North Norfolk CCG
South Norfolk CCG

DATA PROTECTION IMPACT ASSESSMENT REPORT
January 2019

1. This report has been prepared as part of the Information Governance (IG) mechanisms of the Risk Stratification suppliers and Data Processor, NHS Arden and Greater East Midlands Commissioning Support Unit (AGCSU).

2. The DPIA for this Risk Stratification Programme is informed by requirements set out in the NHS England Risk Stratification Assurance Statement and by an NHS England Privacy Impact Assessment (PIA) for risk stratification, available at the end of this document in Annex 2.

3. The context of the Data Protection Impact Assessment promoted by the AGCSU is to enable the facilitation of fair, lawful and proportionate data processing activities in relation to the programme for risk stratification for case finding and risk stratification for commissioning purposes so that the benefits far outweighing any data protection risks relating to any associated data processing activities.

4. The CCG (NHS North Norfolk CCG and NHS South Norfolk CCG CCG) have commissioned a Risk Stratification Programme. The Risk Stratification Programme comprises a:
   4.1. Risk Stratification for Case Finding Programme – that involves clinical care related decision making to directly support individuals and involves the direct use of a patients Personal Confidential Data; and
   4.2. Risk Stratification for Commissioning Programme – that is population based and does not involve the direct use of patients Personal Confidential Data.

5. On behalf of their General Practice member, the CCGs have procured the services of AGCSU as the supplier of the Risk Stratification Programme.

6. The Risk Stratification Programme is informed by requirements set out in the NHS England Risk Stratification Assurance Statement - https://www.england.nhs.uk/wp-content/uploads/2016/07/risk-stratification-ass-statement.pdf and Privacy Impact Assessment related exercises undertaken by NHS England - https://www.england.nhs.uk/ourwork/tsd/ig/ig-consultations/priv-impact-assess/

7. The purpose of the programme is to focus on adults who are at higher risk of hospital admission and/or have complex needs, with the aim of delivering improved outcomes; access to more integrated care outside of hospital; a reduction in unnecessary hospital admissions; and enable effective working of professionals across provider boundaries.

8. The Risk Stratification Programme will require primary care data from General Practices and CCG commissioning data (made available by NHS Digital/Data Services for Commissioners Regional Office (DSCRO). The risk stratification tool does not require identifiable data.

9. AGCSU will act as a data processor on behalf of General Practices to receive identifiable data from the GP Systems Suppliers into a secure environment especially created for risk stratification. AGCSU will de-identify the data as soon as it is received. The data will contain a pseudonym for the purpose of linking it to the CCG commissioning data. The data will fall into the category of 'anonymised in accordance with the ICO Anonymisation Code of Practice'. The data will fall outside the scope of data protection regulations but will still require controls to minimise any risk of inappropriate re-identification.

10. AGCSU will segregate the identifiable and de-identified data. De-identified data will be used for the risk stratification, but there will be a link to the identifiable data for authorised users of each General Practice who need to re-identify for direct care purposes. There will be strong access controls surrounding this.

11. AGCSU will also receive commissioning data from NHS Digital/DSCRO on behalf of the CCGs.

12. Both sets of de-identified data will be fed into the risk stratification tool.

13. The legal basis that supports the risk stratification programme is:

    (a) Articles 6(1)(e) and 9(2)(h) of GDPR:
    - **Articles 6(1)(e) -** processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
    - **Article 9(2)(h)** - processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3 of Article 9.

    (b) Common Law Duty of Confidentiality
    This is set aside as the data will be de-identified therefore any disclosure will not represent a breach of confidentiality. Additionally, sharing for the purposes of risk stratification and health care planning is presumed to be within the "reasonable expectations" of patients – in accordance with the findings of the 2012 Caldicott Review. Controller Fair Processing materials also serve to raise the "reasonable expectations" of patients through specifically mentioning this information sharing.

14. The stakeholders involved in the CCGs' Risk Stratification Programme currently include:
    14.1. Patients;
    14.2. General Practices that constitute the membership of the CCG;
    14.3. NHS North Norfolk CCG;
    14.4. NHS South Norfolk CCG;
    14.5. NHS England; and
    14.6. NHS Digital.

