an audit log of all user activity within the Arden and GEM secure portal reporting tool.

## **7.4 How is information going to be shared?**

7.4.1 The data will be extracted on behalf of the GP practice by their system supplier (i.e. EMIS or TPP SystmOne) for the sole purposes of supporting risk stratification for case finding and risk stratification for commissioning. The data will be transferred by secure file transfer protocol (SFTP) to the Arden and GEM CSU.

7.4.2 Reports will be made available through the Arden and GEM CSU secure portal reporting tool to authorised users in either aggregated or pseudonymised format, depending upon the user's approved level of access.

- 7.4.3 Pseudonymised or aggregated reports (non-PCD) will be available for Commissioners (CCGs for their Member Practices, for respective public health department users or for GPs acting in a commissioning role). All reports will be in accordance with the Information Standards Board Anonymisation Standard (as per paragraph 1.8). Where necessary, small number suppression will be applied to avoid any unintentional possibility of re-identification. Any variation to this will require separate authorisation from the respective GP Practices.
- 7.4.4 Users approved by the GP Practice will be able to access pseudonymised reports (for their Practice only) showing the scores for patients in all Resource Utilisation Bands (RUBs). Users with a direct care relationship with the patient (as approved by the GP Practice) will be able to re-identify the patient. The re-identification is enabled via secure environment automated processing.

## **7.5 Who will have access to Personal Confidential Data (PCD) and what may they use it for?**

- 7.5.1 Risk stratification is not a form of direct care (as reaffirmed by Caldicott 2). However, the tools can be used for identifying individual patients who are at risk of adverse outcomes such as unplanned hospital admissions and who may benefit from additional preventative support. Therefore authorised GP Practice staff with a direct care relationship with patients will be able to re-identify patients from their Practice when required to do so for direct care purposes. Only these staff will have access to PCD when they require it for direct care purposes.
- 7.5.2 Access to PCD will be strictly controlled and evidence of the GP Practice's Caldicott Guardian or Senior Partner or Practice Manager approval will be required for each user who requires access to PCD.
- 7.5.3 GP Practices should only authorise staff to have access to PCD whom they have identified as having a direct care relationship with patients. This may involve, for example, initial screening and then selection of a subsequent subset for multi-disciplinary team review or other clinical review as deemed necessary by the GP Practice. At this point the data will be used for direct care and so it is reasonable to rely upon implied consent, provided the GP Practice has appropriate fair processing/privacy notices and that they have a process to handle requests from patients to opt-out of their data being processed for risk stratification.
- 7.5.4 Patients will be informed before any referral is made to a new service. Explicit consent<sup>5</sup> will be obtained before any information is shared with a non-healthcare organisation.
- 7.5.5 Commissioners will **not** have access to PCD; they will only have access to pseudonymised or aggregated reports as per paragraph 7.4.3.

## **7.6 How long will the data be retained?**

- 7.6.1 The raw data file extracted from the GP Practice will be retained in a secure segregated environment for a maximum period of 7 days (to enable validation checks and allow re-running in the event of any technical failure).

---

<sup>5</sup> Explicit consent is specific permission to disclose data in response to a direct question to the patient. The answer must be clear and unequivocal. The patient must be fully informed about what will be shared, who with and the purpose of sharing. Permission must be voluntary and the person consenting must have the capacity to make the decision. Explicit consent may be given in writing or verbally but details should be recorded in the patient record.

- 7.6.2 The pseudonymised data file will be retained in a secure segregated environment for a maximum period of 3 months (to enable validation checks in the event of system/technical changes or problems).
- 7.6.3 The risk analysis dataset (with a pseudonymised identifier) calculated every month is retained for a maximum period of three years in archive for long term patient trend analysis.

## 7.7 Access Control

- 7.7.1 Arden and GEM CSU will manage the process of access to risk stratification reports via their secure portal reporting system.
- 7.7.2 All GP Practice applications for access to pseudonymised reports will require approval from the relevant GP Practice. Applications for access to individual risk scores and identifiable data will require approval by the GP Practice's Caldicott Guardian or Senior Partner or Practice Manager.
- 7.7.3 Applications for CCG commissioning staff to have access to pseudonymised or aggregated reports will require approval of the CCG Caldicott Guardian, Senior Information Risk Owner (SIRO) or Accountable Officer.
- 7.7.4 Applications for Public Health commissioning staff to have access to pseudonymised or aggregated reports will require approval of the respective Director of Public Health or Deputy Director of Public Health.

