Data Privacy Impact Assessment (DPIA)
Risk Stratification for Case Finding (IPA Tool)

Index

Need for a DPIA - Article 35(1)

This project has several criteria that warrant a DPIA:

- Processing special category data – health & social care data
- Large Scale of special category data - Article 35(3)(b)
- Children
- Vulnerable adults
- Matching and combining datasets
- Evaluation or scoring (i.e. *profiling*)
- Long-term processing (potentially)
- The absence of explicit consent for secondary purposes

Back to Index

Data Privacy Impact Assessment (DPIA)
Risk Stratification for Case Finding (IPA Tool)

Documents

List all documents provided and which this DPIA utilises

We have been provided with:

1) An Information Sharing Agreement between NEHFCCG and the practice.
   This is not a legal requirement but is regarded as good practice, and defines the responsibilities around each (joint) data controller and the data that it retains controllership for

2) A Data Processor Agreement between SCW CSU (the data processor) and the practice (the data controller).
   The CCG is listed as "an agent", but for the purposes of this contract should be regarded as a third-party beneficiary.

   It is not necessary for the CCG to be a party at all to the data processor contract.

   It should also be noted that the CCG has its own data processor contract with SCW CSU, with respect to the processing of secondary care data (SUS/HES/"commissioning datasets") that the CCG is the data controller for.

Note is made of the name of the risk stratification tool – *Insights Population Analytics Service (IPA)* – however no "population analytics" (or "population health management") takes place as such.

Each individual is scored (i.e. profiled) and that score made available *only* to the GP practice.

Back to Index

Data Privacy Impact Assessment (DPIA)
Risk Stratification for Case Finding (IPA Tool)

Article 35(7)(a)

- **The type(s) of data being processed**

The data that is ultimately processed has two sources:

1) Data from GP records (including prescription data)
2) Data from secondary care (SUS/HES/"commissioning datasets")

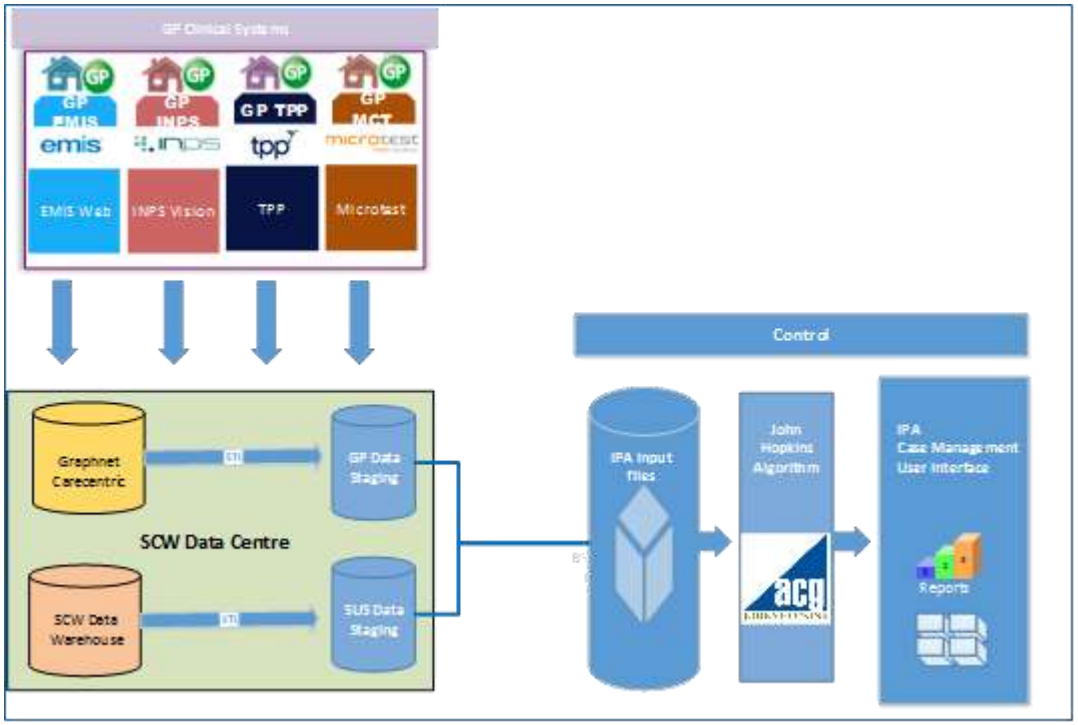
SCW CSU is the data processor.