15. The NHS England Risk Stratification Privacy Impact Assessment (PIA) Report of 2014 iterates the need for a further local Risk Stratification impact assessment. The NHS England Risk Stratification Guidance of 2018 recommends the following:
    15.1. To ensure there is a legal basis for the processing of the data; and
    15.2. To ensure there are appropriate and robust information governance controls in place; and
    15.3. To clarify and document data controllership and lines of accountability;
    15.4. To put in place appropriate contractual arrangements and managing these arrangements; and
    15.5. To ensure patients are informed about how their data will be used; and
    15.6. To put in place mechanisms that enable patient's objections to be respected.

16. A key starting point for DPIA exercises is to assess the implications of relationships, data controllership authority and lines of accountability. This is because the potential/actual data protection relationship context and consequent governance mechanisms [to be] employed between stakeholder organisations involved in a data processing activity impact upon:
    16.1. The fair, legitimate and proportionate reasons upon which stakeholders can rely to run the risk stratification programme, either through direct collection from individuals or through indirect collection from other organisations.

17. Clarity about relationships, data controllership authority and lines of accountability is particularly important for the Data Controller-Data Processor relationship because:
    17.1. a Data Processor, as a supplier, is an honest broker organisation;

    17.2. a Data Controller may be obliged to instruct the Data Processor to grant access to the Data Controller's Risk Stratification information via the Data Processor's Risk Stratification systems to General Practice aligned staff;

    17.3. the Data Controllers' and Data Processor's business models and reputation as providers of NHS services, require all Parties to be heavily dependent on the confidence in their information governance (IG) related endeavours and associations;

17.4. the status of the data controllers fluctuates between sole data controller and joint data controller.

17.5. the NHS England Risk Stratification Assurance Statement obligations require the Data Controllers and Data Processor to seek to know and control risk implications relating to re-identification issues and the legitimacy of providing access to the Data they are processing;

17.6. this iteration of a Data Protection Impact Assessment is therefore focused on identifying and assessing potential roles, relationships, known governance mechanisms [to be] employed regarding access to and the utility of re-identified Personal Confidential Data from the perspective of the Data Controller and the Data Processor;

17.7. it identifies in Table 1, the stakeholder analysis and potential accountability and relationship context that has consequent implications regarding the re-identification of Personal Confidential Data.

Impact Findings

18. Table 1 on page 3 below provides potential impact findings and potential recommendations for consideration and action. It is clear that the nature, form and governance mechanisms underpinning the IG relationships between Risk Stratification stakeholders and how these are executed is material in enabling Risk Stratification to deliver from a data protection perspective, Fairness and transparency i.e. benefits of the Purpose far outweigh the data processing risks.

19. The summary of the local data protection impact assessment is:

13.1 For a fair, lawful and proportionate basis to be reflected in the Risk Stratification programme, CCGs and by the General Practices need to make their patients aware of the programme and its benefits; how their data is used and that they have the right to opt-out of their data being included. They need to be aware of how to engage the General Practice's opt-out process. All possible opportunities should be engaged to deliver the message, e.g. patient newsletters, General Practice noticeboards and websites. It is part of the risk stratification project plan that the Privacy Notices will be updated prior to Go Live. CCGs and Practices will also be encouraged to utilise any other patient engagement opportunity available to deliver the message.

13.2 Whilst GP Practice System Suppliers will transfer PCD level data to the risk stratification supplier, it will be transferred by secure means and de-identified upon landing. PCD required to support the re-identification process will be segregated . Any PCD not required will be deleted as soon as the processing has been completed. De-identified data will be used for the risk stratification processing and not PCD. The commissioning data received will have already been de-identified before receipt. The processing of PCD is at the minimum level possible.

13.1 General Practices are required to ensure that they only provide authority for their staff with a legitimate relationship with the patients to have access to PCD level data and that the staff will only access such data for direct care purposes.