## 7.8 Training

- 7.8.1 All staff must undergo risk stratification training before using risk stratification reports.
- 7.8.2 Arden and GEM CSU will provide training.

## 8 Security Obligations

- 8.1 Arden and GEM CSU will ensure that they have confidentiality and information security measures in place to comply with Principle 7 of the Data Protection Act 1998 and NHS requirements as contained within the Information Governance Toolkit. This entails organisational and technical security measures to protect against unauthorised or unlawful access to, or processing of, risk stratification data and against accidental loss or destruction of, or damage to, risk stratification data. Strict controls and procedures will be adhered to at all times to ensure that the terms and conditions of this Agreement applicable to Arden and GEM CSU (the data processor) are complied with.
- 8.2 Arden and GEM CSU will have a full set of information governance policies in place that meet the requirements of the NHS Information Governance Toolkit, to a minimum of level 2.
- 8.3 Further details of security measures are available in Appendix E of this Agreement.

## 9 Further Use of Information

- 9.1 The use of PCD by any party is **not permitted** for any purpose other than the risk stratification for case finding outlined in this Agreement.



- 9.2 Re-identified output from risk stratification analysis will not be used for any purpose other than direct patient care within the GP Practice.
- 9.3 Even though commissioners do not have access to PCD, pseudonymised or aggregated data with small number suppression may still have sensitivities. Therefore, due consideration must be exercised by all participating organisations before they reuse or further disclose risk stratification for commissioning outputs. Any reuse or disclosure must be in accordance with legal obligations.
- 9.4 There will be no attempt by any party to re-identify any data (other than within a GP Practice when an authorised user with a legitimate direct care relationship with the patient requires re-identification for the primary care of a patient).
- 9.5 Arden and GEM CSU shall not disclose any PCD supplied as part of this Agreement to any third party, or process it for any purpose outside of this Agreement without separate specific approval from the GP Practices (Data Controllers).
- 9.6 The Arden and GEM CSU will only share pseudonymised or aggregated risk stratification output with organisations that are signatories of this Agreement.

## **10 Breach of confidentiality or any other Information Governance Breach**

- 10.1 In the event of any suspected breach of confidentiality, or any other information governance breach, the organisation identifying a breach or potential breach, will immediately instigate an investigation following their existing Incident Reporting Policy and procedures.
- 10.2 Such investigation should be consistent with the current national requirements for incident reporting. At the time of writing this Agreement the current requirements are contained in the HSCIC document "Checklist Guidance for Reporting, Managing and Investigating Information Governance Serious Incidents Requiring Investigation".
- 10.3 The identifying organisation will notify other affected organisations as appropriate. In particular the relevant GP Practice (as Data Controller) and the relevant CCG must be informed.
- 10.4 The identifying organisation will also inform the Arden and GEM CSU Information Governance Team ([informationgovernance@gemcsu.nhs.uk](mailto:informationgovernance@gemcsu.nhs.uk)). Where necessary, Arden and GEM CSU will conduct an investigation in accordance with their Incident Reporting policy and procedures and the national requirements, as per 10.2 above. The Arden and GEM CSU will also ensure that the GP Practice and the CCG are informed of any such breach and be kept up to date on the progress and outcomes of the investigation and action taken to prevent further breaches. Where necessary, the HSCIC will also be informed.

## **11 Oversight of Risk Stratification Programme on behalf of GP Practices**

- 11.1 The Risk Stratification programme will be governed by the LLR IM&T Project Board which will maintain strategic oversight of the delivery of the programme. They will co-ordinate and represent the interests of all the Data Controllers (GP Practices) and approve any changes to the programme, for example the inclusion of any newly developed diagnostic codes, or changes to the excluded sensitive diagnostic codes.

The GP representatives of this Board, in consultation the Arden and GEM CSU Information Governance Team, will advise if any proposed changes to the programme require full scale consultation with GP Practices, as Data Controllers, and the issue and signature of a revised Agreement.