- **The nature of the processing**

The CCG is the data controller for the SUS/HES data provided to the processor.
The GP practice is the data controller for the GP data provided to the processor.

The two organisations are, therefore, joint data controllers, sharing a common data processor.

An algorithm (ACG) is applied to the combined data and a "risk stratification score" is generated for each individual. That score is then stored against that individual's primary care record and made available to the GP practice (only).



Data Privacy Impact Assessment (DPIA)
Risk Stratification for Case Finding (IPA Tool)

GP data

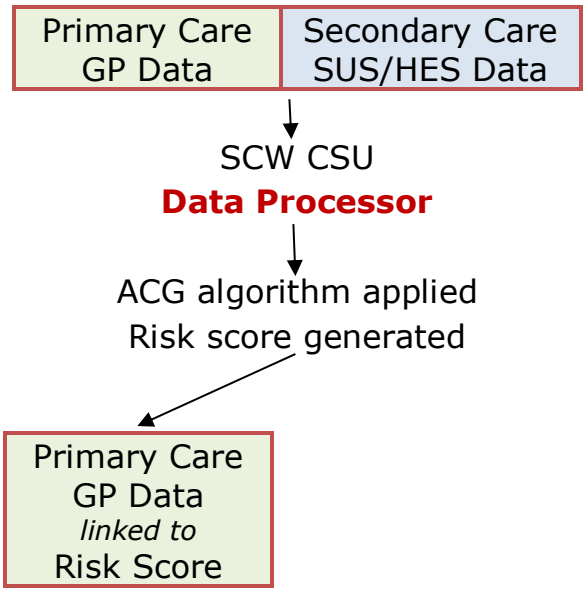
Data controller: **GP surgery**

Release without consent
authorised by CAG 7-04(a)/2013

SUS/HES data (2° care)

Data controller: **CCG**

Release without consent
authorised by CAG 2-03(a)/2013



Risk score available *only* to GP practice (data controller)

NO other purposes of processing

- **Scope of Processing**

Sensitive category (health), personal data is processed. It is extracted and uploaded securely to a data processor. The types of personal data and special category data processed can be found detailed in Appendix A of the Information Sharing Agreement between the two joint data controllers (the GP practice and the CCG), as well as the Schedule in the data processor agreement.

The data would be extracted from the GP records of all patients unless an opt-out (objection) code is present in their record.

- **Context**

GP practices provide primary care data sourced from the electronic GP record that we maintain.

Patients can control whether to allow risk stratification or not, by simply objecting/opting out.
The data does include data from vulnerable subjects and *would* include that of children unless mitigated against.

There have been prior concerns about the purposes of processing, however referral to the HRA has previously clarified that, and those concerns are no longer replicated in this project.

- **Purposes**

The sole purpose of processing is for risk stratification for case finding, that is attributing a "score" to an individual and making that score available *only* to the GP practice.

Previously, the HRA have commented on the purpose(s) authorised under this CAG approval. See

https://www.hra.nhs.uk/documents/1337/CAG_Meeting_-_12_October_2017.pdf

How does this directly benefit data subjects?

What is the intended outcome for individuals?

The benefit to patients is the identification of those data subjects who:

- are at risk of hospital admission, and/or
- would benefit from targeted intervention by the GP practice (usually by means of the ICT, Integrated Care Team), and/or
- who are either not already known to the ICT or "on our radar"

Back to Index

How does this directly benefit our organisation?

