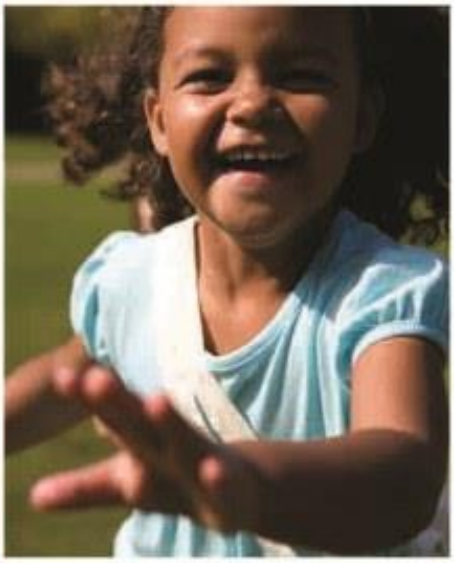
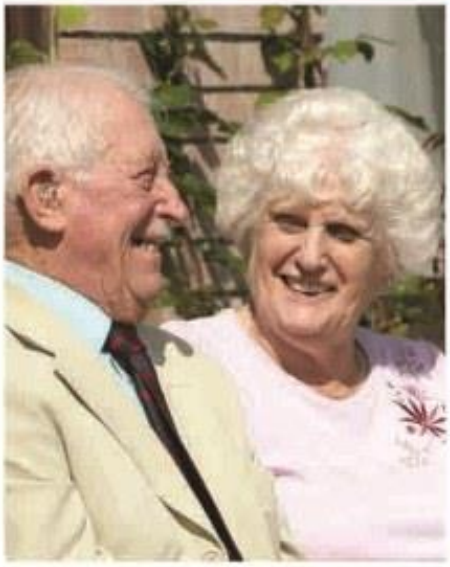
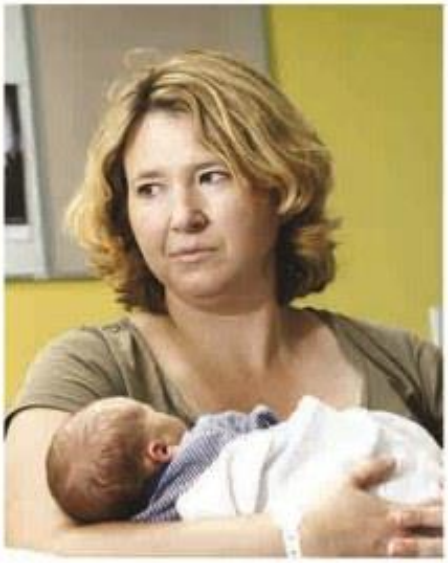
NHS England

Information Governance and Risk Stratification: Advice and Options for CCGs and GPs







THE NHS CONSTITUTION
the NHS belongs to us all

NHS England INFORMATION READER BOX		
Directorate		
Medical	Operations	**Patients and Information**
Nursing	Policy	Commissioning Development
Finance	Human Resources	

Publications Gateway Reference:	**177**
Document Purpose	Guidance
Document Name	Information Governance and Risk Stratification: Advice and Options for CCGs and GPs
Author	Karen Thomson Geraint Lewis
Publication Date	June 2013
Target Audience	CCGs, CSUs, GPs, IDSPs
Additional Circulation List	Department of Health, HSCIC, BMA, Intellect
Description	This document describes the options for GPs and CCGs to continue to perform risk stratification.
Cross Reference	N/A
Superseded Docs (if applicable)	The use of patient information in the Long Term Conditions Programme, London: Department of Health and Patient Information Advisory Group, December 2006 Advice on Risk Prediction and Stratification, London: National Information Governance Board for Health and Social Care, July 2012
Action Required	Review October 2013
Timing/Deadlines (if applicable)	
Contact Details for further information	england.riskstratificationIG@nhs.net Chief Data Officer's Team Patients and Information Directorate, NHS England, Quarry House, Leeds

Document Status

This is a controlled document. Whilst this document may be printed, the electronic version posted on the intranet is the controlled copy. Any printed copies of this document are not controlled. As a controlled document, this document should not be saved onto local or network drives but should always be accessed from the intranet.

Information Governance and Risk Stratification: Advice and Options for CCGs and GPs

Karen Thomson
Information Governance Lead

Geraint Lewis
Chief Data Officer

Key points

- Risk stratification tools can help determine which people in a population are at high risk of experiencing outcomes, such as unplanned hospital admissions, that are simultaneously: undesirable for patients; costly to the health service; and potential markers of low-quality care.
- Also known as *predictive risk models,* these tools are used widely in the NHS, both for:
    - analysing the health of a population ("risk stratification for commissioning"); and
    - targeting additional preventive care interventions, such as the support of a community matron, to high-risk patients ("risk stratification for case finding").
- The Health and Social Care Act 2012 has complicated the legal landscape relating to risk stratification (see page 10).
- In this paper, we:
    - **explain** the information governance issues relating to risk stratification
    - provide a **checklist** of steps that GP practices, CCGs, and other organisations involved in risk stratification should undertake to comply with the law (see page 13)
    - describe a range of **options** (options A to F) that CCGs can use in order to conduct risk stratification legally (see page 17)

Contents

Overview

Risk stratification tools have had a profound impact on the delivery of health services across the developed world.[1] These tools use relationships in historic population data to estimate the use of health care services for each member of a population. Risk stratification tools can be useful both for population planning purposes (known as "risk stratification for commissioning") and for identifying which patients should be offered targeted, preventive support (known as "risk stratification for case finding").

Published in April 2013, the second Caldicott review of information governance (Caldicott2) reaffirmed that risk stratification is *not* a form of direct care and that organisations need to identify a legal basis to process confidential patient information[a] for this purpose. To ensure that they comply with the law, all organisations that undertake risk stratification should adhere to the following recommendations.

- For **risk stratification for commissioning**: use pseudonymised data.

- For **risk stratification for case finding**:

    1. Use **pseudonymised data;**[b] or
    2. Where it is not feasible to use pseudonymised data, use **weakly pseudonymised**[c] data in an **Accredited Safe Haven**; or
    3. Where using **confidential patient information** can be **justified as necessary,**
        - ensure there is a legal basis to use identifiable data; and
        - ensure **there** are appropriate and robust **information governance controls** in place; and
        - clarify and document **data controllership** and **lines of accountability;** and
        - put in place appropriate **contractual arrangements** and manage these arrangements; and
        - ensure patients are **informed** about how their data will be used; and
        - put in place mechanisms that enable Patients' **objections** to be respected.[d]
    4. Where the data are **weakly pseudonymised**,
        - ensure **there** are appropriate and robust **information governance controls** in place; and

[a] Defined in Section 251 of the NHS Act 2006
[b] Data with no identifiers except unique pseudonyms that do not reveal patients' 'real world' identities
[c] Data with a **single** identifier such as the NHS number or postcode
[d] In line with the requirements of the NHS Constitution and the commitment given by the Secretary of State for Health at the launch of the Caldicott Review on 26 April 2013

- clarify and document **data controllership** and **lines of accountability;** and
- implement appropriate **contractual arrangements** and manage these arrangements; and
- ensure patients are **informed** about how their data will be used; and
- implement mechanisms that enable patients' **objections** to be respected.[e]

- **In order to ensure that they conduct risk stratification ethically and legally, GP practices and CCGs should follow the steps in the checklist shown on page 12 and use one of the options (options A – F) on page 16.**

- **We recognise that the issues covered in this document are complex. We will develop additional supporting materials in the coming weeks and will keep this document under continual review.**

[e] In line with the requirements of the NHS Constitution and the commitment given by the Secretary of State for Health at the launch of the Caldicott2 report on 26 April 2013

NHS England Position Statement

NHS England encourages CCGs and GP practices to use risk stratification tools as part of their local strategies for supporting patients with long-term conditions and to help prevent avoidable unplanned admissions.

As part of the 2013/14 GP contract, NHS England has introduced a new *directed enhanced service* (DES) that promotes the use of risk stratification tools for identifying and managing patients who are chronically ill or who are at high risk of emergency hospital admission.[f] GP practices choosing to take up this DES may elect to work collectively through their CCG to commission risk stratification tools. In this case, the risk stratification tool would be used to help identify patients at high risk of unplanned hospital admission (risk stratification for case finding). Alternatively, CCGs may themselves commission risk stratification services to support commissioning decisions more generally (risk stratification for commissioning). In this case, knowledge of the risk profile of a population can be useful for commissioning wider preventive services and for promoting quality improvement across member practices. In both cases, CCGs need the support and agreement of their member GP practices if risk stratification is to be conducted most effectively.

NHS England has asked CCGs to take the lead in agreeing the details of the risk stratification DES with their participating GP practices so that the arrangements support the CCG's wider strategy for patients with long-term conditions. NHS England is also working with the Health and Social Care Information Centre (HSCIC) to support this work. For example, regional offices of the HSCIC are being asked to make data services available to commissioners. However, capacity and capability issues within the HSCIC's regional offices mean that this support may not be fully available immediately in all circumstances. Therefore, NHS England has identified alternative arrangements that CCGs can pursue in the interim, as described in this document.

[f] Organisations wishing to take up this DES need to indicate by the end of June 2013 their intention to do so and must then deliver risk profiling for the latter three quarters of the 2013/14 financial year. For further details, see http://www.england.nhs.uk/wp-content/uploads/2013/03/ess-risk-profiling.pdf

Purpose

The purpose of this document is to address current concerns in the NHS relating to risk stratification. These concerns have arisen following the implementation of the Health and Social Care Act 2012 and the publication of the Caldicott2 review of information governance.

Scope

This document addresses the information governance arrangements for risk stratification – both *risk stratification for commissioning* and *risk stratification for case finding*. The information governance approaches proposed in this document are also applicable to urgent care dashboards. However, neither the information governance of integrated care programmes nor the issue of remuneration of CSUs and of HSCIC regional offices for supporting risk stratification are covered.

Background

In recent years, risk stratification tools have become an important part of local NHS strategies for supporting patients with long-term conditions. These tools are used both for understanding the characteristics of a local population (known as "risk stratification for commissioning") and for identifying individual patients who are at risk of adverse outcomes such as unplanned hospital admissions, and who may benefit from additional preventive support such as that provided by community matrons (known as "risk stratification for case finding"). Risk stratification tools have a number of synonyms, including "predictive risk models" and "risk profiling tools" (see Box 1).

