CAG 7-04(a)/2013 compliance for CCGs – Valid until 31st March 2017

The application from NHS England on behalf of GPs, as the relevant data controllers, seeking support for the activity of risk stratification to be used by GPs supported by CCGs to target specific patient groups and enable clinicians with the duty of care for the patient to offer appropriate interventions, has been approved.

NHS England has given an undertaking to the Secretary of State for Health to seek assurance from eligible organisations and to provide a register of approved organisations for the receipt and processing of the patient data for this purpose. As such NHS England is seeking assurance from Clinical Commissioning Groups and their appointed risk stratification suppliers to provide assurance that processing of the data is in accordance with the Data Protection Act 1998[1] and that the conditions set out for processing of personal confidential data are undertaken and maintained.

It should be noted that this approval only applies to the use of GP and SUS data and does not cover disclosure of social care data for risk stratification. Where social care data are to be used then the relevant parties need to assure themselves there is a legal basis for the disclosure and linkage for this purpose. This can be achieved using a third party and pseudonymised data or with consent.

Please complete Section A and return it to NHS England via email: england.riskstratification@nhs.net to provide assurance that your organisation and risk stratification toolset is in compliance with the requirements for processing outlined in the approval letter CAG reference CAG 7-04(a)/2013. Compliance with these requirements is necessary for the processing to be lawful.

Section A: Assurance Statement

1. To provide assurance that CCGs as the commissioner of the risk stratification service have appropriate agreements in place with their GP practices and contractual levers in place to ensure that the risk stratification supplier (data processor) is acting in accordance to the conditions set out by CAG approval letter. The organisation will ensure it meets the requirements set out below, which NHS England reserves the right to audit.

   1.1 Only named and existing risk stratification suppliers and existing contracts[2] listed in the latest version of the Risk Stratification register available on the NHS England website are eligible to provide risk stratification services under the conditions set out in CAG 7-04(a)/2013

   1.2 Support is provided up to and including **31st March 2017.** CCGs are required to collaborate with NHS England to implement a data standard for risk stratification that minimises the use of patient confidential data.

   1.3 CCGs agree to work in collaboration with NHS England and HSCIC to identify and work towards an agreed exit option(s).

[1] http://www.legislation.gov.uk/ukpga/1998/29/contents

[2] Whilst contracts between NHS bodies would be NHS contracts under Section 9 of the NHS Act 2006 and therefore not legally enforceable, the contracts with independent sector risk stratification toolset suppliers must be legally binding contracts to satisfy principle 7 of the DPA.

1.4 The CCG will ensure that the risk stratification supplier also completes and returns the assurance statement in Annex 1.

Please tick appropriate boxes below to indicate acceptance of conditions

Name of risk stratification supplier _____ ☐

There is a current and signed contract in place with the risk stratification supplier ☐

There is a data processing contract in place between the relevant practices as data controllers, the CCG acting as their agent and one of the named risk stratification suppliers (data processor) and this contract sets out the requirements for adequate controls and provisions for handling patient confidential data, including provisions in place in the event of a data breach and retention and destruction at termination of contract. ☐

The risk stratification supplier (data processor) meets the IG Toolkit at a minimum level 2 or equivalent standards (e.g. ISO 27001 accredited) ☐

The GP practice, CCG and data processers have in place a process and mechanisms for handling patient objections ☐

The CCG has in place an arrangement with a HSCIC regional Office (DSCRO) on behalf of the relevant GP practices for the data processor to receive secondary use data (SUS) for inclusion into risk stratification tool ☐

Name of DSCRO _____

Or Will not be using SUS data in the risk stratification tool

2 **The CCG undertakes to ensure that**:

No.	Condition
2.1	The relevant staff have read, understood and implemented the requirements within the risk stratification checklist referenced in Annex 3.
2.2	Member GP practices are made aware of their responsibilities as data controllers, and have in place an agreement with the CCG in respect of the CCG acting as an agent of the GP practice in relation to the use of the GP data (and SUS data, where applicable) for the purposes of risk stratification.
2.3	It has made arrangements to ensure that the public understand the proposed use of data for risk stratification purposes between a commissioner and a provider of NHS funded health services. (This may be achieved through fair[3] processing notices by CCG and its member practices). This should include an explanation of risk stratification, clarity about who the data controller and data processors are, what type of data will be used for risk stratification, the rights individuals can exercise in relation to this i.e. the right to access their personal data and to object to its use for this purpose and how to exercise this right. **Please add a link below to your Fair Processing Notice (FPN) on your CCG website:** [ ]
2.4	It has agreed a process with GP Members on how patient objections will be handled
2.5	Risk stratification suppliers will process personal confidential data (PCD) in the following manner: Data is received in a "de-identified data for limited access"[4] form (i.e. NHS number as the patient identifier) or is pseudonymised on landing; AND Processing is within a "closed box" with strict role based access control; AND Re-identification is solely for the purpose of direct care and is available only to those with a direct clinical care relationship with the patient. Any publication of data other than in accordance with 2.5.3 must be anonymised in line with the ICO Anonymisation Code of Practice
2.6	It has ensured that all staff handling data for the purpose of risk stratification are made aware and will operate in compliance with the requirements of Section 251 approval.
2.7	The named risk stratification supplier processes the minimum data necessary (ie. the data specifications will have specific exclusions for sensitive information [5] (see

[3] See http://www.england.nhs.uk/wp-content/uploads/2013/06/ig-risk-ccg-gp.pdf Annex 3 FAQs 8 & 9

[4] As defined in the Caldicott Information Governance Review, *To Share or not to share*, Department of Health April 2013 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/192572/2900774_InfoGovernance_accv2.pdf [pp 127]

	Appendix 4), and will only utilise the minimum data necessary to identify the candidate risk cohorts).
2.8	The named risk stratification supplier will provide a written procedure outlining a secure mechanism for receipt and processing of data within the risk stratification tool. These should include as a minimum the process for: Receipt of data; Retention period; Role based access controls, authorisation and maintenance; Induction and training processes for users; How audit trails will be maintained and confidentiality audits may be undertaken.
2.9	Staff using the risk stratification toolset and reports will receive formal training and can demonstrate they are working in compliance to the written procedure.
2.10	Staff handling patient confidential data are made aware of and will operate in compliance with the obligations set out in the confidentiality clauses in their contract of employment and, where applicable, their professional obligations. Any suspected data breach relating to risk stratification must be subject to the CCG's and NHS England's data breach reporting mechanisms.
2.11	It has appropriate processes and contractual provisions with the risk stratification tool supplier to securely destroy all PCD held in manual or electronic form once deemed it is no longer necessary for the purpose of risk stratification.
2.12	It works with risk stratification suppliers to make provision for the transition towards the exit strategy defined by NHS England
2.13	It undertakes to carry out a check on its risk stratification suppliers and their processes to ensure that it has taken all reasonable organisational and technical measures to prevent unlawful processing of the PCD held for risk stratification purposes. **Insert date of check below:** **Date of Check:** | **Meets requirements: Yes/No**
2.14	It undertakes a Privacy Impact Assessment for risk stratification in accordance to the ICO guidance: http://ico.org.uk/pia_handbook_html_v2/html/0-advice.html

We undertake to ensure the appropriate processes and controls are in place to comply with the conditions set out 2.1 to 2.14 above and that the information provided in 1 above is correct.

CCG Caldicott Guardian Name:	**CCG Caldicott Guardian Signature:**	**Date:**

[5] Whilst all personal health data is regarded as sensitive under the DPA, within the context of health services, sexual and reproductive health data have particular additional legal protections. A list has been included in Appendix 4 but see also ISB approved standard on sensitive data for further details http://www.isb.nhs.uk/library/standard/229. It should be noted that this standard is not up to date in relation to all the relevant applicable data fields.

CCG Senior Information Risk Owner Name:	CCG Senior Information Risk Owner Name:	Date:

Completion Note:
On completion please send signed and completed Sections A for your CCG and Annex 1 for your Risk Stratification supplier.