Does this give us a "competitive advantage"?

This tool does not give us a competitive edge as such (it does not generate income, for example) but identifying and intervening where appropriate would be regarded as good clinical care.

Back to Index

Article 35(9)

- **Consultation process with data subjects & others**

Was it undertaken? Do we need to? Do we need to get advice from experts?

No consultation process has been undertaken. The practice has previously processed data for risk stratification, although this ceased last October.

A consultation process is not warranted given that such processing has previously been assessed by the HRA as part of the CAG approval, and as long as mitigating factors for children are taken (see later).

Advice on the scope of processing purposes has previously been sought from the HRA, and indeed contact has recently been made with them again regarding the ongoing CAG approval.

The following is our understanding of CAG approval, and HRA confirmation of this is sought. However, the data processing contract now clearly limits processing to risk stratification for case finding, with data provided to GP practices only, so the HRA's determination will now not materially affect such processing.

CAG 7-04(a)/2013 permits the linkage of identifiable primary care data with secondary data (as authorised by CAG 2-03 (a)/2013), for the sole purpose of a risk stratification algorithm (in this case, the John Hopkins ACG) being applied by the CSU to individual patients, and for that information to be made available back to the GP practice only (the data controller).
The CSU (in this case) is acting as a data processor "working under the instruction of GPs as data controllers".
(That linkage supposedly refines the algorithm, in an attempt to improve the reliability of the score beyond that which would be achieved by basing the calculation on primary care data only).

CAG 2-03 (a)/2013 permits the use of identifiable secondary care data alone for commissioning purposes, by CCGs, and in so the CCG is a data controller for this defined purpose.

CAG 2-03 (a)/2013 permits the linkage of secondary data with identifiable primary care data (as authorised by CAG 7-04(a)/2013), for the sole purpose of a risk stratification algorithm (in this case, the John Hopkins ACG) being applied by the CSU to individual patients, and for that information to be made available back to the GP practice only (the data controller). That is, for risk stratification for case finding only.

CAG 7-04(a)/2013 does not permit the use of identifiable primary care data for any other purpose, such as:

- *Use of primary care data alone for commissioning/PHM/PHA purposes*
- *Use of primary care data alone for "risk stratification for planning"*
- *Use of primary data once linked with secondary care data for commissioning/PHM/PHA purposes*
- *Use of primary data once linked with secondary care data for "risk stratification for planning"*

That applies even if the linked data were to be subsequently processed by the CSU to anonymised or pseudonymised data.

And it does not permit the release of pseudonymised, record-level data (whether primary care data alone or linked with secondary care data) to anyone else, except for the data controller, for any purpose.

CAG 2-03 (a)/2013 does not permit the use of secondary data once linked with primary data, for commissioning/PHM/PHA purposes.

CAG 2-03 (a)/2013 does not permit the use of secondary data once linked with primary data, for "risk stratification for planning"

That applies even if the linked data were to be subsequently processed by the CSU to anonymised or pseudonymised data.

And it does not permit the release of pseudonymised, record-level, linked, data to the CCG, for any purpose.

Back to Index

Article 35(7)(b)

- **Necessity and proportionality (data protection compliance)**

Common Law (CLoC)

How is this met?

Risk Stratification is authorised under s251 approval from HRA CAG, namely CAG 7-04(a)/2013, which sets aside the common law of confidentiality. Accordingly, the explicit consent of patients does not have to be sought and recorded before their confidential medical information is processed in this way. S251 is *permissive*.

Back to Index

Caldicott Principles

1. Justify the purpose(s)

The sole purpose of processing is for risk stratification for case finding. No other processing purposes (e.g. commissioning, "business analytics", population health management) are permitted.

We recognise that there is no justification for profiling the data of children in this way.

2. Don't use personal confidential data unless it is absolutely necessary

Personal confidential data is necessary for the algorithm.