13.2 The nature and form of the Agreements in relation to the Risk Stratification Programme should be supportive of each Party to enable each to confidently demonstrate and give effect to their complex data sharing legal obligations and NHS policy requirements. It is anticipated that the Data Sharing and Data Processing Agreement that will be prepared for signature by each CCG, the risk stratification supplier and each participating General Practice, will meet this requirement.

14 Conclusion:

This risk stratification programme can deliver significant benefits to the CCGs, General Practices and patients.

Provided all the requirements of the NHS England Risk Stratification Assurance statement are met, then it is concluded that this risk stratification programme will have taken all appropriate measures to comply with Data Protection Legislation, protecting patient privacy and patient right's. It is

recommended that CCGs and General Practices start their patient engagement programme as soon as possible. Assurance will be obtained by the project team methodology that all the requirements of the NHS England Risk Stratification Assurance Statement will be met before the programme goes live. All of the controls and requirements will be contained within a Data Sharing and Processing Agreement which will be signed by all participating organisations before the programme goes live. It is concluded that this programme offers significant benefit to the CCGs, General Practices and patients. All risk to data protection obligations have been minimised and the benefits of the programme far outweigh those.

The risk stratification analysis will produce an automated risk profile of patients. This profile will allow authorised GP Practice staff to make decisions about suitable interventions. Therefore, whilst there is an element of automated profiling, there is always human involvement by authorised GP Practice staff in making decisions about the management and treatment of patients.

Therefore, there does not appear to be an impact on the legal rights of any individual nor any significant negative effect for those having decisions made about them. Where GP Practice staff have identified risk and feel an intervention or care option is appropriate, the individual being profiled is likely to benefit from any decisions made. Additionally, an individual retains choice and control about whether to take options provided to them such as referral to a third-party healthcare provider.

The risk of re-identification of individuals, other than by authorised users from the relevant GP Practice, is deemed unlikely, un-reasonable and remote.

Since the processing for this risk stratification programme does not fully match the data protection definition of automated decision-making and profiling, it is concluded that the processing can proceed without the need for any additional restrictions under GPDR Article 22.

The programme will have all the appropriate measures and controls to protect patient privacy and comply with Data Protection Legislation provided all the requirements of the NHS England Risk Stratification Assurance statement are met. The benefits far outweigh any data protection risks. The submission of the completed Assurance Statement to NHS England will provide confirmation that the requirements will be met.

Report prepared by:

Marie Matthews
Senior Manager – Data Controls and Governance
Data and Systems
NHS Arden and Greater East Midlands Commissioning Support Unit
Marie.matthews@nhs.net
23 January 2019

The input from Emma Cooper, DPO for North Norfolk CCG GP Practices is gratefully acknowledged.

Annex 1

Table 1 - Locally Assessed Stakeholders, Roles, Potential Impacts and Potential Mitigating Measures

Stakeholder	Risk Stratification Role	Potential Impact	Potential Mitigating/Control Measures for the Data Controller
Patient	Risk Stratification for Case finding related decisions are to be applied to benefit individual patients. Required to be offered opportunities to opt out and not be surprised about Risk Stratification activities A legitimate clinical relationship should exist with the patient for the use of patient's re-identified Personal Confidential Data for direct care purposes.	Potential for patients to lose trust in the confidential nature of the health service. Potential for unfair and unlawful processing of personal confidential data. Potential evidence base to support Risk Stratification for case finding may be lessened if patients opt out of the Programme. Activities of the Data Controller in relation to patients must be seen to demonstrate that benefits far outweigh the risks of data processing.	• Actively promote transparency and communication activities (how we use your information) above and beyond the norm in relation to Risk Stratification, so that there are no surprises such as on the websites of practices, Practice newsletters and noticeboards and CCG websites. • Enable and support an informed opt-out process. • Provide assurance that only Practice staff will access PCD level data when they need to do so for the direct care of the patient.
General Practice	Originating and superior Data Controller for all matters to do with Risk Stratification. Authorisation of access to its Risk Stratification information. Re-identification necessary at times to support direct care, for example when risk scores are high and discussions need to take place/decisions need to be made in relation to optimum care for the patient.	Will determine how fair, legitimate and proportionate the processing is. Will inform instructions to the data processor regarding Data Processors relating to the granting of access to Personal Confidential Data is.	• The General Practice should only instruct the Data Processor to undertake actions where the General Practice (Data Controller) considers the impacts of any instruction to be fair, lawful and proportionate, e.g. when intending to authorise access to their risk stratification information at identifiable level, to staff with a direct clinical care relationship with the patient for the purpose of direct care. • General Practices will only enable the sharing of primary care data when they have signed the Data sharing and Processing Agreement for Risk Stratification. • General Practices will have an opt-out process available to patients and will apply an opt-out code to the record of any patient who does want to be included in the risk stratification programme. .
Clinical Commissioning	Driving the use of Risk Stratification as a core component of its delivery mechanism	Delivery mechanism and strategy for Risk Stratification and integrated care is	• The CCGs and General Practice risk stratification privacy notices strategy should be inclusive of the data sharing