- 11.2 In the event that governance of the risk stratification programme switches from the LLR IM&T Project Board to another forum, all GP Practices will be notified, but this will not necessitate re-signing of a new version of this Agreement.

## **12 Review of this Agreement**

- 12.1 This Agreement will be reviewed on an annual basis. A working group will be established by the LLR IM&T Project Board to undertake this review.
- 12.2 The Agreement will be reviewed earlier in the event of a change in legislation or national guidance.

## **13 Patient or Public Requests for Access to Information**

- 13.1 Any request for information under the provisions of the Data Protection Act 1998 will be submitted to the relevant GP Practice for it to process.
- 13.2 Any request under the Freedom of Information Act 2000 will be submitted to the relevant commissioner or GP Practice.

## **14 Previously Signed Risk Stratification Agreements**

- 14.1 Previously signed Agreements for Risk Stratification for Case Finding will remain in force until a new Agreement is signed, or is formally terminated in accordance with the termination clauses of that Agreement.
- 14.2 Previously signed Agreements for risk stratification for case finding will be replaced by a signed version of this Agreement (as this Agreement covers risk stratification for case finding and risk stratification for commissioning) and the former Agreement will become redundant.

## **15 Closure/Termination of Agreement**

- 15.1 This Agreement shall continue in full force and effect for so long as the Data Processors are processing personal data on behalf of the GP Practice for risk stratification, or until it is replaced by a newer version. In the event that there is a change in legislation or guidance, the Agreement will be updated accordingly and reissued.
- 15.2 Any participating organisation can suspend this Agreement for 45 days if security has been seriously breached. Such request should be in writing to the Arden and GEM CSU – [gem.dmic@nhs.net](mailto:gem.dmic@nhs.net)
- 15.3 Any participating organisation can terminate this Agreement. At least 30 days' notice of termination should be given in writing to Arden and GEM CSU - [gem.dmic@nhs.net](mailto:gem.dmic@nhs.net).
- 15.4 Within 30 days following termination of this Agreement, the Data Processor shall, at the direction of the Data Controller, (a) comply with any other agreement made between the parties concerning the return or destruction of data or, (b) return all personal data passed to the Processor by the Controller for processing or, (c) on receipt of written instructions from the Data Controller, destroy all such data unless prohibited from doing so by an applicable law.

## 16 Signatories

AS WITNESS this Agreement has been signed off on behalf of each of the parties by its duly authorised representative:

### 16.1 GP PRACTICE Caldicott Guardian or Senior Partner to sign here

On behalf of my GP Practice, the Data Controller, I agree to the processing of patient data for risk stratification for case finding and risk stratification for commissioning in accordance with the terms and conditions outlined in this Agreement.

<b>Signature:</b> (Caldicott Guardian or Senior Partner)	
<b>Printed Name:</b>	
<b>Job Title:</b>	
<b>GP Practice name and address:</b>	
<b>GP Practice stamp</b>	
<b>Date:</b>	

<b>Practice Code:</b>	
<b>Practice email:</b>	


<b>Clinical System:</b> (Please tick)
--

TPP SystemOne	
------------------	--

EMIS	
------	--


## 16.2 SIRO or Caldicott Guardian for NHS Arden and GEM CSU to sign here

On behalf of the Arden and GEM CSU, a Data Processor, I agree to the processing of patient data for risk stratification for case finding and risk stratification for commissioning in accordance with the terms and conditions outlined in this Agreement.

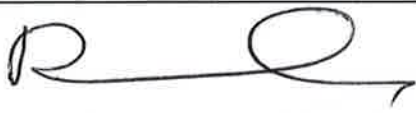
<b>Signature:</b> (SIRO or Caldicott Guardian)	
<b>Printed Name:</b>	Dave Marsden
<b>Job Title:</b>	Director of IT Services and Information Systems and Senior Information Risk Owner (SIRO)
<b>Organisation name and address:</b>	NHS Arden and GEM CSU St John's House East Street, Leicester LE1 6NB
<b>Date:</b>	22 July 2015 22 July 2015

## 16.3 Accountable Officer, SIRO or Caldicott Guardian of the NHS East Leicestershire and Rutland CCG to sign here

This CCG is fully supportive of the use of risk stratification for case finding and for commissioning purposes. On behalf of the CCG, I agree to the terms and conditions outlined in this Agreement.