Completed Section A and Annex 1 for each Risk Stratification supplier should be returned to:
IG Team
NHS England, Email: england.riskstratassurance@nhs.net

Section A Completed by: Name	Contact email address:	Date:

Annex 1 – Risk Stratification Supplier Assurance Statement

To provide assurance that risk stratification suppliers are acting in accordance to the conditions set out by CAG approval letter (reference CAG 7-04(a)/2013). The organisation will ensure it meets the requirements set out below, which NHS England reserves the right to audit.

Name of CCG	
Name of Risk Stratification tool supplier	
Name of DSCRO (if using SUS data)	

Please tick appropriate box to indicate acceptance:

The risk stratification supplier (data processor) can provide assurance that it meets the IG Toolkit at a minimum level 2 or equivalent standards (ISO 27001 accredited) ☐

Has in place arrangement with a HSCIC regional Office (DSCRO) via the CCG or GP Practices to receive secondary use data (SUS) for inclusion into risk stratification tool ☐

Or ☐

Will **NOT** be using SUS data in the risk stratification tool

Has removed all highly sensitive data set (minimum excluded data set in Annex 4) from the risk stratification data set. ☐

1. The **Risk stratification supplier** undertakes to ensure that:

No.	Condition
1.1	It will process personal confidential data (PCD) in the following manner: Data is received in a "de-identified data for limited access"[6] form (i.e. NHS number as the patient identifier) or is pseudonymised on landing; AND Processing is within a "closed box" with strict role based access control; AND Re-identification is solely for the purpose of direct care and is available only to those with a direct clinical care relationship with the patient.
1.2	Has ensured that all staff handling data for the purpose of risk stratification are made aware and will operate in compliance with the requirements of Section 251 approval.
1.3	It will only processes the minimum data necessary (i.e. the data specifications will have specific exclusions for sensitive information, and will only utilise the minimum data necessary to identify the candidate risk cohorts).
1.4	It will provide a written procedure outlining a secure mechanism for receipt and processing of data within the risk stratification tool. These should include as a minimum

[6] As defined in the Caldicott Information Governance Review, *To Share or not to share*, Department of Health April 2013 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/192572/2900774_InfoGovernance_accv2.pdf [pp 127]

	the process for: • Receipt of data • Retention periods • Role based access controls, authorisation and maintenance • Induction and training processes for users • How audit trails will be maintained and confidentiality audits may be undertaken
1.5	Staff using risk stratification toolset and reports will receive formal training and can demonstrate they are working in compliance to the written procedure.
1.6	Staff handling patient confidential data are made aware of and will operate in compliance with the obligations set out in the confidentiality clauses in their contract of employment
1.7	Report any suspected data breach relating to risk stratification to the CCG (data controller) in line with the CCG's and NHS England's data breach reporting mechanisms
1.8	It has appropriate processes to securely destroy all PCD held in manual or electronic form once deemed it is no longer necessary purpose of risk stratification at the end of the agreed retention period of end of the data processing contract.
1.9	It will take appropriate actions to work with CCGs and NHS England to transition the risk stratification service towards an approach that meets the exit strategy defined by NHS England
1.10	It undertakes an audit of their processes to ensure that it has taken all reasonable organisation and technical measures to prevent unlawful use of the PCD held for risk stratification purposes

I undertake to ensure the appropriate processes and controls are in place to comply with the conditions set out 1.1 to 1.10 above and that the information provided in 1 above is correct

Risk Stratification Supplier/CSU MD Name	**Risk Stratification Supplier/CSU MD Signature**	**Date**

Form submitted by (Name):	**Email address:**	**Date**

Completion Note: On completion please send signed Annex 1 for return by CCG customers for submission with Section A:
Completed Section A and Annex 1 for each CCG / Risk Stratification supplier should be returned to IG Team, NHS England
Email: england.riskstratassurance@nhs.net

Annex 2 – Named Register of Existing Risk Stratification Suppliers

HSCIC Data Services for Commissioner Regional Offices (DSCROs) where the risk stratification solutions are available

NHS Commissioning Support Units (CSUs)