Stakeholder	Risk Stratification Role	Potential Impact	Potential Mitigating/Control Measures for the Data Controller
Group	for delivering its commissioning integrated care strategy. Procurement of supplier services as an Agent on behalf of the General Practices. CCG is not currently regarded as the Originating or Superior Data Controller for Risk Stratification purposes (it is the General Practice. Requires Risk Stratification Information for Commissioning Purposes i.e. no access Personal Confidential Data and no re-identification ability.	made clear to General Practices by the CCG. General Practices should be supported were necessary by the CCG to ensure that the General Practices are satisfied with the controls in place for secure and confidential processing for risk stratification purposes. Controls will be in place to ensure that CCG staff do not have the ability to identify individuals, either deliberately or inadvertently.	and processing agreement when Risk Stratification issues are being actively communicated to their patient population. • The CCG must complete and comply with the requirements for risk stratification suppliers within the NHS England Risk Stratification assurance statement. These assurance statements must be duly signed and submitted to NHS England before Go Live. • All data that is processed for risk stratification is de-identified i.e. all attributes that could possibly be associated with a specific individual will have been removed. The data will have been de-identified in accordance with the ICO Anonymisation Code of Practice, which is still an applicable document and standard. Neither the CCG nor AGEM CSU will hold any other datasets if linked to risk stratification would enable re-identification. In addition both organisations will commit through a signed Agreement that will not attempt to re-identify data. • Further publication of data outside of the CCG or GP Practice will require small number suppression. • This risk stratification programme has been running for several years in other areas. There are no known incidents of intentional or accidental inappropriate rep-identification. • There will be a mechanism in place for authorised GP Practice staff to re-identify patients when they need to do so. AGEM CSU will accept grant PCD level access when it has been authorised by Caldicott Guardian/IG Lead of the Practice (or other authorised approved as delegated by the Practice) • The risk of re-identification of individuals, other than by authorised users from the relevant GP Practice, is deemed unlikely, un-reasonable and remote.
GP Practice and CCG as joint	Validation, matching, application of algorithms and presentation of risk	The risk stratification analysis will produce an automated risk profile of	The automated risk stratification profile will allow authorised GP Practice staff to make decisions about suitable