<b>Signature:</b> Accountable Officer, SIRO or Caldicott Guardian)	
<b>Printed Name:</b>	CARMELO'BRIEN
<b>Job Title:</b>	CHIEF NURSE + QUALITY OFFICER. CALCICOTT GUARDIAN
<b>CCG name and address:</b>	EAST LEICESTERSHIRE + RUTLAND CCG HQ SUITE 2+3, BRIDGE PARK. HEITON ROAD THURMASTON, LEICESTER LE4 8BL.
<b>Date:</b>	4th August 2015.

This CCG is fully supportive of the use of risk stratification for case finding and for commissioning purposes. On behalf of the CCG, I agree to the terms and conditions outlined in this Agreement.

<b>Signature:</b> Accountable Officer, SIRO or Caldicott Guardian)	
<b>Printed Name:</b>	DAWN LEESE
<b>Job Title:</b>	Director of Nursing and Quality and Caldicott Guardian
<b>CCG name and address:</b>	Leicester City CCG St John's House, 6 <sup>th</sup> Floor 30 East St, Leicester, LE1 6NB
<b>Date:</b>	23rd July 2015

**16.5 Accountable Officer, SIRO or Caldicott Guardian of the NHS West Leicestershire CCG to sign here**

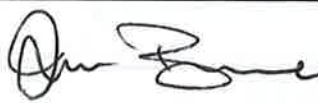
This CCG is fully supportive of the use of risk stratification for case finding and for commissioning purposes. On behalf of the CCG, I agree to the terms and conditions outlined in this Agreement.

<b>Signature:</b> Accountable Officer, SIRO or Caldicott Guardian)	
<b>Printed Name:</b>	CAROLINE TREVITHICK
<b>Job Title:</b>	CHIEF NURSE & QUALITY LEAD.
<b>CCG name and address:</b>	WEST LEICESTERSHIRE CCG 55 WOODGATE LOUGHBOROUGH LE11 2TZ
<b>Date:</b>	22 July 2015



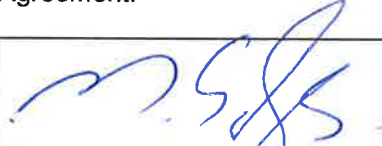
**16.6 Director of Public Health or Deputy Director of the Leicester City Council to sign here**

I agree to the participation in risk stratification for commissioning in accordance with the terms and conditions outlined in this Agreement.

<b>Signature:</b> (Director or deputy director of Public Health)	
<b>Printed Name:</b>	IVAN BROWN
<b>Job Title:</b>	DEPUTY DIRECTOR OF PUBLIC HEALTH
<b>Public Health organisation name and address:</b>	LEICESTER CITY COUNCIL CITY HALL 115 CHARLES STREET LEICESTER.
<b>Date:</b>	29/07/2015.


**16.7 Director of Public Health or Caldicott Guardian of the Leicestershire County Council to sign here**

I agree to the participation in risk stratification for commissioning in accordance with the terms and conditions outlined in this Agreement.

<b>Signature:</b> (Director or deputy director of Public Health)	
<b>Printed Name:</b>	MIKE SANDERS.
<b>Job Title:</b>	DIRECTOR OF PUBLIC HEALTH - LCC.
<b>Public Health organisation name and address:</b>	LEICESTERSHIRE COUNTY COUNCIL, COUNTY HALL CHAMPIONSHIP WAY. GLINFIELD LE18 3QA.
<b>Date:</b>	29/07/2015

**16.8 Director of Public Health or Caldicott Guardian of the Rutland County Council to sign here**

I agree to the participation in risk stratification for commissioning in accordance with the terms and conditions outlined in this Agreement.

<b>Signature:</b> (Director or deputy director of Public Health)	
<b>Printed Name:</b>	MIKE SANDS.
<b>Job Title:</b>	DIRECTOR OF PUBLIC HEALTH.
<b>Public Health organisation name and address:</b>	RUTLAND COUNTY COUNCIL, OAKHAM, RUTLAND.
<b>Date:</b>	24/07/2015.

## 17 Appendix A:

### **Information Governance and Risk Stratification: Advice and Options for CCGs and GPs, Gateway publication 01128**

This risk stratification guidance has been provided by NHS England to ensure legal processing of data for risk stratification purposes. The Arden and GEM CSU implementation of risk stratification for case finding and for commissioning is in compliance with the requirements of this guidance.