3. Use the minimum necessary personal confidential data

Only relevant medical information (that would affect a risk score) is extracted and uploaded.

4. Access to personal confidential data should be on a strict need-to-know basis

Only the GP practice has access to the NHS number, the risk score and any other confidential data needed to provide direct care.

5. Everyone with access to personal confidential data should be aware of their responsibilities

The GP practice and the CSU (data processor) are aware of this.

6. Comply with the law

This processing complies with all relevant laws (see later).

7. The duty to share information can be as important as the duty to protect patient confidentiality

This does not apply as information is not required to be shared between healthcare providers for direct care purposes.

Back to Index

Article 5 GDPR – the data protection principles

Personal data shall be:

a) processed lawfully, fairly and in a transparent manner in relation to individuals (lawful purpose)

Processing data in this way complies with the law.
Comprehensive fair processing information will be provided to patients.
The lawful bases for such processing are

- Article 6(1)(e) – Official Authority
- Article 9(2)(h) – Provision of Health

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (purpose limitation)

The sole purpose has been defined, reiterated by the HRA, and the information sharing agreement and data processor contracts reflect this.

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (data minimisation)

Only that data which is medically necessary to generate a risk score is extracted and uploaded.
See later for "children".

d) accurate and, where necessary, kept up to date (accuracy)

Data at source (i.e. from the GP record) is kept accurate and up to date in line with GDPR/DPA and GMC guidelines.

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed (storage limitation)

Data is processed in this way for as long as the patient is receiving medical care by the GP practice. Since patients can develop medical problems at any time, that would materially affect their risk stratification score, regular and ongoing assessments need to be made.

f) processed in a manner that ensures appropriate security of the personal data (confidentiality)

Appropriate security is maintained by the processor both in the transmission of data from the GP records database to the processor and in the storage of the personal data by the processor.

Back to Index

No surprises

"there must be no surprises to the citizen about how their health and care data is being used" (NDG)
Is this met?

As long as:

1) Fair processing information is provided in a comprehensive manner
2) The purpose of this processing is strictly limited to risk stratification for case finding only
3) An adequate "lead-in" time (for example 6 weeks) is given to inform patients and allow those who wish to object/opt-out to do so before processing commences
4) The personal data of patients who have already expressed a "Type 1" objection, or other similar objections, will not be processed

then risk stratification for case finding in this manner should comply with the "*no surprises*" rule.

Back to Index

Data Processors – Article 28

A controller determines the purposes and means of processing personal data. A processor is responsible for processing personal data on behalf of the controller and can act only upon the instructions of the controller.
Does the practice retain full data controllership?
How do we ensure that processors comply?

Does processing require the use of a data processor?
YES

If yes:

Has a **written** data processor contract been provided?
YES

Are both the controller and processor **parties** to the contract?
YES

Are both controller and processor **signatories** to the contract?
YES

Does the processor contract contain the following compulsory details?

- the name of the controller and the processor
  YES
- contact details for the controller and the processor
  YES
- the subject matter and duration of the processing
  YES
- the nature and purpose of the processing
  YES
- the type of personal data and categories of data subject
  YES
- the obligations and rights of the controller
  YES

Does the processor contract contain the following compulsory terms?

- the processor must only act on the written instructions of the controller (unless required by law to act without such instructions)
  YES

- the processor must ensure that people processing the data are subject to a duty of confidence
  YES

- the processor must take appropriate measures to ensure the security of processing
  YES

- the processor must only engage a sub-processor with the prior consent of the data controller and a written contract
  YES

- the processor must assist the data controller in providing subject access and allowing data subjects to exercise their rights under the GDPR
  YES

- the processor must assist the data controller in meeting its GDPR obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments
  YES

- the processor must delete or return all personal data to the controller as requested at the end of the contract
  YES

- the processor must submit to audits and inspections, provide the controller with whatever information it needs to ensure that they are both meeting their Article 28 obligations, and tell the controller immediately if it is asked to do something infringing the GDPR or other data protection law of the EU or a member state
  YES

Does the processor contract?