Box 1: Terminology

For non-specialists, the following terms can be considered to be roughly synonymous:

- Risk stratification tools
- Risk profiling tools
- Risk prediction tools
- Predictive risk models
- Predictive models
- Risk models

One of the most common applications of risk stratification for case finding is to predict the risk for each individual in a population of experiencing an unplanned hospital admission in the next 12 months.[2] Unplanned hospital admissions are seen as an important event for health systems to predict and attempt to prevent because they simultaneously:

- are a marker of **potentially suboptimal** care; and
- represent a **poor patient experience**; and
- are **costly** to the health service.

In other words, unplanned hospital admissions are a "*Triple Fail event*".[3] Other examples of Triple Fail events that may be predicted using different predictive risk models include unplanned readmissions within 30 days of discharge, and unplanned admissions to nursing homes. Predictive models tend to be more accurate at predicting Triple Fail events than clinical opinion alone.[4,5] They can therefore be a useful tool for supporting clinical decision-making and are now in widespread use in the NHS.

Some predictive models are proprietary (e.g., the ACG system[6]) whereas others are open-source (e.g., PARR,[7] PARR-30,[8] and the Combined Predictive Model[9]). Predictive models have also been developed to stratify a population according to individual risk of being admitted to a nursing home or of starting another form of intensive social care in the next 12 months.[10] However, social care predictive models have yet to be implemented widely in practice.

Risk stratification tools typically use historic information such as age, gender, diagnoses, and patterns of hospital use as the basis of their predictions. Some models (e.g., PARR and PARR-30) use a combination of hospital data and geographical data such as the *Index of Multiple Deprivation*. Other models (e.g., the Combined Predictive Model) use primary care data derived from GP practice systems in addition to hospital data as the basis of their predictions.

Current Issues

The legal landscape in relation to the use of personal data changed following the implementation of the Health and Social Care Act 2012 and the re-organisation of the NHS in England on 1 April 2013. These changes have had several implications for risk stratification, including:

- **CCGs do not have the same functions and powers as primary care trusts (PCTs).** PCTs had statutory bases to access confidential information,[g] and could then use these data in pseudonymous form to conduct risk stratification.[h]
- **The statutory authority of CCGs and CSUs to process confidential information for risk stratification must come either from patient consent or from the Section 251 regulations**, as there is no other statutory support available. However, the current Section 251 approval excludes the processing of identifiable data for risk stratification. The framing of the legislation excludes the use of identifiable data where it is feasible to use anonymised or pseudonymised data, or where consent is practicable.[i] It has been demonstrated that using pseudonymised data is feasible (even if not for all of the tools available). Furthermore, obtaining patient consent is typically impracticable for risk stratification purposes and indeed may worsen health care inequalities since patients living in more deprived areas tend to be less likely to provide consent for their data to be processed.[11]
- **While the HSCIC has statutory powers under the Health and Social Care Act 2012 to collect and process confidential information, the circumstances in which it can disclose information are limited by law.** These limitations restrict the ways in which identifiable data can be lawfully disclosed for risk stratification purposes.

In parallel, the second Caldicott review of information governance (Caldicott2)[12] confirmed previous guidance on the topic of risk stratification.[13,14] Specifically, the review confirmed that:

- **risk stratification is a form of *indirect* care rather than direct care**

[g] For example, to manage the GMS and PMS contracts, and for commissioning purposes under the Section 251 regulations.
[h] For example, PCTs could run algorithms on the data using an encryption tool embedded in the software. This arrangement prevented PCT staff from viewing the data but generated outputs as a series of encrypted files. These files were sent to each GP practice and contained the risk scores for their respective patients. However, the regulations supporting the management of primary care have now transferred to NHS England and CCGs do not have the same statutory bases to access confidential information as did PCTs.
[i] While "having regard to the cost and technology available"

- **organisations must not use *personal confidential data* for risk stratification purposes, unless they have a legal basis for doing so**[j]
- **risk stratification should generally be performed using pseudonymous data**
- **only clinicians who have a legitimate relationship with an individual patient may access their re-identified data in order to decide whether to offer them a preventive service such as the support of a community matron.**

For all of these reasons, it is important for CCGs and GP review their local arrangements to ensure that any risk stratification being conducted on their patients' data is done so in ways that are consistent with the new legal environment.

Recommendations

To ensure that they comply with the law, organisations that undertake risk stratification should adhere to the following advice.

- For **risk stratification for commissioning**: use pseudonymised data.
- For **risk stratification for case finding**:
  - Use **pseudonymised data;**[k] or
  - Where it is not feasible to use pseudonymised data, use **weakly pseudonymised**[l] data in an **Accredited Safe Haven**; or
  - Where using **confidential patient information** can be **justified as necessary,**
    - ensure there is a legal basis to use identifiable data; and
    - ensure **there** are appropriate and robust **information governance controls** in place; and
    - clarify and document **data controllership** and **lines of accountability**; and
    - Put in place appropriate **contractual arrangements** and manage these arrangements; and
    - ensure patients are **informed** about how their data will be used; and
    - put in place mechanisms that enable Patients' **objections** to be respected.[m]

[j] For further details, see Annex 2 – Legal Aspects
[k] Data with no identifiers except unique pseudonyms that do not reveal patients' 'real world' identities
[l] Data with a **single** identifier such as the NHS number or postcode
[m] In line with the requirements of the NHS Constitution and the commitment given by the Secretary of State for Health at the launch of the Caldicott Review on 26 April 2013

- Where the data are **weakly pseudonymised**,
    - ensure there are appropriate and robust **information governance controls** in place; and
    - clarify and document **data controllership** and **lines of accountability;** and
    - implement appropriate **contractual arrangements** and manage these arrangements; and
    - ensure patients are **informed** about how their data will be used; and
    - implement mechanisms that enable patients' **objections** to be respected.[n]

These principles are considered in more detail in the checklist on page 13 and in the frequently asked questions (FAQs) in Annex 3. An explanation of the legal requirements underpinning this advice is provided in Annex 2.

[n] In line with the requirements of the NHS Constitution and the commitment given by the Secretary of State for Health at the launch of the Caldicott2 report on 26 April 2013

Checklist

CCGs, GP practices, and other organisations involved in conducting risk stratification for case finding are advised to use the checklist provided in Box 2.

Box 2: Checklist for CCGs, GP practices, and other organisations conducting risk stratification for case finding

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 Management Integration Centre)
   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 (see Box 6).

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 the adverse outcome to be predicted, the accuracy of the predictions, the cost of the model and its software, and the availability of the data on which it is run.[15] 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 only legal basis to process identifiable data "*in the clear"* [o] for risk stratification purposes is 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).[p]

[o] "In the clear" is where an individual can view the data in identifiable form
[p] To comply with the Data Protection Act 1998, only the minimum amount of data necessary to fulfil the purpose should be used.

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***[q] 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 (see Question 11 in Annex 3). 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.[r] These controls include but are not limited to:

   a) Checks to verify the accuracy of the data and to ensure they are up to date.

   b) 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).

   c) Checks that the data are not processed outside the European Economic Area unless there are equivalent legal, technical, and organisational measures in place to protect the data appropriately. The data controllers releasing the data will need to consider whether they have the resources to performance-manage offshore contractors; to ensure there are adequate information governance controls in place; and to check that these arrangements are being implemented effectively.

10) Establish appropriate **contractual arrangements**[s] 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.[t] 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

[q] Defined in Section 12 of the Data Protection Act 1998. For further details, see Annex 3
[r] See Paragraph 12, Schedule 1 Part 2 of the Data Protection Act 1998
[s] Based on the standard contract terms and conditions, but with additional safeguards included as appropriate
[t] Further consideration needs to be given to how this process can be implemented in systems effectively, so it is likely that a manual process will be needed in the short to medium term.

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 (these materials may be incorporated into wider *fair processing* information).

12) **Inform patients** that their identifiable or weakly pseudonymised data[u] may be used for risk stratification purposes.[v]

13) Conduct risk stratification using one of the options outlined in Annex 1 of this document (i.e., options A – F).

14) Ensure that only those **clinicians who are directly involved** in a patient's care can see a patient's identifiable risk score.

15) 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.[w]

16) Refer patients to preventive services **only with their consent**.

17) Using pseudonymous data, **evaluate and refine** the risk stratification model used and the preventive interventions offered according to its predictions.

Annex 1 of this document sets out a range of options that are viable either now or in the future depending on local circumstances. By adopting one or more of these options, CCGs and GP practices can conduct risk stratification legally and in ways that comply with current information governance standards. These options require NHS England to issue *Directions* to the HSCIC to process and provide data to support risk stratification. They are neither exhaustive nor mutually exclusive; instead, they are intended to be illustrative and should be reviewed locally by an information governance manager or lead. In summary, these options are:

Option A - Closed-system technologies
Option B - Pseudonymisation at landing
Option C - Using HSCIC services
Option D - With consent as part of an integrated care programme
Option E - Pseudonymisation at source
Option F - Accredited Safe Haven

[u] Still likely to be personal data under the Data Protection Act 1998, so the *fair processing* obligation remains
[v] See Annex 3
[w] 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.

The choice of which option or options to pursue will depend on a range of local factors, including the current arrangements, any contractual obligations, and the capacities and capabilities of the local CSU and the HSCIC regional office.

Further information

Further information may be obtained from the *Risk Prediction Network* on NHS networks (see http://www.networks.nhs.uk/nhs-networks/risk-prediction-network/?searchterm=risk%20stratification)

Examples of different approaches to risk stratification can be found in the advice produced by the (now defunct) National Information Governance Board for Health and Social Care, "*Risk Prediction and Stratification"*, published in July 2012 (see www.nigb.nhs.uk/advice).

Further advice on the information governance aspects of risk stratification should be obtained in the first instance from local information governance managers and leads. For more complex queries, please contact england.riskstratificationIG@nhs.net

Annex 1 - Options for Risk Stratification

In this annex, we list six approaches to risk stratification that are or will be available to GPs and CCGs for risk stratification purposes, together with the advantages and disadvantages of each option. The current availability and the desirability of each option will vary according to a range of local factors, including:

- current arrangements with local providers;
- any existing contractual obligations;
- technical and human resource capacities and capabilities of the local CSU, and/or HSCIC regional office to support each option, including:
    - how rapidly a CSU can satisfy the requirements to become an ASH
    - local use of closed-system technology;
    - whether the chosen risk stratification tool can be used openly or under licence by the CSU or by the regional office of the HSCIC;
    - staff time;
    - remuneration arrangements;
- whether risk stratification is undertaken as a programme of work in isolation or if it forms part of a broader programme of integrated care.

Note that for all of these options, we assume that the checklist in Box 2 has been followed in relation to planning, communications, information governance requirements, clinical review, patient objections, and the audit and evaluation of the programme.