Information  
Governance & Risk St

If there is any difficulty in opening the embedded document, please contact:

**Information Governance Team, Arden and GEM CSU**

[informationgovernance@ardengemcsu.nhs.uk](mailto:informationgovernance@ardengemcsu.nhs.uk)

## 18 Appendix B:

### **Risk Stratification Assurance Statement CAG 7-04(A)/2013**

In order to comply with the conditions of the NHS Action 2006 Section 251 approval, CCGs are required to complete the embedded Risk Assurance Statement and submit to NHS England for approval:



Risk Strat assurance  
statement-02-141.pdf

If there is any difficulty in opening the embedded document, please contact:

**Information Governance Team, Arden and GEM CSU**

[informationgovernance@ardengemcsu.nhs.uk](mailto:informationgovernance@ardengemcsu.nhs.uk)

## 19 Appendix C: - Data Extraction Specification

### 19.1 Excluded Read Codes – Patient Opt Out

Data containing an **opt-out code** indicating **patient dissent** for processing of data for risk stratification/multi-professional risk assessment will be excluded from the GP system data extraction. The Arden and GEM CSU will run a secondary check to ensure that such data is not processed for risk stratification:

System	Code
TPP practices (CTV3)	<b>XaJDp</b> (Multi-professional risk assessment declined)
EMIS practices (Read2)	<b>9Oh5</b> (Multi-professional risk assessment declined)

### 19.2 Excluded Read Codes - Legally restricted and sensitive data

Where possible (and subject to how the extraction is undertaken), each patient's record will be extracted **with the exception** of the Read codes which fall into the category of legally restricted or sensitive codes. Arden and GEM CSU will run a further exclusion filter to ensure that no such codes are processed in the risk stratification tool. The list below is only an indicator of the codes excluded. The total list is approximately 3500 codes and is available upon request.

<b>Indicative Read code exclusion filter list</b>
<b>HIV &amp; Aids:</b>
13N5. or 43C% or 43WK. or 43d5. or 43h2. or 43W7. or 43W8. or 4J34. or 62b. or 65P8. or 65QA. or 65VE. Or 67I2. or 6827 or 8CAE. or A788% or A789% or AyuC4 or Eu024 or R109. or ZV018 or ZV019 or ZV01A or ZV19B or ZV6D4 or ZV737
<b>Sexually transmitted diseases:</b>
1415 or 43U% or A9% or A780. or A78A. or A78A3 or A78AW or A78AX or 65P7. or 65Q9. or 6832 or A7812 or L172% or ZV016 or ZV028 or ZV745 or EGTON34
<b>Termination of Pregnancy:</b>
1543% or 6776 or 7E066 or 7E070 or 7E071 or 7E084 or 7E085 or 7E086 or 8M6 or 956% or 9Ea% or 8H7W. or L05% or L06%
<b>IVF treatment:</b>
ZV26% or 8C8% or 7E0A% or 7E1F2
<b>Marital Status: 133%</b>
<b>Complaints: 9U%</b>
<b>Convictions and imprisonment:</b>
13H9. or 13HQ. or 13I71 or 6992 or T776. or ZV4J4 or ZV4J5 or ZV625
<b>Abuse (physical, psychological or sexual, by others):</b>
14X. or 1J3. or SN55. or SN571 or TL7. or TLx4. or ZV19C or ZV19D or ZV19E or ZV19F or ZV19G or ZV19H or ZV19J or ZV19K or ZV4F9 or ZV4G4 or ZV4G5 or ZV612



### 19.3 Data set extracted from GP Practices – for filtering and processing for risk stratification analysis:

#### Patient Information

Field Name	Description
Forenames	Forename(s) including middle name(s) of patient
Surname	Surname of patient
Date of Birth	The day, month and year that the patient was born.
Sex	Gender of the patient
Date of Death	The day month and year that the patient died
House Name Flat Number	House name and flat number
Number and Street	Number and street
Village	Village
Town	Town
County	County
Post Code	Patients postcode district
Ethnicity	The ethnicity of the patient
Ethnicity Code	Read code for ethnicity
Patient Type	Regular, Emergency, etc.
Patient Status	Case load status
Organisation	Organisation patient registered to / Practice patient is registered at
NHS Number	Shows the patients NHS Number, (blank if patient does not have one)
GUID	Unique identifier / internal system references
Patient Number	The unique ID for the patient for internal system use.
RegistrationDate	Date Registered with practice
DeRegistrationDate	Date Deregistered with practice