- NHS South, Central and West CSU
- NHS Midlands and Lancashire CSU
- NHS North and East London (NEL) CSU
- NHS North of England CSU
- NHS Arden-GEM Partnership CSU
- NHS South East CSU

Third party data processors with contracts to provide risk stratification services to CCGs that utilise primary care and secondary care linkage

- Bupa HD
- Capita
- Docobo
- Health Intelligence
- Dr Foster Intelligence (eMBED)
- MedeAnalytics
- PI Benchmark (Care & Health Trak)
- Sollis
- United Health (Optum)
- Nottingham Health Informatics Service
- Prescribing Services Ltd

GP system providers providing options to risk stratify directly using GP data as part of their clinical systems

- EMIS
- TPP SystmOne

Annex 3 – CCG Risk Stratification Checklist – for completion by the CCG as evidence of achievement for audit purposes only (Not for return to NHS England)

Adapted from the NHS England Risk Stratification Advice issued in June 2013; the checklist has been updated to reflect conditions that need to be in place to meet the s251 requirements**.**

No.	Conditions	Achieved
1	Develop and implement a risk stratification policy. Where appropriate to the circumstances, this policy should be developed in collaboration with colleagues from the local: a) Commissioning Support Unit (CSU) b) Health and Social Care Information Centre (HSCIC) regional office providing Data Services for Commissioners (often referred to as Data Services for Commissioners, DSCRO) c) Public health team d) Social care team	
2	Conduct an ethical review to safeguard against unintended consequences, such as the inadvertent worsening of health care inequalities.	
3	Develop one or more preventive interventions that will be offered to high-risk patients.	
4	Select a suitable predictive model. The factors that should be considered in selecting a suitable tool include: a) the adverse outcome to be predicted; b) the accuracy of the predictions; c) the cost of the model and its software and; d) the availability of the data on which it is run. Information governance considerations affecting the choice of predictive model include whether the tool can be run using pseudonymised data, weakly pseudonymised data within an Accredited Safe Haven (ASH), or only identifiable data (i.e. confidential patient information); and whether the tool is compatible with privacy enhancing technologies (which are used to prevent unlawful access to confidential patient information).	
5	Where the data are to be processed in identifiable form (i.e. confidential patient information) ensure there is a legal basis to obtain and process the data for these purposes. The legal basis is currently provided by the s251 approval, but longer term arrangements to utilise pseudonymised data and re-identify only by those with a legitimate relationship with an individual should be developed or alternative legal basis sought such as consent.	
6	Agree a defined data set to be used for risk stratification that is adequate, relevant, but not excessive – including the extent of historical data needed to run the model (e.g. two or three years' worth of data[7]).	

[7] Only the minimum amount of data necessary should be used to fulfil the purpose

7	For predictive models that use GP data, consider how the GP data will be obtained (e.g., using the GP Extraction Service [GPES] or directly from the GP system supplier).	
8	Determine whether to use automated decision-taking[8] or human review. With automated decision-taking, the outputs of the tool are used directly to determine which patients should be offered a preventive intervention. With human review, an appropriate clinician, with responsibility for the care of the individual patient, reviews which patients are to be offered preventive services. Their decision is based both on the risk stratification outputs and any other information known to them.	
9	Ensure that any data service providers being used for risk stratification have appropriate information governance controls in place[9]. These controls include but are not limited to: a) Processes to ensure that the data are not retained longer than necessary by the organisation conducting the risk stratification analysis (i.e. there should be a rolling programme of anonymisation or destruction as the data exceed the defined time period required for the risk stratification tool). b) Ensuring that the data is not processed outside the European Economic Area. Please note that s251 approval is not covered for offshore processing and as such would constitute a breach of the conditions of the s251 support.	
10	Establish appropriate contractual arrangements with any data service providers that: a) Ensure there are appropriate organisational and technical measures in place to protect the data; b) Prevent the unauthorised re-identification, onward disclosure, or further unauthorised or unlawful use of the data and; c) Include mechanisms to manage the contract and audit how the data are being used. d) Include a local process for managing patient objections where the data are weakly pseudonymised or identifiable[10]. Patients may object to the disclosure or use of their personal confidential information, and/or they may object to automated decision-taking. Patients' objections must be respected. If a patient objects to the risk stratification tool being used to make automatic decisions about their care then there must be a human review of their data and of the decision made based on their risk stratification score.	
11	Develop a communications plan, including communication materials for patients	

[8] As defined in Section 12, Data Protection Act 1998.