The options are:

Option A - Closed-system technologies
Option B - Pseudonymisation-at-landing
Option C - use of HSCIC services
Option D - With consent as part of an integrated care programme
Option E - Pseudonymisation-at-source
Option F - **Accredited Safe Haven**

NHS England will issue directions to the HSCIC instructing it to support the collection and processing of GP data for risk stratification. These directions will provide a legal basis for the collection of GP data by the HSCIC for this purpose. However, CCGs and/or their local CSUs will need to reimburse the HSCIC for any costs that it incurs as a result of the arrangements agreed locally.

Options

Option A – Closed-system technologies

This option involves the flow of identifiable data (or weakly pseudonymised data) from the HSCIC and/or from GP clinical systems directly into a closed system that processes the data automatically. No human sees the data during this process and therefore no breach of confidence occurs. A secure portal is provided for the clinicians responsible for the care of these patients to view their patients' risk scores and potentially to access other data relating to the patient.

Option A – Closed-system technologies

Steps

1. The GP or CCG asks either an independent sector data services provider (IDSP) or a CSU to conduct risk stratification on behalf of its GP practices. The IDSP or CSU does so under contract, as a data processor. In some instances, the CCG may have in-house processing capacity and may under take risk stratification as a data processor on instruction from the GP as data controller.
2. The GP or CCG asks the HSCIC to provide SUS data for risk stratification purposes and signs the HSCIC's data sharing contract for the SUS data, once the HSCIC is satisfied that the body receiving the data has adequate information governance controls in place.
3. The GP practice collates a list of the verified NHS numbers for those patients who have not objected to the use of their information for risk stratification purposes and sends this list to the HSCIC.
4. The HSCIC collates the SUS data on all the listed patients (i.e. those who have not objected) and provides this information to the body undertaking the risk stratification analysis. The data are provided in identifiable form. They are sent via secure transfer directly into the data processor's closed system. Where the data to be used are weakly pseudonymised then they will include the NHS number but no other direct identifiers.
5. The GP practice either (a) instructs their GP system supplier or (b) asks the HSCIC's GP Extraction Service (GPES) or the HSCIC's data services for commissioning to extract GP data for those patients that have not objected. These data, containing the same verified NHS numbers, are sent via secure transfer directly into the data processor's closed system.
6. The data are linked automatically by the system using the NHS number and possibly also date of birth and postcode.
7. The risk stratification tool is run automatically on the data. The risk-stratified data are then fed automatically into a secure portal for authorised users (i.e., the GPs who have commissioned the risk stratification) to view the risk scores for

individual patients registered in their practice in identifiable form. The portal may also have the capacity to display the underlying SUS data via a webpage, which asks the GP to confirm that the individual patient is aware of and consents to this sharing of their secondary care information. In some instances these tools have the functionality to allow the GP to manipulate the data in different ways (e.g. examining patients with a high risk score and a particular long term condition). Additionally, the portal should also have the functionality to provide pseudonymised and aggregated views of the data, which can support GPs in their role as commissioners. Aggregated information could be shared with colleagues in the CCG.

Legal considerations

Note that this option may involve the use of identifiable data or weakly pseudonymised data.

Where identifiable data are used, the organisation processing the data must be either:

- the data controller (i.e., the GP); or
- a data processor operating under contract to the data controller.

Although identifiable data are used, there will be no breach of confidence because (a) the processing is undertaken entirely by the software; and (b) and no human views the data in identifiable form. As indicated by Annex 2, if the common law duty of confidence can be satisfied in this way then the other legal requirements under the Data Protection Act (DPA) and the Human Rights Act (HRA) are also satisfied, assuming sufficient information governance controls are in place.[x]

The HSCIC has indicated that it is willing to disclose identifiable data to closed system technologies under contract and with safeguards, on the basis that as the data are not viewed, no breach of confidence will occur. Similarly, a GP practice would also need to be satisfied that any organisation to which it was disclosing identifiable data had the appropriate information governance safeguards in place and was operating under contract to the data controller (e.g. the system would need to be able to verify the identity and access permissions of the persons using the portal).

Advantages

- Many of the current proprietary risk stratification tools are designed to use identifiable data (or at least NHS number) using closed system technologies.
- Allows existing contracts using this model to continue

Disadvantages

- Involves the flow of identifiable data from the HSCIC and GP record systems to external systems

Conclusion

This is a viable option now.

[x] For example, to satisfy Data Protection Principle 7 requirements

Option B – Pseudonymisation at landing

This option is similar to using closed system technologies in that identifiable data again need to flow into the system. Here, however, as the data land in the system, they are automatically pseudonymised. As a result, no person can view the data prior to pseudonymisation. The pseudonymised data can then be manipulated and analysed by the analytical staff.

Option B – Pseudonymisation at landing

Steps

1. The GP or CCG asks either an IDSP or a CSU to conduct risk stratification on behalf of its GP practices. The processing takes place under contract as data processors. In some instances, the CCG may have in-house processing capacity and may under take risk stratification as a data processor on instruction from the GP as data controller.
2. The GP or CCG asks the HSCIC to provide SUS data for risk stratification purposes and signs the HSCIC's data sharing contract for the SUS data, once the HSCIC is satisfied that the body receiving the data has adequate information governance controls in place.
3. The GP practice collates a list of the verified NHS numbers of those patients who have not objected to the use of their information for risk stratification purposes, and sends this list to the HSCIC.
4. The HSCIC collates the SUS data on all the listed patients (i.e. those who have not objected) and provides this information to the body undertaking the risk stratification. The data are sent in identifiable form via secure transfer and directly into the landing stage of the data processor's system. Where the data to be used are weakly pseudonymised, they will include the NHS number but no other direct identifiers.
5. The GP practice either (a) instructs either their GP system supplier or (b) asks the HSCIC's GP Extraction Service (GPES) or the HSCIC's data services for commissioning to extract the data for those patients that have not objected. The data, containing the same verified NHS numbers, are sent via secure transfer, directly into the landing stage of the data processor's system.
6. Within the landing stage, the system automatically links and pseudonymises the data. The risk stratification tool provider's staff can then analyse the data in pseudonymised form to produce a risk score for each patient.
7. The risk scores are made available via a secure portal to authorised users (i.e., the GPs who commissioned the risk stratification). This portal allows GPs to view the risk scores for the individual patients registered in their practice in identifiable form. The portal may also have the capability of displaying the underlying SUS data via a webpage that asks the GP to confirm that the individual is aware of and consents to this sharing of their secondary care information. In some

instances, these tools have the functionality to allow the GP to manipulate the data in different ways (e.g. examining patients with a high risk score and a particular long term condition). Additionally, the portal should also have the functionality to provide pseudonymised and aggregate views of the data that can support the GPs role as commissioner. Aggregated data could be shared with colleagues in the CCG.

Legal considerations

Again, because no human can view the data in identifiable form, there will be no breach of confidence and hence the legal requirements can be satisfied. Organisations processing data in this way must be either:

- the data controller (i.e., the GP); or
- a data processor operating under contract to the data controller.

The HSCIC has indicated that it is willing to disclose identifiable data to organisations using pseudonymisation at landing under contract and with safeguards, on the basis that as the data are not viewed, no breach of confidence will occur. Similarly, a GP practice would also need to be satisfied that any organisation to which it was disclosing identifiable data had the appropriate information governance safeguards in place and was operating under contract to the data controller (e.g., the system would need to be able to verify the identity and access permissions of the persons using the portal).

Advantages

- Many of the current proprietary risk stratification tools are designed to use identifiable data (or at least NHS number) using pseudonymisation at landing.
- Allows existing contracts using this model to continue

Disadvantages

- Involves the flow of identifiable data from the HSCIC and GP record systems to external systems

Conclusion

This is a viable option now.

Option C – Using HSCIC Services
There is a variety of ways in which the HSCIC could support risk stratification, all of which would need funding. For example, the HSCIC could:

- hold the data in a **secure data management environment**, hosting the risk stratification tools so that authorised users can run risk stratification within this secure environment (Option C1)
- provide a **re-identification service** for GPs (Option C2)
- **verify, link and pseudonymise** the data (Option C3)

Option C1 – Using the HSCIC to hold the data in a secure data management environment

Description
All the relevant data are held by the HSCIC, which validates the accuracy of the data; links the GP and SUS data together; and hosts the risk stratification tools within a secure data management environment. The HSCIC then makes these tools available to authorised users remotely, who can process and manipulate the data but without viewing it in identifiable form. Once the data have been risk stratified, the HSCIC would provide GPs with data:

- in identifiable form for care purposes (i.e., authorised access to their own patients' data)
- in pseudonymised and aggregated forms for commissioning purposes.

Steps
1. The GP practice or CCG asks the HSCIC to provide risk stratification services using the preferred tool of the GP (provided this is available to be hosted within the HSCIC).
2. The GP practice (or CCG on behalf of its practices) signs the HSCIC's data sharing contract.
3. The GP practice collates a list of the verified NHS numbers of those patients who have not objected to the use of their information for risk stratification purposes, and instructs either their GP system supplier or asks the HSCIC's GP Extraction Service (GPES) or the HSCIC's data services for commissioning to extract the data only for those patients that have not objected.
4. These data are sent via secure transfer to the HSCIC.
5. The HSCIC collates the SUS data for all of the patients for whom it has received GP data (i.e. those who have not objected), performs data validation, and links the data. The HSCIC then makes the data available within its secure data management environment for use with the risk stratification tools in much the same way as HES Business Objects currently functions.
6. Authorised users can then log into the system to use the risk stratification tools available. The tools could have a variety of functionalities, including a view of the risk

score and the underlying detailed data in identifiable form for care purposes; and in pseudonymised and aggregate form to support the GP's role as commissioner.

Legal considerations
The HSCIC is able to hold and use identifiable patient data under the Health and Social Care Act 2012. It is therefore in a position to verify the accuracy, link and make data available in a variety of forms to authorised users as appropriate to their role.

Advantages
- Identifiable data are only processed by the HSCIC and the GP practice
- Because the data can be processed in identifiable form with the HSCIC, the data should be of higher quality. As a result, the linkage between the GP data and the SUS data should be more effective
- Holding the data and risk stratification tools together within the HSCIC makes for a simple and streamlined process
- Other data streams can be added as they become available within the HSCIC.

Disadvantages
- While the HSCIC's *Data Services for Commissioners* may already be providing this service at a local level in some areas, there is an issue about the capacity of the HSCIC to take on this role at present and it will take some time to develop this service nationwide.
- While all open source tools, and some proprietary tools can be hosted by the HSCIC under licence, other providers of proprietary risk stratification tools may be unwilling to allow the HSCIC to host their tool.

Conclusion
This is not currently viable in most areas but may be a preferred solution for the medium term. A list of HSCIC regional offices where this service is available will be posted on the HSCIC website.

