CAG 7-04(a)/2013 compliance for ICBs

The application from NHS England on behalf of GPs and ICBs s, as the relevant data controllers, seeking support for the activity of risk stratification to be used by GPs supported by ICBs 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 Integrated Care Boards and their appointed risk stratification suppliers to provide assurance that processing of the data is in accordance with the Data Protection Act 2018[1] and that the conditions set out for processing of personal confidential data are undertaken and maintained. This assurance statement is required to ensure that all organisations undertaking risk stratification activities are doing so in line with the CAG approval conditions. It does not replace any requirement to undertake data processor assurance under GDPR/DPA legislation.

It should be noted that this approval only applies to the use of GP, SUS data (In-patient/Out-patient/A&E) and the Mental Health Services Data Set. Please be aware that if you require any other datasets to be included in your risk stratification processing, you must contact NHS England so that an amendment application can be made to the Confidentiality Advisory Group.

Please note that the approval 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 - D and return it to NHS England via email: england.riskstratassurance@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.

[1] http://www.legislation.gov.uk/ukpga/2018/12/pdfs/ukpga_20180012_en.pdf

Section A: Assurance Statement

To provide assurance that ICBs 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. 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

2. Support is provided up to and including **30th September 2023.** ICBs are required to collaborate with NHS England to implement a data standard for risk stratification that minimises the use of patient confidential data.

3. ICBs agree to work in collaboration with NHS England and NHS Digital to identify and work towards an agreed exit option(s).

4. The ICB will ensure that the risk stratification supplier also completes and returns the assurance statement in Section C. ***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 ICB (data controller for SUS/MHSDS data) 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 Data Security and Protection Toolkit (DSPT) standard or equivalent (e.g. ISO 27001 accredited) ☐

[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.

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

The ICB has in place an arrangement with an NHS Digital Regional Office (DSCRO) on behalf of the relevant GP practices for the data processor to receive secondary use data (SUS) and MHSDS data (if applicable) for inclusion into risk stratification tool ☐

Name of DSCRO _____

Please indicate which datasets will be required for risk stratification processing*:

Dataset	Includes NHS number as the identifier (Yes/No)	Required (Yes/No)
GP Data		Yes
SUS – In-patient/out-patient/A&E		Yes
MHSDS		

***see page 8 for information on the process to request use of further datasets**

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

1. **The ICB undertakes to ensure that**:

1.1. The relevant staff have read, understood and implemented the requirements within the risk stratification checklist referenced in Annex 2.☐

1.2. Member GP practices are made aware of their responsibilities as data controllers, and have in place an agreement with the ICB in relation to the use of the GP data (and SUS/MHSDS data, where applicable) for the purposes of risk stratification. ☐

1.3. 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 processing notices by the ICB and its member practices). This should include an explanation of risk stratification, clarity about who the data controller(s) 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 ICB website: _____

1.4. It has agreed a process with GP Members on how patient objections will be handled ☐

1.5. Risk stratification suppliers will process personal confidential data (PCD)[3] 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 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. ☐

1.6. 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 of the NHS Act 2006[5]. ☐

1.7. The named risk stratification supplier processes the minimum data necessary (i.e. the data specifications will have specific exclusions for sensitive information[6] (see Annex 3) and will only utilise the minimum data necessary to identify the candidate risk cohorts). ☐

1.8. 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 ☐

1.9. 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 ICB's and/or 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 Data Privacy Impact Assessment for risk stratification in accordance with ICO guidance. ☐

Section B: Signatures

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.

ICB Caldicott Guardian Name:	
ICB Caldicott Guardian Signature*:	
Date:	
ICB Senior Information Risk Owner Name:	
ICB Senior Information Risk Owner Signature*:	
Date:	

[3] https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/what-is-personal-data/
[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]
[5] https://www.legislation.gov.uk/ukpga/2006/41/section/251
[6] 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 Annex 3 but see also ISB approved standard on sensitive data for further details https://digital.nhs.uk/data-and- information/information-standards/information-standards-and-data-collections-including-extractions/publications- and-notifications/standards-and-collections . It should be noted that this standard is not up to date in relation to all the relevant applicable data fields.

*If using electronic signature: As an additional measure of security, we also require an email from signees to the individual completing this form agreeing to the terms of this statement. Alternately we will also accept the use of wet signature.