Stakeholder	Risk Stratification Role	Potential Impact	Potential Mitigating/Control Measures for the Data Controller
data controllers	stratification outputs – where GP Practices and the CCG are now jointly responsible for data held in the shared controlled processing environment of the data processor controlled risk stratification environment (Joint Data Controllers)	patients.	interventions. Therefore, whilst there is an element of automated profiling, there is always human involvement by authorised GP Practice staff in making decisions about the management and treatment of patients. Since the processing for this risk stratification programme does not fully match the data protection definition of automated decision-making and profiling, it is concluded that the processing can proceed without the need for any additional restrictions under GPDR Article 22. Therefore, there does not appear to be an impact on the legal rights of any individual nor any significant negative effect for those having decisions made about them. Where GP Practice staff have identified risk and feel an intervention or care option is appropriate, the individual being profiled is likely to benefit from any decisions made. Additionally, an individual retains choice and control about whether to take options provided to them such as referral to a third-party healthcare provider.
Risk Stratification Supplier/Data Processor	Commissioned by the CCG to provide a Risk Stratification Tool and outputs. Obliged to work as a Data Processor to two Parties: the General Practice and the CCG. Required to communicate and satisfy NHS England Risk Stratification Assurance Statement requirements. Required to ensure that sensitive and legally protected data is not processed for risk stratification purposes.	Complexity of Risk Stratification assurance issues requires the Data Controller and Data Processor to harmoniously and collaboratively work together to satisfy national requirements.	• Data Controller to Data Processor relationship context should be through a contract agreement that enables a mutually balancing Data Controller/ Data Processor relationship context. A Data Sharing and Data Processing Agreement will be signed by each CCG, the CSU as Data Processor and risk stratification supplier and each participating member General Practice. • Data Processor must act in accordance with the instructions of the Data Controllers in relation to the risk stratification data, which will be contained in the Data Sharing and Data Processing Agreement. • The Data Processor must complete and comply with the requirements for risk stratification suppliers within the NHS England Risk Stratification assurance statement. Arden and GEM CSU have signed the appropriate

Stakeholder	Risk Stratification Role	Potential Impact	Potential Mitigating/Control Measures for the Data Controller
			section of other CCG Risk Stratification Assurance Statements confirming compliance with the NHS England requirements. The Processes used for this programme will be the same as previously used. AGCSU will sign the risk stratification statement for North Norfolk CCG and South Norfolk CCG when asked to do so by the CCGs. The assurances that AGCSU give include: o Safe Haven controls for the secure processing of all data o De-identification of PCD level primary care data (on behalf of GP Practices) upon landing and deletion of PCD as quickly as possible. o Access control procedures whereby access will only be granted to risk stratification outputs/reports in accordance with the approval of the data controller organisations. o A process to ensure that any record with risk stratification opt-out codes, will not be processed for risk stratification o A process to ensure that sensitive/legally restricted codes are not included in the risk stratification programme as per the NHS England risk stratification assurance statement. o Type 1 opt-out codes (or National Data Opr-outs) will not need to be applied. AGEM CSU will be de-identifying the data on behalf of GP Practices. When the de-identified data leaves the safe haven for primary care data, it is being released on behalf of the GP Practices and so effectively this means that the GP Practice is releasing de-identified data for the purpose of risk stratification.
NHS England	Oversight of compliance with Risk Stratification activities nationally. Represented General Practices in initiating exemptions to the Common Law Duty of Confidentiality	To hold every organisation involved in Risk Stratification to account	• Data Processor and Risk Stratification Procuring CCG should maintain a supplier Risk Stratification Risk log and communicate accordingly through internal and external governance mechanisms. • The submission of a risk stratification assurance statement by the Procuring CCG and the risk stratification

Stakeholder	Risk Stratification Role	Potential Impact	Potential Mitigating/Control Measures for the Data Controller
			supplier. • NHS England maintains a register of all CCGs approved to undertake risk stratification and who their risks stratification supplier is. • NHS England also maintains a list of approved risk stratification suppliers.
NHS Digital	Provisions Secondary Care Data for Risk Stratification Purposes. Requires CCG to adhere to Data Sharing Contract and Agreement before providing Secondary Care Data for Risk Stratification processing.	Management of National Data Opt-Out codes and application of opt codes may impact on its data flows received. Lack of control over the use of the data.	• NHS Digital/DSCRO will only be releasing commissioning data in a format which is anonymised in accordance with the ICO Code of Practice i.e. de-identified. Therefore, National Data Opt-Out codes do not need to be applied. • There are controls in place to ensure no inappropriate re-identification. Re-identification only takes place for direct care purposes, which does not require the application of National Data Opt-Outs. • Both CCGs have the required Data Sharing Framework Contract and Data Sharing Agreement for commissioning purposes in place. • CCGs to actively promote transparency and communication activities (how we use your information) in relation to Risk Stratification, so that there are no surprises e.g. in Practices on the Practice and CCG websites.

Annex 2 - NHS England Overarching Risk Stratification

NHSE
priv-imp-assess.pdf