Option C2 – Using the HSCIC to provide a re-identification service for GPs

Description
This is a service that can be used in conjunction with either:
- Option C3 (HSCIC verify, link and pseudonymise the data). After the HSCIC has provided pseudonymised data to a risk stratification tool provider, the HSCIC could provide a portal for GPs to be able to re-identify individual patients; or
- Option B (pseudonymisation at source). Here, the HSCIC would provide a service for managing the pseudonymisation key.

Steps
1. The GP or CCG asks either an IDSP or a CSU to conduct risk stratification on behalf of its GP practices using pseudonymised data. In some instances, the CCG may have in-house processing capacity and may under take risk stratification on behalf of

the GP.

2. The GP or CCG may have previously asked the HSCIC to provide a data validation, linkage and pseudonymisation service using both SUS and GP data for risk stratification purposes; or it may have adopted a pseudonymisation-at-source approach.
3. In either case, the GP will need to sign the HSCIC's data sharing contract for the risk stratification provider to receive the SUS data in pseudonymised form.
4. The GP practice collates a list of the verified NHS numbers of those patients who have not objected to the use of their information for risk stratification purposes and sends this list to the HSCIC to extract the SUS data.
5. The GP practice will either have to ask the HSCIC to provide it with a pseudonymisation key (so that the GP data can be extracted using the same key as the SUS data) or it will need to ask the GP system supplier to provide the pseudonymistion key and send this key to the HSCIC.
6. The GP practice either (a) instructs their GP system supplier or (b) asks the HSCIC's GP Extraction Service (GPES) or the HSCIC's data services for commissioning to extract the data for those patients that have not objected, using the same list of verified NHS numbers. This information is sent in pseudonymised form via secure transfer to the risk stratification provider.
7. The HSCIC collates the SUS data for all the listed patients and provides these data via secure transfer to the risk stratification provider in pseudonymised form *using the same key*.
8. The risk stratification provider then links and analyses the data and makes the risk stratified data available via a secure portal to the HSCIC and authorised users in pseudonymised form.
9. 7 In addition, the HSCIC could provide a portal that is connected to (and sits in front of) the risk stratification provider's portal. The HSCIC's portal would then re-identify the risk scores of individual patients and the underlying data, and make this information available to authorised users.

<u>Legal considerations</u>

The HSCIC is able to hold and use identifiable patient data under the Health and Social Care Act 2012. It is therefore in a position to verify the accuracy, link, and make data available in a variety of forms to authorised users as appropriate to their role.

<u>Advantages</u>

- This option would offer a single, national portal for GPs to access risk stratified data, with standardised access controls for users;
- It could build on existing user registration, identity management and authentication processes.
- It could facilitate access to a wide variety of tools
- It could ensure appropriate management of pseudonymisation keys

Disadvantages

- As most existing tools do not currently utilise pseudonymised data, it is not an appropriate approach at present

Conclusion

It is not currently a viable option; however, it may be a solution in the longer term (both for tools sitting outside the HSCIC as well as those hosted within it).

Option C3 – Using the HSCIC to verify, link and pseudonymise the data

Description

All the relevant data are sent to the HSCIC, which conducts the initial steps to process the data for risk stratification, including validating the accuracy of the data; linking GP and SUS data together; and pseudonymising the data. The HSCIC then passes the linked, pseudonymised data to another body to run the risk stratification analysis. Finally, the HSCIC provides the means to re-identify individuals to the GP practice.

Steps

1. The GP or CCG asks either an IDSP or a CSU to conduct risk stratification on behalf of its GP practices using pseudonymised data. In some instances, the CCG may have in-house processing capacity and may undertake risk stratification on behalf of the GP.
2. The GP or CCG asks the HSCIC to provide a data validation, linkage, and pseudonymisation service using both SUS and GP data for risk stratification purposes. It signs the HSCIC's data sharing contract for the SUS data, once the HSCIC is satisfied that the body receiving the data has adequate information governance controls in place.
3. The GP practice collates a list of the verified NHS numbers of those patients who have not objected to the use of their information for risk stratification purposes and either (a) instructs their GP system supplier or (b) asks the HSCIC's GP Extraction Service (GPES) or the HSCIC's data services for commissioning to extract the data for those patients that have not objected, using this list of verified NHS numbers. These data are sent via secure transfer to the HSCIC.
4. The HSCIC collates the SUS data for all the patients for whom it has received GP data (i.e. those who have not objected) and performs validation, linkage, and pseudonymisation on the data. The HSCIC then provides this information to the risk stratification provider in pseudonymised form via secure transfer.
5. The risk stratification provider then analyses the data and makes the risk-stratified data available via a secure portal to authorised users in pseudonymised form. The tool could have a variety of functions in addition to providing a view of the risk score, such as providing the underlying detailed data in pseudonymised form, and aggregated data that can support the GP's role as commissioner. Aggregated data

could be shared with colleagues in the CCG.

6. In parallel, the HSCIC provides the GP with the pseudonymsation key so that when the risk stratification provider makes the data available to the GP, a staff member within the GP practice delegated with the task of re-identifying individuals can identify the individuals with the highest risk scores that are to be offered further services.

Legal considerations

The HSCIC is able to hold and use identifiable patient data under the Health and Social Care Act 2012. It is therefore in a position to verify the accuracy, link, and make data available in pseudonymised form (or in identifiable form where the recipient has a legal basis to obtain them).

Advantages

- Identifiable data are only processed by the HSCIC and the GP practice
- Because the data can be processed in identifiable form with the HSCIC, the data should be of higher quality, and the linkage between the GP data and the SUS data should be more accurate.

Disadvantages

- Most current risk stratification tools are not designed to use pseudonymised data;
- There is additional work for the GP practice to re-identify the relevant patients before they can review the results

Conclusion

This is not currently a viable option.

Option D – Consent
There are several advantages to seeking consent at the start of the process from all the individuals whose data are to be processed:

- It provides greater flexibility in relation to the approaches taken;
- It means that individuals will not be surprised to receive a communication from a community matron or from another staff member with whom they have not previously had contact; and
- It is useful where the risk stratification tool may be used for automated decision-taking.

However, seeking consent has implications for health care inequalities because the most vulnerable patients tend to be the least likely to respond to a request for consent, unless it is sought within the context of a routine consultation. Note that if for whatever reason it is not possible to use pseudonymised data, consent is the only lawful means to conduct risk stratification where data from both health and social care are to be used.

Option D – With consent as part of an integrated care programme

Description
In some local areas, an integrated care programme may exist to provide services in a more unified manner to patients with multiple care needs. Here, a process of consent will be in place for sharing information across health and social care. Risk stratification could be included within this consent process in relation to the *fair processing* information provided to individuals as part of the integrated care programme.

Steps

1. The GP practice (or CCG on their behalf) will work with colleagues such as those in social care to agree the details of an integrated care programme. As part of this agreement, consideration will need to be given to (a) what kind of data need to be shared; (b) how is this sharing of data should be communicated to patients; and (c) how their consent will be obtained to enable the described information to be shared by professionals across health and social care.

2. The initial process of informing individuals may be undertaken by either the GP practice, the CCG on their behalf, or the local authority's adult social care team. This process must include risk stratification as one purpose of data sharing, together brief explanation about which organisations and which types of staff may obtain access to their confidential data. The provision of this information would then need to be followed up with a consent process. Patients' consent may be obtained by letter, by telephone, or during routine consultations. Implied consent is not acceptable for this option see Annex 2 – 'why can consent not be implied'.

3. Once consent has been obtained, patients' data may be shared both for risk stratification and for the other purposes covered by the consent process.

4. The GP practice (or the CCGs on its behalf) would then collate a list of the verified NHS numbers of those patients who had given their consent. It would then request to the HSCIC for the SUS data for those patients to be sent to the risk stratification provider.

5. The GP practice would need to sign the HSCIC's data sharing contract on behalf of the risk stratification provider, which would act as a data processor under contract. As part of this process, both the HSCIC and the GP as data controller should assure themselves of the information governance controls that risk stratification provider has in place.

6. The HSCIC would then provide the SUS data in identifiable form to the GP practice or to the body undertaking risk stratification on behalf of the GP.

7. Using the same list of verified NHS numbers, the GP would instruct the GP's system supplier to provide the GP data for those individuals who had given their consent (or ask the HSCIC to extract the GP data on their behalf via GPES or HSCIC's data services for commissioners) and provide these data to the risk stratification provider.

8. The risk stratification provider would then process the data and provide the results via secure transfer back to the GP.

<u>Legal considerations</u>

Sometimes, risk stratification forms one element of a wider programme of integrated care. Since consent will be needed for the disclosure of information across different parts of the health and social care system, there may be an opportunity to include information about risk stratification in the fair processing information provided to patients, and to obtain patients' explicit consent for the use of their data both for integrated care and for risk stratification. Such consent then provides a legal basis for the use of patients' identifiable data for risk stratification (and for the other purposes that form part of providing integrated care). For risk stratification that includes both health and social care data, the only applicable legal basis in relation to confidentiality and the Data Protection Act is consent (aside from using pseudonymised data).

Identifiable data can be obtained from HSCIC provided that the data controller is able to offer evidence of consent. As it is not currently technically feasible to provide such evidence electronically for each individual patient, other evidence may be sufficient, such as providing an appropriate consent protocol and evidence that a system is in place for managing the data of patients who withhold their consent or who give their consent and later withdraw it.

Since consent is in place, there is no issue with patients' secondary care data being shared with their GP.

Advantages

- Provides greater freedom in relation to which bodies can be involved in processing the data and which tools may be used;
- Explicit consent from patients means that they are informed and are less likely to object later to how their personal and confidential information have been used;
- It accords with an integrated care approach, where consent for risk stratification will be part of the consent process for integrated care.

Disadvantages

- Relatively laborious and not cost effective if only used for risk stratification;
- A significant proportion – and possibly a majority – of patients will not typically reply to communications;
- May worsen health care inequalities if patients in more deprived areas or with greater health needs are less likely to respond (a phenomenon known as the *inverse equity hypothesis*[11]*)*.

Conclusion

This is a viable option in the context of an integrated care programme but has a number of disadvantages. Alternatively, one of the other options for risk stratification could be used, prior to gaining consent for the integrated care programme once patients have been selected based on their risk profile.

Option E – Pseudonymisation at source

This option involves all suppliers of data using the same pseudonymisation mechanism and the same pseudonymisation key.

Option E – Pseudonymisation at source

Description

The data are pseudonymised by the bodies that legitimately hold the data. They use the same pseudonymisation key to facilitate linkage by the risk stratification provider.