Section A completed by:	
Email address:	
Date:	

Section C: 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 ICB : _____

Name of Risk Stratification tool supplier: _____

Name of DSCRO (if using SUS/commissioning data): _____

Please tick appropriate box to indicate acceptance:

The risk stratification supplier (data processor) can provide assurance that it meets Data Security and Protection Toolkit (DSPT) standards or equivalent (ISO 27001 accreditation) ☐

Has removed all highly sensitive data set (minimum excluded data set in Annex 3) from the risk stratification data set. ☐

Has in place an arrangement with an NHS Digital Regional Office (DSCRO) via the ICB or GP Practices to receive secondary use data (SUS/MHSDS if applicable) for inclusion into risk stratification tool ☐

Or

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

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

1.1. It will process personal confidential data (PCD) in the following manner:
Data is received in a "de-identified data for limited access"[7] 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 process 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 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 ICB (data controller) in line with the ICB's and/or 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 ICBs 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 ☐

Section D: Signatures

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:	

*If using electronic signature: As an additional measure of security, we also require an email from signees to the individual completing this form agreeing to the terms of this statement. Alternately we will also accept the use of wet signature.

Annex 1 – Named Register of Existing Risk Stratification suppliers and Approved Datasets

NHS Commissioning Support Units (CSU's)

- NHS South, Central and West CSU
- NHS Midlands and Lancashire CSU
- NHS North of England CSU
- NHS Arden-GEM Partnership CSU

[7] 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]

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

- Bupa HD
- Capita
- Cerner
- Docobo
- Health Intelligence
- Dr Foster Intelligence
- MedeAnalytics
- PI Benchmark (Care & Health Trak)
- Sollis
- United Health (Optum)
- Nottingham Health Informatics Service
- Prescribing Services Ltd
- EMIS
- TPP SystmOne
- MSD Ltd
- Graphnet

Approved Datasets from September 2018
The datasets which are now approved for use under CAG approval CAG 7-04(a)/2013* are as follows:

Dataset	Includes NHS number as the identifier	Required (Yes/No)
GP Data	**Yes**	**Yes**
SUS – In-patient/out-patient	**Yes**	**Yes**
MHSDS	**Yes**	

*** Please note:** If you require a new dataset to be included in risk stratification processing, you will need to complete the NHSE Risk Stratification Amendment form available via the link below or by sending a request to england.riskstratassurance@nhs.net.

Annex 2 - ICB Risk Stratification Checklist – for completion by the ICB 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) NHS Digital 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, within a secure processing area 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[8].	
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[9]).	

[8] https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/what-is-personal-data/what-is-personal-data/

[9] 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 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[10]. 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 identifiable[11]. 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	

[10] Chapter 4, Section 107, Data Protection Act (2018) http://www.legislation.gov.uk/ukpga/2018/12/section/107/enacted
[11] 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

	data and of the decision made based on their risk stratification score.	
11	Develop a communications plan, including communication materials for patients (these materials may be incorporated into wider fair processing information).	
12	Inform patients that their identifiable data 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 data which has been pseudonymised, evaluate and refine the risk stratification model used and the preventive interventions offered according to its predictions.	

Annex 3 – 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:

List of Legally Restricted Records
Confidentiality Category 2

Code	Description
OPCS	Classification of Interventions and Procedures
N341	Fertility investigation of Male NEC
N342	Collection of sperm NEC
N343	Male colposcopy
N344	Microsurgical epididymal sperm aspiration
N345	Percutaneous epididymal sperm aspiration
N346	Testicular sperm extraction
Q131	Transfer of embryo to uterus NEC
Q132	Intracervical artificial insemination
Q133	Intrauterine Artificial insemination
Q134	Intrauterine insemination with superovulation using sperm partner

[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.

Q135	Intrauterine insemination with superovulation using donor sperm
Q136	Intrauterine insemination without superovulation using partner sperm
Q137	Intrauterine insemination without superovulation using donor sperm
Q138	Other specified introduction of gamete into uterine cavity
Q139	Unspecified introduction of gamete into uterine cavity
Q211	Transmyometrial transfer of embryo to uterus
Q218	Other specified other introduction of gamete into uterine cavity
Q219	Unspecified other introduction of gamete into uterine cavity
Q382	Endoscopic injection into fallopian tube
Q383	Endoscopic intrafallopian transfer of gamete
Q411	Salpingography
Q412	Hydrotubation for fallopian tube
Q413	Dye test of fallopian tube
Q414	Insufflation of fallopian tube
Q415	Operations to ensure patency of fallopian tube NEC
Q416	Recanalisation of fallopian tube
Q417	Aspiration of fallopian tube
Q48	Oocyte recovery
Q481	Endoscopic transurethral ultrasound directed oocyte recovery
Q482	Endoscopic transvesical recovery
Q483	Laparoscopic oocyte recovery
Q484	Transvaginal oocyte recovery
Q488	Other specified oocyte recovery
Q489	Unspecified oocyte recovery
Q555	Transvaginal ultrasound examination of female genital tract
Q561	Fertility investigation of female NEC
Q562	Fertiloscopy
U321	Human Immunodeficiency Virus blood test
X866	Antiretroviral drugs Band 1
X88	High cost reproductive and urinary tract drugs
X888	Other specified high cost reproductive and urinary tract drugs
X889	Unspecified high cost reproductive and urinary tract drugs
X15	Operations for sexual transformation
X151	Combined operations for transformation from male to female
X152	Combined operations for transformation from male to female
X154	Construction of scrotum
X158	Other specified operations for sexual transformation
X159	Unspecified operations for sexual transformation
Y961	In vitro fertilisation with donor sperm
Y962	In vitro fertilisation with donor eggs
Y963	In vitro fertilisation with intracytoplasmic sperm injection and donor egg
Y964	In vitro fertilisation with pre-implantation for genetic diagnosis
Y965	In vitro fertilisation with pre-implantation for genetic diagnosis
Y966	In vitro fertilisation with surrogacy