[9] See Paragraph 12, Schedule 1, Part 2, Data Protection Act 1998

[10] Consideration needs to be given to how this process can be implemented into systems effectively, so it likely a manual process will be needed in the short to medium term

	(these materials may be incorporated into wider fair processing information).	
12	Inform patients that their identifiable or weakly pseudonymised data[11] may be used for risk stratification purposes.	
13	Ensure that only those clinicians who are directly involved in a patient's care can see a patient's identifiable risk score.	
14	Where a tool provides other clinical information (such as information derived from secondary care data), the GP must ensure that these types of data are relevant and that they have the consent of the patient to view this additional information[12].	
15	Refer patients to preventive services only with their consent.	
16	Using pseudonymous data, evaluate and refine the risk stratification model used and the preventive interventions offered according to its predictions.	

[11] Weakly pseudonymised data is data that has the potential to readily identify individuals outside of restricted environments. This data may contain a single "identifying" data item such as the NHS Number or a postcode that do not directly identify individuals but which, if used by people who had access to identifiable systems such as PDS, render the data identifiable.

[12] Such as would be the case where consent had been obtained as part of an integrated care programme, or where the patient is fully cognisant that all or most of their secondary care data will be shared with their GP and they have not withheld their consent for this sharing of information.

Annex 4 – Excluded data

As part of the approval process the CAG were assured that the following data would not flow into a risk stratification tool. Local agreement should be reached on the final dataset but as a pre-requisite the following will not be included

HIV risk lifestyle	13N5.
HTLV-3 antibody test	43C%
Human immunodeficiency virus antibody level	43WK.
HIV antibody/antigen (Duo)	43d5.
HIV 1 PCR	43h2.
HIV1 antibody level	43W7.
HIV2 antibody level	43W8.
HIV viral load	4J34.
Antenatal HIV screening	62b..
AIDS contact	65P8.
AIDS carrier	65QA.
Notification of AIDS	65VE.
Advice about HIV prevention	67I2.
AIDS (HTLV-III) screening	6827.
Patient advised about the risks of HIV	8CAE.
Acquired immune deficiency syndrome	A788%
Human immunodef virus resulting in other disease	A789%
[X]Hiv disease resulting in other infectious and parasitic diseases	AyuC4
[X]Dementia in human immunodef virus [HIV] disease	Eu024
[D]Laboratory evidence of human immunodeficiency virus [HIV]	R109.
[V]Human immunodeficiency virus – negative	ZV018
[V]Contact with and exposure to human immunodeficiency virus	ZV019
[V]Asymptomatic human immunodeficiency virus infection status	ZV01A
[V] Family history of immunodeficiency virus [HIV] status	ZV19B
[V] Human immunodeficiency virus counselling	ZV6D4
[V]Special screening examination for human immunodeficiency virus	ZV737
H/O: venereal disease	1415
Chlamydia antigen test	43U%
Syphilis and other venereal diseases	A9%
Molluscum cantagiosum	A780.
Molluscum contagiosum with eyelid involvement	A7800
Chlamydial infection	A78A
Chlamydial infection of lower genitourinary tract	A78A0
Chlamydial infection of pharynx	A78A1
Chlamydial infection of anus and rectum	A78A2
Chlamydial inf of pelviperitoneum oth genitourinary organs	A78A3
Chlamydial conjunctivitis	A78A4
Chlamydial infection, unspecified	A78AW
Chlamydial infection of genitourinary tract, unspecified	A78AX
Venereal disease contact	65P7.
Venereal disease carrier NOS	65Q9.
Venereal disease screening	683200%
Genital warts	A7812
Other maternal venereal diseases during pregnancy, childbirth and the puerperium	L172%
[V]Contact with or exposure to venereal disease	ZV016
[V]Other venereal disease carrier	ZV028