## Appointment

Field Name	Description
Start Date Time	Start date time for appointment
End Date Time	End date time for appointment
Current Status	Current status of appointment. Did not attend, cancelled, etc.
Arrival Date Time	Time patient arrived
Seen Date Time	Date time patient was seen
Time Booked	Regular, Emergency, etc.
GUID	Unique identifier
User ID Role	Clinician who holds the session
Session Type	Type for the session, Timed Appointment, Untimed Appointments, etc.
Session Location	Location for the session
Patient Number	The unique ID for the patient

## Referral

Field Name	Description
Original Term	Textual description of read code
Referral Reason	The textual reason for referral may also be a version 3 Read code.
Status	The status for this referral, values are: Active, Dormant, Rejected, Ended
Effective Date	The date of the referral
Authorising User	User authorised
Service Type	The source of the referral e.g. self referral, Day Care etc.
Urgency	Urgency of the referral, values are : Urgent Referral, Routine Referral, Referral Soon
Read Code	Read code for referral
Consultation Id	Id of consultation linked
GUID	Unique unit identifier
Patient Number	The unique ID for the patient
Direction	Inbound or Outbound
Transport	None Required, Required, Stretcher
Ended Date	End date of referral
Source Organisation Name	Referring Organisation
Target Organisation Name	Target Organisation
Received Date	Date referral received

## Interactions

### Event/code/problems/ consultations

Diagnosis, consultations, problems, information points and notes

Field Name	Description
Read Code	Read code for event
Original Term	Textual description of read code / describes diagnosis, interaction or event information point.
Numeric Value	The number value of this coded entry / e.g. diagnosis, Temperature reading etc
Numeric Units	Units of numeric value / e.g. temperature value
Effective Date	The date and time that the coded entry was recorded / e.g. date of diagnosis, problem or temperature reading etc
Episodicity	None, First, New, Review, Flare Up, Ended, Changed, Evolved
Associated Text	Additional text for event / notes
Type of Staff	Type of staff seeing patient
Authorising User	User authorised
Organisation	Organisation patient belongs to
Consultation Id	Id of consultation linked
GUID	Unique unit identifier
Patient Number	The unique ID for the patient
Abnormal	Abnormal
Abnormal Reason	Reason for abnormality
Status	Active, past, etc.
Significance	Major, Minor
Last Review Date	Problem last review date
End Date	Problem end date
Location	Location of consultation
Duration	Duration

## Medication

Field Name	Description
Read Code	Read Code for medication
Original Term	Textual description of the read code
Effective Date	The date and time that the medication was recorded
Authorising User	Authorising user for diary entry
GUID	Unique unit identifier
Patient Number	The unique ID for the patient
Dosage	Dosage for medication
Quantity	Quantity for medication
Quantity Units	Units for the medication
Prescription Type	Acute, repeat, dispensed, automatic
Drug status	Active, cancelled, never active
Expiry Date	Date of expiry
Review Date	Date of medication review
No of Authorised Issues	Number of issues authorised
Course Duration	Course duration in days
Most Recent Issue Method	Most recent issue method
Most Recent Issue Date	Most recent issue date
Number of Issues	Number of issues
Patient Text	
Pharmacy Text	
Prescribed as Contraceptive	
Privately Prescribed	
Consultation ID	Id of consultation linked
Prescription Type	Acute, repeat, dispensed, automatic
Estimated NHS Cost	
Issue Method	Issue method
Script Pharmacy Stamp	
Compliance	
Average Compliance	
Cancelled	

## 20 Appendix D

### Guidance on Data Controller and Data Processor responsibilities

The Information Commissioner's Office has provided guidance to help in understanding the difference between a data controller and a data processor, and their roles and responsibilities.

The document is entitled "Data controllers and data processors: what the difference is and what the governance implications are", version 1, 20140506.