Y968	Other specified in vitro fertilisation
Y969	Unspecified in vitro fertilisation
ICD-10	**International Classification of Disease**
B20	Human immunodeficiency virus [HIV] disease resulting in infectious and parasitic diseases
B200	HIV disease resulting in mycobacterial infection
B201	HIV disease resulting in other bacterial infections
B202	HIV disease resulting in cytomegaloviral disease
B203	HIV disease resulting in other viral infections
B204	HIV disease resulting in candidiasis
B205	HIV disease resulting in other mycoses
B206	HIV disease resulting in Pneumocystis
B207	HIV disease resulting in multiple infections
B208	HIV disease resulting in other infectious and parasitic disease
B209	HIV disease resulting in unspecified infectious or parasitic disease
B21	Human immunodeficiency virus [HIV] disease resulting in malignant neoplasms
B210	HIV disease resulting in Kaposi sarcoma
B211	HIV disease resulting in Burkitt lymphoma
B212	HIV disease resulting in other types of non Hodgkin lymphoma
B213	HIV disease resulting in other malignant neoplasms of lymphoid, haematopoietic and related tissue
B217	HIV disease resulting in multiple malignant neoplasms
B218	HIV disease resulting in other malignant neoplasms
B219	HIV disease resulting in unspecified malignant neoplasm
B22	Human immunodeficiency virus [HIV] disease resulting in other specified diseases
B220	HIV disease resulting in encephalopathy
B221	HIV disease resulting in lymphoid interstitial pneumonitis
B222	HIV disease resulting in wasting syndrome
B227	HIV disease resulting in in multiple diseases classified elsewhere
B23	Human immunodeficiency virus [HIV] disease resulting in other conditions
B230	Acute HIV infection syndrome
B231	HIV disease resulting in (persistent) generalised lymphadenopathy
B232	HIV disease resulting in haematological and immunological abnormalities, not elsewhere classified
B238	HIV disease resulting in other specified conditions
B24X	Unspecified human immunodeficiency virus [HIV] disease
F64	Gender Identity disorders
F640	Transsexualism
F641	Dual-role transvestism
F642	Gender identity disorder of childhood
F648	Other gender identity disorders
F649	Gender identity disorder, unspecified
F651	Fetishistic transvestism

F656	Multiple disorders of sexual preference
F66	Psychological and behavioural disorders associated with sexual development and orientation
F660	Sexual maturation disorder
F661	Egodystonic sexual orientation
F662	Sexual relationship disorder
F668	Other psychosexual development disorders
F669	Psychosexual development disorder
N46X	Male infertility
N97	Female infertility
N970	Female infertility associated with anovulation
N971	Female infertility of tubal origin
N972	Female infertility of uterine origin
N973	Female infertility of cervical origin
N974	Female infertility associated with male factors
N978	Female infertility of other origin
N979	Female infertility, unspecified
N98	Complications associated with artificial fertilisation
O987	Human immunodeficiency [HIV] disease complicating pregnancy, childbirth and the puerperium
R75X	Laboratory evidence of human immunodeficiency virus [HIV]
Z114	Special screening examination for human immunodeficiency virus [HIV]
Z206	Contact with and exposure to human immunodeficiency virus [HIV]
Z21X	Asymptomatic human immunodeficiency virus [HIV] infection status
Z31	Procreative management
Z310	Tuboplasty or vasoplasty after previous sterilization
Z311	Artificial insemination
Z312	In vitro fertilisation
Z313	Other assisted fertilisation methods
Z314	Procreative investigation and testing
Z315	Genetic counselling
Z316	General counselling and advice on procreation
Z318	Other procreative management
Z319	Procreative management, unspecified
Z350	Supervision of pregnancy with history of infertility
Z717	Human immunodeficiency virus [HIV] counselling
Z830	Family history of human immunodeficiency virus [HIV] disease

Dissent/Opt-Out Codes
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.

93C1.	Refused consent for upload to local shared electronic record
93C3.	Refused consent for upload to national shared electronic

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