Steps

1. The GP or CCG asks either an IDSP or a CSU to conduct risk stratification on behalf of its GP practices using pseudonymised data. In some instances, the CCG may have in-house processing capacity and may undertake risk stratification on behalf of the GP.
2. The GP or CCG asks the HSCIC to provide the risk stratification provider with pseudonymised SUS data, using an agreed pseudonymisation approach. Either the HSCIC generates the pseudonymisation key (which can then be provided to the GP practice for their system supplier to use) or the GP system supplier is asked to generate the pseudonymisation key (which is sent to the HSCIC).
3. Before the risk stratification provider can receive the SUS data in pseudonymised form, the GP will need to sign the HSCIC's data sharing contract.
4. The GP practice also either (a) instructs their GP system supplier or (b) asks the HSCIC's GP Extraction Service (GPES) or the HSCIC's data services for commissioning to extract GP data in pseudonymised form, using the agreed key. The pseudonymised data are sent via secure transfer to the risk stratification provider.
5. The HSCIC collates the SUS data for all the relevant patients and provides these data via secure transfer to the risk stratification provider in pseudonymised form, using the agreed key.
6. The risk stratification provider then links and analyses the data and makes the risk stratified data available via a secure portal to the authorised users in pseudonymised form.
7. The GP, a delegated member of staff, or possibly their system supplier, could re-identify the individuals by reversing the pseudonymisation process for those individuals identified as highest risk. This process may be undertake using a look-up table; or, if the pseudonym is available within the GP system, then it may be feasible for the GP system to receive an automatic feed of risk scores. The system could then include the score within the GP record and/or produce a report listing the high-risk patients.

Legal considerations

- As this process uses pseudonymised data, it means that no legal basis for processing is required until the GP receives the risk score from the provider. At that point, the data are used for direct care purposes and consent can be implied.

Advantages

- Keeps identifiable data within their current systems
- As the data are pseudonymised, there is no need to consider objections for the disclosure of data, other than the general objection to all disclosures to the HSCIC.
- As the data are pseudonymised, there is no need to inform patients about how their data are to be used. It needs to be born in mind, however, that this does not remove the obligation to notify individuals where the results of the risk stratification are to be used for automated decision-taking (see Annex 3).

Disadvantages

- Current tools do not tend to use pseudonymised data
- Needs careful management of the pseudonymisation keys
- Needs development work for the data being re-identified within the practice or the HSCIC to provide a re-identification service portal

Conclusion

This is not currently a viable option.

Option F- Accredited Safe Haven

This option is currently in development. The concept of an accredited safe haven (ASH) is that it is a secure environment in which data that is weakly pseudonymised can be processed with organisational and technical safeguards to prevent re-identification, to satisfy the common law duty of confidence within the context of the ASH. The data within the safe haven because it is only weakly pseudonymised still constitutes personal data and therefore needs to meet Data Protection requirements. Because it is only weakly pseudonymised it would still be subject to the common law duty of confidence,[y] if released from the ASH.

Option F – Accredited Safe Haven

Description

Weakly pseudonymised data (i.e., data with one direct identifier such as the NHS number) can be processed within an Accredited Safe Haven environment for a variety of medical purposes in the public interest. These purposes include risk stratification and do not require a statutory basis as the data are sufficiently de-identified to satisfy the common law (albeit that the data still constitute personal data under the Data Protection Act).

Steps

1. The GP or CCG (on behalf of the GP practice) asks a commissioning organisation that has been accorded the status of Accredited Safe Haven (ASH) to conduct risk stratification on behalf of the practice (or group of practices). This ASH could be a CSU or, exceptionally,[z] the CCG itself.
2. The GP practice collates a list of the verified NHS numbers of those patients who have not objected to the use of their information for risk stratification.
3. Using the same list of verified NHS numbers, the GP practices asks either (a) their GP system supplier or (b) the HSCIC's GPES or the HSCIC's data services for commissioning service to extract the GP data for those patients who have not objected.
4. These GP data are sent to the HSCIC.
5. In parallel, the GP or CCG would ask the HSCIC to provide a linkage service to link the GP data with SUS data and to provide the linked and weakly pseudonymised data (i.e., with the NHS number, or other agreed identifier) to the ASH.
6. An ASH organisation will need to sign a contract with the GP as data controller setting out (a) the purposes for which the data are to be used, (b) the information governance safeguards that will be adhered to, and (c) the rights of the controller to audit how the data are used, etc.
7. The CSU or CCG undertaking the risk stratification would process the data in weakly pseudonymised form within the ASH, and make the risk stratification score (and potentially other data) available to the GP via a secure portal outside of the ASH. The portal would be hosted within the CSU and would enable

[y] As well as the Data Protection and Human Rights Acts.

[z] It is expected that all CSUs will seek to become ASHs; overall, however, the numbers of ASHs are expected to remain low.

authorised users (i.e., the GPs) to access the data in identifiable form or with the NHS number so that a staff member within the practice would quickly be able to re-identify those individuals at highest risk.

Legal considerations

- This option involves using weakly pseudonymous data (i.e., data containing only one identifier, such as the NHS number). The ASH organisation will not require a legal basis to obtain weakly pseudonymised data provided that the organisation has been accredited as meeting the ASH requirements to protect the data and to prevent the re-identification of individuals. As it includes the NHS number or another identifier, the ASH can link data obtained from multiple sources.
- Commissioning organisations working towards ASH status do not have support under the current Section 251 approval to process data for risk stratification purposes. Such organisations would need to demonstrate that they met the relevant standards before attaining full ASH status.

Advantages

- Enables risk stratification tools hosted within an ASH to use the NHS number for linkage;
- Because both CSUs and CCGs meeting the requisite standards can become ASHs, this arrangement creates more capacity for analysis overall but also provides greater flexibility to meet different local needs
- A simple approach for GPs

Disadvantages

- The ASH accreditation criteria and process are not yet agreed and it is an untested approach
- Some of the risk stratification tools may not currently be able to produce reliable results using only the NHS number;

Conclusion

This will be a viable option shortly, once the requirements and accreditation process for ASHs have been approved.

Annex 2 - Legal aspects

Overview

This annex covers the following topics:

- The general legal framework for lawful processing
- The legal framework to process personal and confidential data for risk stratification
- How the Health and Social Care Act 2012 changed the legal landscape
- How the HSCIC can receive and disclose confidential information for risk stratification
- Implications for GPs, CCGs, CSUs and independent sector data services providers

Introduction

Risk stratification can either be conducted using identifiable patient data or pseudonymised data. A legal basis is required for the processing of identifiable patient data for risk stratification or any other purpose. Where pseudonymised data are used, then a legal basis is not required. The use of pseudonymised data is discussed further below, but the first part of this annex concerns the use of identifiable data.

Lawful processing

All processing of personal data must, as a minimum, satisfy the Data Protection Act 1998. Public bodies (and, via contract, their providers) also need to comply with the Human Rights Act 1998. Furthermore, where information is confidential, it is additionally protected through the common law duty of confidence or, in some specific instances, through statute. See Box 3

Box 3: Legal framework for the NHS to process personal confidential information

The overarching legal framework for the NHS to process personal confidential information is comprised of:

(a) the Data Protection Act
(b) the Human Rights Act
(c) the common law duty of confidence
(d) certain specific statutory provisions that require, permit, or prohibit the use of personal data and confidential information

Finally, the Health and Social Care Act 2012 introduced statutory obligations of confidence on the HSCIC by prohibiting the publication of personal data relating to individual patients, and by specifying the circumstances in which it could disclose different types of information.

Data Protection Act 1998
In order to comply with the Data Protection Act 1998, organisations need to meet the eight *data protection principles* (unless an exemption applies). The first principle requires that:

(a) personal data are processed fairly and lawfully;
(b) one of the conditions in Schedule 2 are met; and
(c) where the data are "sensitive personal data", one of the conditions in Schedule 3 are met

In order to meet the first arm of the first principle, organisations must meet all other legal requirements, such as the common law duty of confidence. The first principle therefore brings together all of the legal requirements for lawful processing. As a result, a breach of these other legal requirements would, automatically, also be a breach of the first principle.

In relation to the other two arms of the first principle, the data for risk stratification include health information; therefore, they constitute "sensitive personal data" and so any risk stratification activities must meet at least one condition in both Schedule 2 and Schedule 3. See Box 4

Box 4: Conditions for Schedule 2 and Schedule 3 of the Data Protection Act

While more than one condition may be met under each of Schedules 2 and 3, the most secure conditions for risk stratification appear in paragraph 5(d) of Schedule 2 and in paragraph 8 of Schedule 3, namely:

Schedule 2
The processing is necessary for the exercise of any other functions of a public nature exercised in the public interest by any person.

Schedule 3
The processing is necessary for preventive medicine, and the management of healthcare services and is undertaken by a person who in the circumstances owes a duty of confidentiality which is equivalent to that which would arise if that person were a health professional.

Note: "Medical purposes" only applies to health data, so Schedule 3 paragraph 8 cannot be used in relation to social care data. The only applicable option in this case is explicit consent.

These schedules clarify that in relation to data protection requirements, the consent of the individual is not required. However, consent may still be required to satisfy other legal obligations, such as the duties of confidence.

In relation to the second data protection principle, risk stratification is classified as indirect care; therefore, it falls within the category of *further processing.*[aa] However, as we saw under paragraph 3 of Schedule 3, risk stratification is a medical purpose and would therefore be regarded as a *compatible purpose*.

With regard to the other data protection principles, the following requirements are important for risk stratification:

- The data used for risk stratification should adequate, relevant, but not excessive.
- Likewise, the information derived from the risk stratification tool and given to GPs should be adequate, relevant, but not excessive (given that the data used for risk stratification are usually much broader than the data held by the GP).
- Checks are needed to verify the accuracy of the data and to ensure they are up to date
- The data must 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 period required for the risk stratification tool
- Patients must be informed that their personal data will be used for risk stratification purposes
- If a patient does not want their data to be used for risk stratification, their wishes should 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
- There must be appropriate organisational and technical measures to protect the data
- The data must not be processed outside the European Economic Area unless there are equivalent legal, technical, and organisational measures in place to protect the data appropriately.

Common law duty of confidence

The common law duty of confidence applies where information is identifiable and has either

a) been imparted in circumstances where there was an expectation that the information would be treated in confidence; or
b) where the nature of information was obviously sensitive and, therefore, had the "necessary quality of confidence".

[aa] The Second Data Protection principle requires that "Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes". Where data have been collected and used for a set of purposes, any subsequent additional processing can only be for compatible purposes or a new legal basis must be obtained (e.g. by writing to the data subjects to tell them of the new purpose and therefore having a basis on which to imply consent).