- state that nothing within the contract relieves the processor of its own direct responsibilities and liabilities under the GDPR
  YES

- reflect any indemnity that has been agreed
  YES

- contain an expiration date for processing (after which all processing must cease)
  YES

- Make clear how either the data controller or the data processor may voluntarily terminate the contract, including the notice required
  NO

Is it clear that the data processor must?

- only act on the written instructions of the controller (Article 29)
  NO
- not use a sub-processor without the prior written authorisation of the controller (Article 28.2)
  NO
- co-operate with supervisory authorities (such as the ICO) in accordance with Article 31
  YES
- ensure the security of its processing in accordance with Article 32
  YES
- keep records of its processing activities in accordance with Article 30.2
  YES
- notify any personal data breaches to the controller in accordance with Article 33
  YES
- employ a data protection officer if required in accordance with Article 37
  YES

Does Oakley Health Group retain ***full data controllership*** over all aspects of processing?
YES

Back to Index

Ability to implement Data Subject Rights

1. The Right to be informed

The practice will need to provide comprehensive fair processing information about this project.
The practice will need to provide a "lead-in" time of 6 weeks to allow patients to be informed and for those who wish to opt-out/object to be able to do so *before* their data is extracted and uploaded.

2. The Right of access

Patients already have the right of access to their GP record, from which their primary care data is sourced.
Patients have the right to access their data as held by SCW CSU for this project, either their primary care data or their SUS/HES data, as well as their risk score. The data processor is obliged to facilitate provision of such data to the data subject.

3. *The Right to rectification*

Patients already have the right to rectification (and the right to restrict processing that goes with this) of their data as held within their GP record.

Patients can apply for rectification of secondary care data by approaching either the data processor or the CCG.

4. ***The Right to object***

Patients can easily object to the processing of their data in this way. An opt-out mechanism already exists : the Type 1 opt-out (universal secondary uses opt-out, 9Nu0) and patients can do so in a variety of ways (http://www.oakleyhealth.org/website/X82206/files/A4%20universal%20opt%20out%20form.pdf)

Other opt-out codes exist that, when present in the GP record, will also prohibit extraction and uploading for risk stratification, for example EMIS Web data sharing (93C1), 9Nd1 (CHIE opt-out), 9q7 ("Declined consent for use of patient data in risk stratification for unplanned admissions").

Back to Index

Things to think about

Do we have to do this?

What legislation mandates this? Is this just a contractual obligation?

We are under no legal obligation to process data in this way.
We are under no contractual obligation to process data in this way.

S251 approval is *permissive* only.

Back to Index

Can we do this without processing the data? Can we do this, or process data, in a less intrusive way?

There already exists validated and effective risk stratification tools available to GP surgeries, such as QAdmissions, and which are integrated within their clinical systems
(see : *https://www.emishealth.com/products/risk-stratification/*).

Such tools do not require secondary care data, and do not require the exaction and uploading of confidential medical information from the GP record into the hands of a third-party data processor under s251/CAG approval.

The additional of SUS/HES data probably adds little as patients who have recently been admitted to hospital are already targeted by the integrated care teams (ICTs) at GP surgeries, who are the sole users of the risk stratification tool. Historic SUS data (such as admissions for heart attacks, strokes and other such conditions) has, in many cases, already been coded within primary care data.

The linkage of secondary care data to primary care data for such profiling *may not* be necessary for effective risk stratification for case finding.

However, if processing is sought that uses an algorithm combining primary care *and* secondary care data then there is no obvious way to undertake this without processing data via a third-party processor.

Back to Index

Is this lawful?

- ***Common law, and***
- ***Caldicott Principle 6, and***
- ***Article 5(a) GDPR, and***
- ***Any other relevant laws (e.g. PECR, Article 10 GDPR)***

Yes, this is lawful, it complies with all necessary laws and principles.