[V]Screening for venereal disease	ZV745
H/O: abortion	15.43
Preg. termination counselling	6776
Hysterotomy and termination of pregnancy	7E066
Dilation of cervix uteri and curettage of products of conception from uterus	7E070
Curettage of products of conception from uterus NEC	7E071
Suction termination of pregnancy	7E084
Dilation of cervix and extraction termination of pregnancy	7E085
Termination of pregnancy NEC	7E086
Requests pregnancy termination	8M6..
HSA1-therap. abort. green form	956%
Reason for termination of pregnancy	9Ea%
Refer to TOP counselling	8H7W.
Legally induced abortion	L05%
Illegally induced abortion	L06%
[V]Infertility management {?all daughter codes}	ZV26%
Treatment for infertility	8C8%
Introduction of gamete into uterine cavity	7E0A%
Endoscopic intrafallopian transfer of gamete	7E1F2
Marital status {not all daughter codes apply}	133%
Complaints about care	9U%
Imprisonment record	13H9.
In prison	13HQ.
Husband in prison	13I71
Prison medical examination	6992
Place of occurrence of accident or poisoning, prison	T776.
[V]Conviction in civil and criminal proceedings without imprisonment	ZV4J4
[V]Problems related to release from prison	ZV4J5
[V]Imprisonment	ZV625
History of abuse	14X..
History of physical abuse	14X0.
History of sexual abuse	14X1.
History of emotional abuse	14X2.
History of domestic violence	14X3.
Suspected child abuse	1J3..
Child maltreatment syndrome	SN55.
Emotional maltreatment of child	SN550
Nutritional maltreatment of child	SN551
Non-accidental injury to child	SN552
Battered baby or child syndrome NOS	SN553
Multiple deprivation of child	SN554
Physical abuse of child	SN555
Child maltreatment syndrome NOS	SN55z
Sexual abuse	SN571
Child battering and other maltreatment	TL7..
Assault by criminal neglect	TLx4.
Abandonment of child with intent to injure or kill	TLx40
Abandonment of infant with intent to injure or kill	TLx41
Abandonment of helpless person NOS	TLx4z
[V]Family history of physical abuse to sibling	ZV19C
[V]Family history of physical abuse to sibling by family member	ZV19D
[V]Family history of sexual abuse to sibling	ZV19E

[V]Family history of sexual abuse to sibling by family member	ZV19F
[V]Family history of mental abuse to sibling	ZV19G
[V]Family history of mental abuse to sibling by family member	ZV19H
[V]Family history of sibling abuse NOS	ZV19J
[V]Family history of sibling abuse by family member NOS	ZV19K
[V]Problems related to alleged sexual of abuse child by person outside primary support group	ZV4F9
[V]Problems related to alleged sex abuse child by person within primary support group	ZV4G4
[V]Problems related to alleged physical abuse of child	ZV4G5
[V]Child abuse	ZV612

Plus equivalents for CTV3

Where the following consent or dissent flags have been used they should be understood and where it should be applied consistently within the chosen solution to apply consent and dissent accordingly.

Refused consent for upload to local shared electronic record	93C1.
Refused consent for upload to national shared electronic	93C3.
Informed dissent for national audit	9M1..
Confidential patient data	9R1..
Conf data - patient not to see	9R11.
Conf data - not to be reported	9R12.
Conf data - staff not to see	9R13.
Conf data - paramedics not see	9R14.
Conf data - other Dr not see	9R15.
Confidential data NOS	9R1Z.
No consent for electronic record sharing	9Nd1.
Declined consent for Primary Care Trust to review patient record	9Nd9.
Declined consent to share patient data with specified third party	9NdH.
Consent withdrawn to share patient data with specified third party	9NdJ.
Personal risk assessment declined	9Oh8.
Multi-professional risk assessment declined	9Oh5.
Dissent from disclosure of personal confidential data by Health and Social Care Information Centre	9Nu4.
Dissent withdrawn from disclosure of personal confidential data by Health and Social Care Information Centre	9Nu5.