A legal basis is needed to use or disclose confidential information. The legal bases available under the common law are (1) statute; (2) court order; (3); consent of the individual; or exceptionally (4) public interest grounds.

As risk stratification involves the routine use of confidential information, it cannot generally rely on public interest grounds. Nor would a court order would be applicable; therefore, it leaves either statutory provision or consent as the two legal bases. At present, there is no statutory support for risk stratification in England, which means that where identifiable data are needed, consent is the only available option. However, there are good reasons why seeking consent for risk stratification is not appropriate (e.g., the most vulnerable members of society tend to be the least likely to respond to a request for consent).

In practice, risk stratification should be conducted using either pseudonymised data or using technologies that allow the data to be processed automatically and without being seen by a human.

Why can consent not be implied?

Ordinarily, patients give consent for the use of their identifiable data for their direct care as part of their consent for examination and treatment. In the context of risk stratification, however,

(a) not all individuals will be offered further services as a result of their data being processed for this purpose; and

(b) risk stratification is not necessarily a use of their information that people would expect.

For both of these reasons, it is not reasonable to imply that patients have consented to the use of their data for risk stratification. Therefore, the tests for legally valid consent would not be met.

Human Rights Act 1998

The Human Rights Act 1998 incorporates most of the provisions of the European Convention on Human Rights into UK law. Data Protection requirements are derived from Article 8 of the Convention, which grants individuals a right to have their privacy respected. Article 8, also supports the common law duty of confidence.

The Human Rights Act applies to public bodies and, through contractual arrangements, to their providers. In relation to the right to privacy, public bodies can only interfere with an individual's privacy where it is lawful and is necessary for one several specified purposes, including the protection of health and protection of the rights and freedoms of others.

Risk stratification has a role in protecting the health of individuals. Therefore, risk stratification is a permitted interference with an individual's privacy under the Human Rights Act – provided that the interference was in accordance with the law, was necessary, and was proportionate.

The requirements of the Human Rights Act are similar to the requirements under the Data Protection Act to minimise the use of personal data to circumstances where the use is lawful, necessary, involves using only relevant data, and involves keeping personal data only for the minimum period necessary.

Overall Legal Framework

So far in this annex, we have considered the means by which risk stratification can be conducted lawfully under the different component parts of the legal framework (viz., the Data Protection Act, the Human Rights Act, and the common law duty of confidence). These individual elements, however, need to be brought together to arrive at an overall position for determining how identifiable data can be used lawfully for risk stratification purposes in England.

It is clear that under the Data Protection Act, risk stratification can be conducted lawfully without consent. Likewise, under Human Rights legislation, an individual's privacy can be interfered with for risk stratification purposes, provided the use of the data is lawful, necessary, and proportionate. However, the common law duty of confidence requires either consent, or the use of pseudonymised or de-identified data for the analysis (with access to identifiable data being limited to clinicians who are involved in the care of the patient).

While the common law may be overridden by statute, this override only applies to the particular circumstances set out in the relevant legislation and does not apply here. The requirements of the common law therefore set the standard. Furthermore, because the processing needs to be lawful (i.e. it must comply with the common law), so the Data Protection Act and Human Rights Act both reconfirm the duty of confidence.

The overall legal framework for risk stratification requires either that consent is obtained or that pseudonymised or de-identified data are used.

Health and Social Care Act 2012

Under the Health and Social Care Act 2012, the Health and Social Care Information Centre (HSCIC) was empowered to collect and process confidential patient informationbb where directedcc to collect the data by the Secretary of State for Health or by NHS England;dd or where requested to do so by other bodies.ee These provision means that the common law duty of confidence no longer applies to the HSCIC – but only as prescribed in the Act.

The HSCIC has a legal basis under the Act and its supporting regulations to continue to obtain and process data falling within the defined data sets that were collected prior to 31 March 2013.ff To collect data that were not previously collected, however, the HSCIC needs to be directed or requested to do so. NHS England will be directing the HSCIC to collect GP data and any other required data not already in its possession, to support risk stratification. The Directions will need to take account of the fact that not all GPs are taking up the DES for risk stratification, so this collection will need to be a service offered to GPs rather than a mandatory collection of data from GPs.

In relation to disclosures of data from the HSCIC, the Act sets out specific conditions for both the publication[gg] and the dissemination of information.[hh] The Act therefore imposes a *statutory obligation of confidence* on the HSCIC and it sets the parameters for the HSCIC to make decisions about disclosures. Note, however, that in some circumstances, the common law duty of confidence continues to apply,[ii] and that these provisions only apply to the HSCIC. Additionally, where the intention is for identifiable data to be disclosed by the HSCIC to another body, the disclosure needs to meet the criteria set out under Sections 261 and 262 of the Health and Social Care Act 2012. See Box 5

Box 5: Lawful Disclosure of data by the HSCIC

For risk stratification, the most appropriate route for disclosure of data from the HSCIC is under Section 261(5)(d) where the disclosure is made to the GP for the exercise of their functions conferred under their obligations to provide medical services under Part 4 of the NHS Act 2006.

NHS England is in the process of drafting directions for the HSCIC to support risk stratification.

[bb] Under Sections 256 and 259
[cc] Section 254
[dd] NHS England is the operating name for the NHS Commissioning Board as defined in the Act.
[ee] Section 255
[ff] The Health and Social Care Act (Commencement No. 4, Transitional, savings and Transitory provisions) Order 2013 http://www.legislation.gov.uk/uksi/2013/160/article/9/made
[gg] Section 260
[hh] Section 261 and 262
[ii] Section 261 (5)(c)-(e)

Implications for GPs

As data controllers of the data that they hold, GPs could commission risk stratification to be conducted on their behalf; however, they would need a legal basis to obtain identifiable secondary care data for use in a risk stratification tool. **There would be no breach of confidence provided that another body, acting as a data processor under contract, undertook the processing using pseudonymised data.**

Once the population has been stratified using the predictive model, high-risk individuals can then be re-identified so that their GP can offer them additional, preventive services. At this point the data will be used for direct care and so it is reasonable to imply consent. To support the validity of the consent, however, there is a need to ensure that individuals are informed about how their information is used.

Implications for CCGs

CCGs do not have a statutory basis to process identifiable data for risk stratification purposes. However, the GP practices that form the CCG could decide to act collectively to commission or undertake risk stratification on their behalf. Where the CCG commissions a risk stratification service, then the data processing contract would be between all the GPs (as data controllers) and the data processor undertaking the work. The data processor would need to use pseudonymised or de-identified data. Once the data had been risk stratified, the target population of high-risk individuals would need to be provided to their respective practices for referral for additional support.

Where the CCG is unaligned to a CSU and is conducting risk stratification on behalf of its member GP practices, it will act as a data processor on behalf of the respective GP practices, and would need to do so under contract to them.

Implications for CSUs

CSUs are part of NHS England and may be asked to provide data processing services to GPs or CCGs. Because NHS England will be directing the HSCIC to provide data for the purposes of risk stratification, disclosures to CSUs are still classified as dissemination under the Health and Social Care Act 2012, and therefore there is still a need to comply with the provisions of the Act and the relevant Directions for any disclosures to CSUs. As NHS England will be directing the HSCIC in this regard, and therefore to some degree controlling the purpose for which the data are to be processed, the data controller responsibilities may be shared between NHS England and the GPs. As a result, data controllership is also likely to apply to the CSU.

As the current Section 251 support does not include risk stratification purposes, CSUs will need to use pseudonymised data for risk stratification purposes and maintain these data separately from any identifiable data they holds or will need to use closed systems technologies (Option A). This separation is necessary to prevent any risk of re-identification of the data being used for risk stratification. As CSUs become ASHs, they will be able to receive weakly pseudonymised data (or de-identified data for limited

access[jj]) containing the NHS number as the sole identifier, unless they are already able to use pseudonymised data, in which case such data should be used in preference to more identifiable datakk.

Implications for independent sector data services providers

Independent sector data services providers (IDSPs) can process pseudonymised or de-identified data on behalf of the commissioning GP practice. They can also process identifiable data, provided that the GP practice, as the data controller, has a lawful basis to obtain and disclose the confidential data (e.g., by using closed system technologies, or with the consent of the individuals). In these circumstances, the IDSP must take appropriate steps to protect the data. For example, they should use technologies and access controls that ensure that the data can be processed automatically and can only be viewed by clinicians who are responsible for providing care to the relevant individuals.

For risk stratification purposes, IDSPs will be acting as a data processor; therefore, the information governance requirements must be included within their contracts. Note that ISDSPs will not be Accredited Safe Havens, at least in the first instance.

[jj] As defined by the Caldicott Review – see Annex 4
[kk] In line with the data minimisation principle underpinning Data Protection requirements

Annex 3 - FAQs

1. Why might identifiable data be needed for risk stratification?

Data containing identifiers such as the NHS number may be needed to enable data from different sources to be linked together. Additionally, some risk stratification tools have been designed to use identifiable data, and it is not always straightforward for these tools to be adapted so that they can use pseudonymised data. However, suppliers should now consider how they can adapt their systems to use pseudonymised data.

2. Will the Section 251 approval recently obtained by NHS England allow CSUs and CCGs to perform risk stratification using identifiable data?

No, the Section 251 approval does not permit CCGs, CSUs or GPs to perform risk stratification on confidential patient information; however, any confidential patient information legitimately held for another purpose may be used in pseudonymised form for this purpose.

Up until the end of March 2013, support was in place under the Section 251 regulations to enable providers to disclose data to the Information Centre for Health and Social Carell and onwards to PCTs for the purposes of commissioning. NHS England has obtained a temporary extension of this support until 4 July 2013 as a transitional measure to provide a legal basis for NHS England's CSUs (and a limited number of specified CCGs doing in-house processing) to continue to process confidential patient information for the commissioning purposes specified in the application. These purposes did not include risk stratification because alternatives are available to the processing of confidential patient information for this purpose (i.e., processing using pseudonymised data). Section 251 powers can only be used where neither consent nor using de-identified data is practicable.

On 19 May 2013, NHS England received further partial and conditional support under the Section 251 regulations for commissioning organisations to work towards becoming Accredited Safe Havens (ASHs).mm.The criteria and process for organisations to become ASHs are currently being developed by NHS England in collaboration with the HSCIC and the Department of Health. ASHs will have robust information governance controls, including contractual obligations and audit measures, to prevent patients' data from being re-identified. They will be permitted to process data that have been de-identified but are at high risk of re-identification (e.g., data containing NHS numbers as the sole identifier). NHS England will issue further details about ASH requirements shortly.