The full guidance document is available from the Information Commissioner's Office website:  
<https://ico.org.uk/media/for-organisations/documents/1546/data-controllers-and-data-processors-dp-guidance.pdf>

The following is an extract from guidance to support this Agreement:

### Overview

It is essential for organisations involved in the processing of personal data to be able to determine whether they are acting as a data controller or as a data processor in respect of the processing. This is particularly important in situations such as a data breach where it will be necessary to determine which organisation has data protection responsibility.

The **data controller** must exercise overall control over the purpose for which, and the manner in which, personal data are processed. However, in reality a data processor can itself exercise some control over the manner of processing – e.g. over the technical aspects of how a particular service is delivered.

### Section 1 - What is the difference between a data controller and a data processor?

#### What the Data Protection Act (DPA) 1998 says

1. The DPA draws a distinction between a 'data controller' and a 'data processor' in order to recognise that not all organisations involved in the processing of personal data have the same degree of responsibility. It is the **data controller that must exercise control over the processing and carry data protection responsibility for it**. This distinction is also a feature of Directive 94/46/EC, on which the UK's DPA is based.
2. Section 1(1) says that:  
  
    **"data controller"** means a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be processed  
  
    **"data processor"**, in relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller.



**“processing”**, in relation to information or data means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including—

- a) organisation, adaptation or alteration of the information or data,
- b) retrieval, consultation or use of the information or data,
- c) disclosure of the information or data by transmission, dissemination or otherwise making available, or
- d) alignment, combination, blocking, erasure or destruction of the information or data

3. The definition of processing can be useful in determining the sort of activities an organisation can engage in and what decisions it can take within its role as a data processor. The definition of ‘processing’ suggests that a data processor’s activities must be limited to the more ‘technical’ aspects of an operation, such as data storage, retrieval or erasure. Activities such as interpretation, the exercise of professional judgement or significant decision-making in relation to personal data must be carried out by a data controller. This is not a hard and fast distinction and some aspects of ‘processing’, for example ‘holding’ personal data, could be common to the controller and the processor.

## **21 Appendix E - Security Measures to be adhered by the Data Processor (Arden and GEM CSU)**

Arden and GEM CSU have a full set of information governance policies in place to meet the requirements of the NHS information Governance Toolkit, Level 2 and will ensure the secure risk stratification data processing.

In summary, the following information security requirements are the minimum requirement:

### **21.1 Security – General**

The Data Processors shall not under any circumstances share, disclose or otherwise reveal NHS Information (in whole or in part) to any individual, business or other organisation (3<sup>rd</sup> party) unless explicitly covered by the Data Processing Agreement or by seeking explicit written consent of the Data Controller.

### **21.2 Security – Physical**

The Data Processors shall ensure that all NHS information is physically protected from accidental or deliberate loss or destruction arising from environmental hazards such as fire or flood.

The Data Processor shall ensure that all NHS information is held on premises that are adequately protected from unauthorised entry and/or theft of NHS Information or any IT equipment on which it is held by, for example, the use of burglar alarms, security doors, ram-proof pillars, controlled access systems, etc.

### **21.3 Security – IT Systems**

21.3.1 The Data Processors shall hold electronically-based NHS information on secure servers unless otherwise agreed in writing.

21.3.2 The Data Processors shall ensure that:

- All portable media used for storage or transit of NHS information are fully encrypted in accordance with NHS Guidelines on encryption to protect personal information (January 2008).
- Portable media are not left unattended at any time (e.g. in parked cars, in unlocked and unoccupied rooms, etc.).
- When not in use, all portable media are stored in a locked area and issued only when required to authorised employees, with a record kept of issue and return.
- The Data Processors shall not allow employees to hold NHS Information on their own personal computers.
- The Data Processors shall ensure adequate back-up facilities to minimise the risk of loss of or damage to NHS information and that a robust business continuity plan is in place in the event of restriction of service for any reason.

21.3.3 The Data Processors shall not transmit NHS information by email except as an attachment encrypted to 256 bit AES\Blowfish standards or from NHS mail to NHS mail.

21.3.4 The Data Processor shall only make printed paper copies of NHS information if this is essential for delivery of the contracted service.