Back to Index

Is this ethical? Is this fair?

*"You need to stop and think not just about how you can use personal data, but also about **whether you should**" (ICO)*

The identification of patients at risk of deterioration in their physical health, or social situation, is ethically sound given that the processing of such data is purely for this purpose, effectively a direct-care purpose, and the outcome of the profiling (i.e. the scores) are only available to the GP practice.
Patients will be provided with fair processing information, a 6 week "lead-in" time during which they can opt-out (or object), and the ability to opt-out at any time thereafter.

We will need to consider the processing of information relating to children (see below). It would neither be justifiable, nor ethical, nor fair to process the confidential medical information of children in this way.

Back to Index

Is there a risk of reputational damage if we proceed with processing?

To the practice/To the profession/What would the GMC say?

As long as we mitigate for profiling of children then there appears to be no reputational risk.

Back to Index

What are the consequences of not proceeding with this processing? Can we mitigate against any negative effects?

Does it matter at all if we say no?

Oakley Health Group has not used the risk stratification tool for more than a year and we have been able to identify patients at risk, and who would benefit from ICT input, in a variety of ways.

The QAdmissions tool would be available to us should we not proceed with this processing.

Other risk scoring tools, such as frailty scores, exist, and we regularly monitor admissions to, and discharges from, hospital, in order to identify patients who might be at risk.

Back to Index

What about children?

The ICT deals almost exclusively with the elderly, usually patients over the age of 60 years old.

Children (<18 yrs old) are nearly always know to the practice if they are at risk of hospital admission. Complex children are almost always already under the care of a paediatrician. We are not going to suddenly "discover" a child who is at risk of hospital admission that we were not already aware of.

It cannot be justified to profile the data of a new born baby in this way, for example.

The GDPR stresses that profiling is a high-risk purpose with respect to children, particularly in this instance when explicit consent from either the child or their parents/guardians are not being sought.

Back to Index

Article 35(7)(c)

- **Risks to data subjects**

What are they?

There is always a risk that patients will not have been made aware of this new processing, and that the first time that they discover that their data was processed in this way was *after* such profiling had occurred.

There is a high risk that the confidential medical data of children will be profiled, in the absence of explicit consent from either the child or their parents/guardians. Such profiling is extremely unlikely to identify individuals who would not already be known to be at risk; such individuals are almost certainly known to their GP, their Health Visitor or Midwife, Social Services, and they are likely to be under the care of a hospital paediatrician (secondary or tertiary care).

Back to Index

Article 35(7)(d)

- **Measures to manage, reduce or eliminate risks**

What can we do?

We can ensure:

- Comprehensive fair processing information, a clear privacy notice, and widespread dissemination of our intention to undertake such processing (i.e. profiling) via posters, handouts, leaflets, our website and Facebook page
- A reasonable lead-in time of 6 weeks during which time patients who wish to opt-out can do so *in advance* of their data being extract, uploaded and profiled
- Simple and straightforward opt-out mechanisms, ensuring that patients who have already opted out by virtue of a pre-existing objection expressed and recorded in their GP record are made aware of this

The data of children (i.e. <18yrs old) should *not* be profiled in this way.

It is *possible* that the HRA might mandate that one of the conditions of CAG approval is that the data of children is not extracted and uploaded at source (i.e. built-in to the extraction software).

Nevertheless, and in the meantime, we should:

- Add a specific read-code to the records of all children that specifically and purely prohibits risk stratification (i.e. 9q7) without affecting any other data sharing schemes; unless a pre-existing opt-out read code exists in that child's record
- Remove the 9q7 read-code for children as (or soon after) they turn 18yrs old
- Ensure that our fair-processing information makes clear that we only process the data of *adults* for this purpose

Back to Index

Conclusion

- **Article 36 – Need for prior consultation with the ICO**

Do we need to?

No – as long as we do not process (i.e. profile) the data of children in this way.