[ll] Which was replaced on 1 April 2013 by the Health and Social Care Information Centre (HSCIC)
[mm] Details of the approval can be found at http://www.hscic.gov.uk/dataflowstransitionmanual

3. Are CCGs different from PCTs in terms of risk stratification?

Under the Health and Social Care Act 2012, CCGs were not given a statutory basis to access confidential patient information. This situation contrasts with PCTs, which did have limited powers to access confidential patient information. For example, PCTs could access such data in order to manage primary care contracts, where anonymised or pseudonymised data could not be used. This responsibility for managing primary care contracts has now moved to NHS England.nn

In relation to risk prediction, PCTs were not empowered to use confidential patient information for risk stratification; however, they could use confidential patient information that they held legitimately for other purposes, in pseudonymised form, for risk prediction. Therefore, in this regard, CCGs are not in the same position as PCTs.

4. Why can't the HSCIC do all of the processing for risk stratification?

The situation depends on the risk stratification tool that the GP practices or the CCG wish to use. Open-source tools, and proprietary tools made available under licence, could potentially be implemented within the HSCIC. Under this arrangement, all of the identifiable data would be processed within the HSCIC.oo However, the HSCIC currently has limited capacity to support all of the various demands placed upon it to process data. Additionally, organisations may have a preference for particular tools provided by third parties, who may be unwilling to allow their proprietary software to be installed on HSCIC servers. Some HSIC regional offices (formerly known as DMICs) may have capability to perform risk stratification on behalf of their local CSUs – please contact your CSU to discuss potential arrangements if you would like to use this option.

Use of the GP Extraction Service (GPES) to support risk stratification would need to be considered by the HSCIC's GPES Independent Advisory Group (IAG). Consideration would need to be given as to which dissent codes to use for recording objections to the use of GP data for risk stratification purposes.

5. Why is an ethical review recommended?

Risk stratification is analogous to screening because it uses a population's data to identify individuals that are at sufficiently high risk of a *Triple Fail* event[pp] (such as an unplanned hospital admission) to justify offering a preventive intervention (such as the support of a community matron). Any screening test has the potential to cause more harm than good; for example, by exposing patients to false positive and false negative results.

For these reasons, strict ethical guidelines are required to safeguard against the inappropriate use of risk stratification. In 1968, The World Health Organization published ten prerequisites that should be met by any ethical screening program.

[nn] The Confidentiality and Disclosure of Information (General Medical Services, Personal Medical Services and Alternative Provider Medical Services) Directions 2013

[oo] Under Directions from NHS England

[pp] A 'Triple Fail' event is simultaneously costly, represents a suboptimal health outcome, and is a poor patient experience (Lewis et al., 2013).

Known as the Wilson and Jungner criteria, they have recently been adapted for risk stratification purposes (see Box 6).

Box 6: Ethical criteria for risk stratification programmes

1. The Triple Fail event should be an important health problem.
2. There should be an intervention that can mitigate the risk of the Triple Fail event.
3. There should be resources and systems available for timely risk stratification and preventive interventions.
4. There should sufficient time for intervention between stratification and the occurrence of the Triple Fail event.
5. There should be a sufficiently accurate predictive risk model for the Triple Fail event.
6. The predictive risk model and impactibility model should be acceptable to the population.
7. The natural history of the Triple Fail event (i.e., the practices and processes that typically lead to the event) should be adequately understood by the organisation offering the preventive intervention.
8. There should be an accepted policy about who should be offered the preventive intervention.
9. The cost of risk stratification should be “economically balanced” (i.e., it should not be excessive in relation to the cost of the programme as a whole).
10. Risk stratification should be a continuous process, not just a "once and for all" occurrence.

Source: Lewis et al., 2013, based on Wilson & Jungner, 196816

6. How can we quality-assure the risk stratification and referral process?

The CCG, GP practice or CSU should collect and analyse pseudonymised data on the accuracy of the risk stratification tool and on the effectiveness of the preventive interventions offered to patients. The selection criteria for the preventive interventions should be adapted according to the responses of different types of patient to the different interventions offered.

7. What contractual arrangements are needed?

The consortium of GP practices that constitute a CCG can decide that the CCG will act on behalf of all the GP practices in relation to contracting particular services. However, as data controllers, all the GP practices will need to be parties to the contract. Alternatively, the practices may decide to ask one GP practice to be the lead, again acting on behalf of the other practices. Such decisions need to be documented in the CCG’s board minutes and detailed in a formal agreement between all the parties. These steps are required to ensure that there is clarity about roles and responsibilities, including the legal accountabilities and liabilities.

GP practices remain the data controllers for their data and if they gain access to SUS, HES,[qq] or other secondary care provider data in identifiable form, then they become data controllers for these data as well, unless the provider is also a commissioner of the risk stratification service.

If the data analysis is being conducted by a health service body (e.g., by the HSCIC or NHS England), then an NHS contract[rr] needs to be signed. Where an independent sector provider is used, a legally-binding contract must be signed, even where the data received by the independent sector provider are pseudonymised. A contract is needed to prevent the:

- use of the data for non-agreed purposes;
- re-identification of individuals; and
- onward disclosure of the data to others.

Contractual arrangements need to be monitored on an on-going basis. For example, arrangements for periodic audits need to be place.

8. Why do we need to inform patients that their data are being risk stratified?

Where identifiable and weakly pseudonymised data are being used, these data are personal data. Under the Data Protection Act, all organisations processing personal data are obliged to provide fair processing information to individuals about how their information is to be used. GPs and other providers are therefore under a general obligation to inform patients about how their personal information is to be used, and information about risk stratification should be included within this information.

9. How should GP practices inform their patients about risk stratification?

GP practices must ensure that they have met their fair processing obligations by including risk stratification within their privacy notices and must take reasonable steps to ensure that all patients in their practice have had access to this information using a range of channels (see Box 7).

Box 7: Communicating with patients

GP practices should provide information to patients explaining how their data will be used and what to do if they have any concerns or objections.

This information should be provided by means of:

- posters and leaflets available within the surgery;
- actively providing information at the time of registration and other points of written communication;
- dissemination via local patient groups; and
- inclusion of the information on the practice website.

[qq] Hospital Episode Statistics
[rr] Defined under Section 9 of the NHS Act 2006

Note: where automatic decision-taking is being undertaken on the basis of risk stratification without review by a clinician (see FAQ number 11), specific notification to individuals about risk stratification must also be issued.

10. What if a patient objects to the use of their information?

If consent is the legal basis for processing confidential patient information, then the individual patient has a right to refuse to give their consent (or to give and later withdraw it), and their wishes must be respected.

If the legal basis of processing is that pseudonymised data are to be used, with only the HSCIC having access to confidential patient information, then the HSCIC has the legal authority to process confidential information under the Health and Social Care Act 2012,ss as defined by the Act. However, the Secretary of State for Health has given a commitment that in relation to disclosures of GP data to the HSCIC, patient objections will be respected other than in exceptional circumstances, such as where there is an overriding public interest justification for doing so. In light of this commitment, patient objections in relation to the flow of identifiable data to the HSCIC must therefore be respected, including for risk stratification purposes.

11. What is automatic decision-taking, and what additional safeguards apply?

If a risk prediction algorithm is to be applied to a patient's data and the risk score generated is then to be used as the sole basis of decision-taking, then this procedure would be classified as "automated decision-taking". In circumstances where (a) a pre-determined percentage of patients with the highest risk scores, or (b) patients with a risk score above a defined risk threshold are automatically referred to an intervention (such as the support of a community matron), then these arrangements would constitute automated decision-taking.

Automated decision-taking is likely to have a significant impact on an individual, for example by determining whether additional preventive services are to be offered, such as the support of a community matron. In these circumstances, the requirements of Section 12 of the Data Protection Act apply, and a specific notification should be issued so that patients are given the opportunity to object to the use of their data for automated decision-taking and to ask for human review.

Typically, however, there will be a process of human review of the outputs of risk stratification (i.e. review by a clinician). Here, risk stratification will be used as an aid to clinical decision-making rather than as a substitute for it. Where such clinical review is undertaken, the specific obligation to notify individuals about automated decision-taking does not apply; however, the general obligation to inform patients about risk stratification remains.

[ss] Section 259 http://www.legislation.gov.uk/ukpga/2012/7/section/259

What kind of clinical review is needed?

In the case of risk stratification for case finding, once the data have been analysed, the risk scores (and sometimes relevant additional data) are communicated to the GP and other relevant members of the care team. The care team may include regulated social workers but only if social care data have been used in the risk prediction tool.

Unless the organisation has elected to use automated decision-taking, a process of clinical review is needed. Clinical review involves the following steps:

First, a GP should review the records of those patients identified as having a borderline high risk score, or where the risk score seems anomalous, to determine whether it is appropriate to offer them additional support.

Second, the GP or another clinician with a legitimate relationship with the patient will need to contact those individuals they have verified as being at high risk to offer them appropriate preventive interventions. As with any other form of referral for care or treatment, the patient's consent is needed. This consent may be implied, provided that the individual:

- has been given sufficient information about the preventive intervention;
- has the capacity to understand what they are agreeing to; and
- understands and gives their consent voluntarily.

Where an adult individual lacks capacity to understand what is being offered to them, clinicians can act on best interest grounds rather than on the grounds of consent. As with any other form of care, clinicians should keep the use of preventive interventions under review to ensure that the care remains appropriate for the individual.

What re-identified information should be provided to the GP?

Clinicians should only be given access to the risk score and information to which they would normally have access through their legitimate relationship with the patient. Additional information generated through the linkage of data from multiple sources may only be disclosed with the consent of the individual because otherwise this would be a breach of confidentiality.

Consent to share additional information may be implied in circumstances where:

- individuals have been informed of the proposed use and disclosure of their confidential information;
- they understand that they have the right to withhold their consent; and
- they have been given a reasonable period of time in which to withhold their consent.

Only relevant data should be shared (i.e., the data must not be excessive) and patients must understand what types of information are to be shared. A defined data set must be agreed in advance and highly sensitive information should be excluded without the explicit agreement of the individuals concerned. Highly sensitive information includes codes related to sexually transmitted infections, terminations of pregnancy, abuse, or the fact that an individual has been imprisoned. In addition, there are specific legal restrictions for protected information such as that relating to IVF treatment and other assisted reproductive technologies; and gender identity disorders and previous gender identity. Additionally, particular care must be taken when sharing information between health and social care services as this sharing of data can only be undertaken with explicit patient consent to meet one of the conditions in Schedule 3 of the DPA.
GPs may wish to ask patients for permission to share any additional data during the clinical review and referral stages, to assure themselves that patients agree to this use of their information. Such checks are particularly pertinent with individuals who have previously expressed objections to the sharing of their data.