- 21.3.5 The Data Processor shall store printed paper copies of NHS information in locked cabinets when not in use and shall not remove from premises unless this is essential for delivery of the contracted service.
- 21.3.6 The Data Processor shall provide the Data Controller with a signed Information Governance Statement of Compliance (IGSoC) (as confirmation of achieving level 2 in respect of the NHS Information Governance Toolkit) OR evidence of compliance with another agreed Information Security Management System (ISMS), before the Data Controller can allow any access to networked IT systems (e.g. N3, Summary Care Record, etc).
- 21.3.7 Subject to ISMS assurance requirements specified at 10.8, The Data Processor shall register as a NHS Business Partner at <http://www.connectingforhealth.nhs.uk/systemsandservices/infogov/igsoc/nonnhs> for IGSoC.

#### **21.4. Secure Destruction**

- 21.4.1 The Data Processors shall ensure that NHS information held in paper form regardless of whether as originally provided by the Data Controller or printed from the Data Processors' IT systems) is destroyed using a cross cut shredder or subcontracted to a confidential waste company that complies with European Standard EN15713.
- 21.4.2 The Data Processors shall ensure that electronic storage media used to hold or process NHS Information is destroyed or overwritten to current CESG standards as defined at [www.cesg.gov.uk](http://www.cesg.gov.uk)
- 21.4.3 In the event of any bad or unusable sectors that cannot be overwritten, the Data Processors shall ensure complete and irretrievable destruction of the media itself.
- 21.4.4 The Data Processors shall provide the Data Controller with copies of all relevant overwriting verification reports and/or certificates of secure destruction of NHS information at the conclusion of the contract.

## 22 Appendix F - Document Control

Document Creation			
Date	Author	Version	Description
11/12/15	<ul style="list-style-type: none"> <li>Byron Charlton</li> <li>Marie Matthews</li> </ul> IG Consultants for Arden & GEM CSU	0.1	This Agreement for Risk Stratification for Case Finding and for Commissioning purposes, was created by the Information Governance (IG) Team of Arden and GEM CSU, based upon the Risk Stratification Information Sharing and Data Processing Agreement for Case Finding already in place.

Change/Amendment History			
Version	Date	Author	Changes
0.2	19/1/15	Byron Charlton & Marie Matthews	Draft updated to reflect NHS England advice for CCGs and GPs (Appendix A)
0.3 & 0.5	January-February 2015	Marie Matthews Mark Pierce	Draft updated to include feedback from internal consultation exercise within Arden and GEM Information Governance and Development Teams, along with additional clarification from author and support from Mark Pierce, Strategy and Planning Officer, Leicester City CCG.
0.5	2/3/15	Marie Matthews	Circulated for consultation to all 3 CCGs
0.6	2 2/3/15	Marie Matthews	No changes following consultation with all 3 CCGs but in further consultation with Mark Pierce Section 12 on governance of the programme was added. The data set tables in Appendix C, Section 19.3, were amended to reflect the dataset from each System Supplier, following recent changes to the way in which TPP submits the data.
0.6	30/3/15	Mark Pierce	Submitted to the Leicester, Leicestershire and Rutland Local Medical Committee for consultation.
0.6	10/6/15	Mark Pierce Marie Matthews	Reviewed by LLR Local Medical Committee and clearance to offer of this Agreement out to Practices for their consideration was granted.
1.1	10/7/15	Marie Matthews	Document converted to final version and ready for issue following LLR IM&T Strategy Group meeting.

Reviewers
This document has been reviewed by the following:
Byron Charlton, Information Governance Consultant, NHS Arden and GEM CSU
Lisa Wakeford, Head of Information Governance Service, NHS Arden and GEM CSU
Ayub Bhayat, Head of Data, Development and Integration, NHS Arden and GEM CSU
Dave Marsden, Director of Information and It Services, NHS Arden and GEM CSU
Mark Pierce, Strategy and Planning Officer, NHS Leicester City CCG
LLR IM&T Project Board on 12/03/2015
Carmel O'Brien, Caldicott Guardian, NHS East Leicestershire and Rutland, CCG
Caroline Trevithick, Caldicott Guardian, NHS West Leicestershire CCG
Dawn Leese, Caldicott Guardian, NHS Leicester City CCG
Leicester, Leicestershire and Rutland Local Medical Committee on 10/06/2015