No – as long as changes to the data processor contract are made to clarify that it is the *data controller* (not the CCG) instructing the processor in how GP primary care data is to be processed (Article 29), and additional terms are added to ensure compliance with Article 28.

The CCG as a party to the data processor contract is wholly unnecessary, as the CCG already has its own data processor contract with the CSU for the processing of HES/SUS data, and a separate service level agreement for the provision of the risk stratification service (and the costs therein).

We do not need to seek the removal of the CCG as a party to the contract, however it *must* be clear that the processor is acting only upon the instructions of the GP practice with regards to the processing of primary care data.

- Within the Information Sharing Agreement with the CCG, in the "Summary" on page 2, the line "*The data is also made available in a pseudonymised format for commissioning purposes*." in the third paragraph must be removed

For the Data Processor Contract:

- On page 4, under "BACKGROUND (C)" the phrase
  "This Agreement sets out the Personal Data that SCW shall Process as instructed by the Agent on behalf of the Controller" should be replaced with
  "This Agreement sets out the Personal Data that SCW shall Process as **instructed by the Controller**"

- On page 8, for 4.2 (Processing under instruction), the phrase
  "process that Personal Data only in accordance with the written instructions of the CCG and as agreed with the Controller" should be replaced with
  "process that Personal Data only in accordance with the written **instructions of the Controller**"

- On page 10, for 6.3.2.2 (security measures), the phrase
  "do not publish, disclose or divulge any of the Personal Data to any third party unless SCW is authorised or directed in advance and in writing to do so by the CCG as Agent of the Controller (or is otherwise permitted by this Agreement);" should be replaced by
  "do not publish, disclose or divulge any of the Personal Data to any third party unless SCW is authorised or directed in advance and in writing to do so **by the Controller** (or is otherwise permitted by this Agreement);"

- On page 10, under 7.1 (sub-processors) the phrase
  "The CCG as Agent of the Controller hereby authorises SCW" should be replaced with
  "**The Controller hereby authorises SCW**"
  Under 7.2.2, the phrase "obtain the written consent of the CCG acting as the Agent of the Controller" should be replaced with
  "obtain the written consent **of the Controller**"

- On page 11, for 10.1 (destruction of data) the phrase
  "at the written direction of the CCG and the Controller delete or return the Personal Data (and any copies of it) on termination of the Agreement" should be replaced by
  "at the written direction **of the Controller** delete or return the Personal Data (and any copies of it) on termination of the Agreement **and within 6 weeks**"

On page 7, for 2.1 (Duration), the following phrase should be added to that line
"*unless terminated earlier in accordance with the terms of this contract by either party*"

Finally, we require a term included under "DURATION", which should then be renamed "DURATION AND TERMINATION", such as:

"*Any Party may leave this Agreement by giving thirty calendar (30) days' notice in writing to the other Parties.* "

[Back to Index]

Data Privacy Impact Assessment (DPIA)
Risk Stratification for Case Finding (IPA Tool)

Sign Off

This DPIA will:

- Be circulated to all GP partners at OHG to decide whether to proceed with such processing, in line with our DPIA policy
- In the event of agreement to proceed with this project, be published and available to patients, linked to within our privacy notice for this processing
- Be disclosable under FOI

Dr Neil Bhatia

GP, IG/FOI/Records Access lead, Caldicott Guardian, DPO
Oakley Health Group
28.10.18

Addendum 02.11.18

At the partners meeting on 2nd November, the 10 GP partners voted unanimously to proceed with processing, subject to:

- All recommendations made in the "conclusion" section of this DPIA being put into force
- Exclusion of children under the age of 18yrs old from processing
- A 6-week lead-in time to permit data subjects to express any objection prior to processing

Addendum 16.11.18

The CCG and CSU agreed to our suggestions and the data processor and information sharing agreements were signed accordingly.

Addendum 19.11.18

Fair processing information uploaded to website, Facebook page. Factsheets printed and distributed to all 3 sites. Privacy notice generated and added to GDPR booklet.