Annex 4 - Glossary

The definitions listed here are drawn either directly from, or are derived from, the Data Protection Act 1998, the NHS Constitution 2013, the Information Commissioner's Anonymisation Code of Practice, or the Caldicott Information Governance Review.

Term	Source	Definition
Accredited Safe Haven	Caldicott Review	An accredited organisation with a secure electronic environment in which personal confidential data and/or weakly pseudonymised data can be obtained and made available to users, generally in de-identified form. An accredited safe haven will need a secure legal basis to hold and process personal confidential data. Weakly pseudonymised data can be held under contract with obligations to safeguard the data.
Anonymised Data	ICO Anonymisation Code of Practice	Data in a form that does not identify individuals and where identification through its combination with other data is not likely to take place.
Automated decision-taking	Section 12 of the DPA	Decisions which significantly affect the individual based solely on the processing by automatic means of personal data in respect of which that individual is the data subject for the purpose of evaluating matters relating to him.
Confidential patient information	Section 251 of the NHS Act 2006	Confidential patient information is patient information where the identity of the individual in question is ascertainable from that information, or from that information and other information which is in the possession of, or is likely to come into the possession of, the person processing that information, and that information was obtained or generated by a person who, in the circumstances, owed an obligation of confidence to that individual.
Compatible purpose	Schedule 1 of the DPA ICO Data Protection Guide Principle 2	The Act clarifies to some extent what is meant by compatibility: it says that when deciding whether disclosing personal data is compatible with the purpose for which you obtained it, you should bear in mind the purposes for which the information is intended to be used by any person to whom it is disclosed. An additional or different purpose may still be

		compatible with the original one. Because it can be difficult to distinguish clearly between purposes that are compatible and those that are not, we focus on whether the intended use of the information complies with the Act's fair processing requirements. It would seem odd to conclude that processing personal data breached the Act on the basis of incompatibility if the organisation was using the information fairly. If you wish to use or disclose personal data for a purpose that was not contemplated at the time of collection (and therefore not specified in a privacy notice), you have to consider whether this will be fair. If using or disclosing the information would be unfair because it would be outside what the individual concerned would reasonably expect, or would have an unjustified adverse effect on them, then you should regard the use or disclosure as incompatible with the purpose you obtained the information for.
Data controller	Section 1 of the DPA	A person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed;
Data processor	Section 1 of the DPA	any person (other than an employee of the data controller) who processes the data on behalf of the data controller;
De-identified data	Caldicott Review derived from ICO Anonymisation Code of Practice	De-identified data: This refers to personal confidential data, which has been through anonymisation in a manner conforming to the ICO Anonymisation code of practice. There are two categories of de-identified data: • ***De-identified data for limited access:*** this is deemed to have a high risk of re-identification if published, but a low risk if held in an accredited safe haven and subject to contractual protection to prevent re-identification. • ***Anonymised data for publication:*** this is deemed to have a low risk of re-identification, enabling publication.

Direct Identifier	ISB Anonymisation for publishing health and social care data ISB 1523 Amd 20/2010 2/2013	Name, address, widely-used unique person or record identifier (notably National Insurance Number, NHS Number, Hospital Number), telephone number, email address, and any other data item that on its own could uniquely identify the individual.
Fair processing	Part 2 Schedule 1 of the DPA	Processing personal data in accordance with the rights of the data subject including, in general, ensuring the individual has been informed about how their personal information is to be used.
Further processing	Schedule 1 of the DPA	Additional use of the data beyond its original intended purpose - See Compatible purpose
Human Review	Section 12 of the DPA	In relation to automated decision-taking, where an individual disagrees with the decision or objects to automated decision-taking, organisations have an obligation to provide review by a person who would take the decision based on the information available.
Identifiable data	ICO Technical guidance	Data in which the identity of individuals can be derived from the data
Indirect care	Caldicott Review	Activities that contribute to the overall provision of services to a population as a whole or a group of patients with a particular condition, but which fall outside the scope of direct care. It covers health services management, preventative medicine, and medical research. Examples of activities would be risk prediction and stratification, service evaluation, needs assessment, financial audit.
Indirect Identifier	ISB Anonymisation for publishing health and social care data ISB 1523 Amd 20/2010 2/2013	A data item (including postal code, gender, date of birth, event date or a derivative of one of these items) that when used in combination with other items could reveal the identity of a person. Also referred to as “quasi-identifier”.
Integrated Care Programmes		Integrated care programmes are local programmes of work that have been agreed by a range of stakeholders to integrate health and social care provision for people with significant or complex health and social care needs. Typically, part of the agreement is to establish

		an integrated care record, which is used alongside the respective health and social care records. The integrated care record contains information that is relevant for all of the professionals caring for the individual patient to access. The creation and contents of the record should be agreed with the individual patient.
Objection	NHS Constitution, Caldicott Review, & SoS commitment at launch of Caldicott Review Report	All processing of personal confidential data requires a legal basis. Where the legal basis for processing is based in statute or on overriding public interest ground then individuals have a right to object to how their information is used and to have their wishes respected unless there is a good reason and to be informed of that reason. This is distinct from where consent is the legal basis for processing and individuals can give or refuse their consent.
Patient information	S251 of the NHS Act 2006	Patient information is information (however recorded) which relates to the physical or mental health or condition of an individual, to the diagnosis of his condition or to his care or treatment, and information (however recorded) which is to any extent derived, directly or indirectly, from such information, whether or not the identity of the individual in question is ascertainable from the information.
Personal confidential data	Caldicott Review	This term describes personal information about identified or identifiable individuals, which should be kept private or secret. For the purposes of this review 'Personal' includes the DPA definition of personal data, but it is adapted to include dead as well as living people and 'confidential' includes both information 'given in confidence' and 'that which is owed a duty of confidence' and is adapted to include 'sensitive' as defined in the Data Protection Act.
Personal data	Section 1 of the DPA	Data which relate to a living individual who can be identified from those data, or from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

Processing	Section 1 of the DPA	Processing in relation to information or data, means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including: • organisation, adaptation or alteration of the information or data; • retrieval, consultation or use of the information or data; • disclosure of the information or data by transmission, dissemination or otherwise making available; or • alignment, combination, blocking, erasure or destruction of the information or data.
Pseudonymisation	ISB Anonymisation for publishing health and social care data ISB 1523 Amd 20/2010 2/2013	A technique that replaces identifiers with a pseudonym11 In practice, pseudonymisation is typically combined with other anonymisation techniques.
Pseudonymised data	Caldicott Review	Pseudonymised data are data in which individuals are distinguished "by using a unique identifier, which does not reveal their 'real world' identity" (i.e., a pseudonym).[12] Data that have been adequately pseudonymised equate to anonymised data in the hands of a recipient; however, they usually can be re-identified by the original holder of the data.
Re-identification	ICO Anonymisation Code of Practice	The process of analysing data or combining it with other data with the result that individuals become identifiable. Sometimes termed 'de-anonymisation'.
Sensitive personal data	Section 2 of the DPA	Data that identifies a living individual consisting of information as to his or her: racial or ethnic origin, political opinions, religious beliefs or other beliefs of a similar nature, membership of a trade union, physical or mental health or condition, sexual life, convictions, legal proceedings against the individual or allegations of offences committed by the individual.
Weakly psedudonymised data	Caldicott Review	Equates to "De-identified data for limited access"
Urgent Care	The Urgent Care	Clinical Dashboards are **a tool designed by**

Dashboards	Clinical Dashboard Implementation Guide	**clinicians, for clinicians** and help to provide clinical teams with relevant, informative and timely information to support clinical decisions that improve the quality and safety of patient care. The Urgent Care Clinical Dashboard helps GPs and other practice-affiliated clinicians to identify the most vulnerable, at risk patients and empowers clinicians by bringing information together in real time. The information provided through the dashboard supports clinicians to improve and to manage and co-ordinate the healthcare of patients more proactively, especially for the most vulnerable and those with long term conditions.

References

[1] Academy Health. “2008 HSR Impact Awardee: Improving the Financing and Delivery of Health Care with Risk-Based Predictive Modeling”. Washington, DC: AcademyHealth, 2008.

[2] Georghiou T, Steventon A, Billings J, Blunt I, Lewis G, Bardsley M. Predictive risk and health care: an overview. London: Nuffield Trust, 2011.

[3] Lewis G, Kirkham H, Duncan I, Vaithianathan R. How health systems could avert 'Triple Fail' events that are harmful, are costly, and result in poor patient satisfaction. Health Affairs (Millwood). 2013;32(4):669-76

[4] Curry N, Billings J, Darin B, Dixon J, Williams M, Wennberg D. Predictive Risk Project Literature Review. London: The King’s Fund, 2005.

[5] Allaudeen N, Schnipper JL, Orav EJ, Wachter RM and Vidyarthi AR. Inability of providers to predict unplanned readmissions. J Gen Intern Med 2011;7(26):771–776.

[6] Weiner, J.P. et al. Development and application of a population-oriented measure of ambulatory care case mix. Medical Care 1991;29(5):453-472.

[7] Billings J, Dixon J, Mijanovich T and Wennberg D. Case finding for patients at risk of readmission to hospital: development of algorithm to identify high risk patients. BMJ 2006;333: 327.

[8] Billings J, Blunt I, Steventon A, Georghiou T, Lewis G, Bardsley M. Development of a predictive model to identify inpatients at risk of re-admission within 30 days of discharge (PARR-30)

[9] Wennberg D and others. Combined Predictive Model: Final report and technical documentation. London: The King’s Fund, 2006.

[10] Bardsley M, Billings J, Dixon J, Georghiou T, Lewis GH and Steventon A. Predicting who will use intensive social care: case finding tools based on linked health and social care data. Age Ageing 2011;40(2):265–270.

[11] Victoria CG, Vaughan JP, Barros FC, Silva AC, Tomasi E. Explaining Trends in inequalities from Brazilian child health studies. Lancet 2000: 356: 1093

[12] Caldicott F and others. *Information: To share or not to share* The Information Governance Review. London: Department of Health, 2013.

[13] The use of patient information in the Long Term Conditions Programme, London: Department of Health and Patient Information Advisory Group, December 2006

http://webarchive.nationalarchives.gov.uk/20070305111133/http://advisorybodies.doh.gov.uk/piag/piag-ltc-nov2006.pdf

[14] Advice on Risk Prediction and Stratification, London: National Information Governance Board for Health and Social Care, July 2012 http://www.nigb.nhs.uk/pubs/guidance/riskpred.pdf

[15] Lewis G, Curry C, Bardsley M. Choosing a predictive risk model: a guide for commissioners in England. London: Nuffield Trust, 2011.

[16] Wilson J, Jungner G. Principles and practice of screening. Geneva:World Health Organization; 1968.