Department of Health

Department for Communities and Local Government

Local Government Association

NHS England

Better Care Fund Task Force

‘How to’ Guide: The BCF Technical Toolkit

Section 1:
Population Segmentation, Risk Stratification
and Information Governance

August 2014

The Better Care Fund

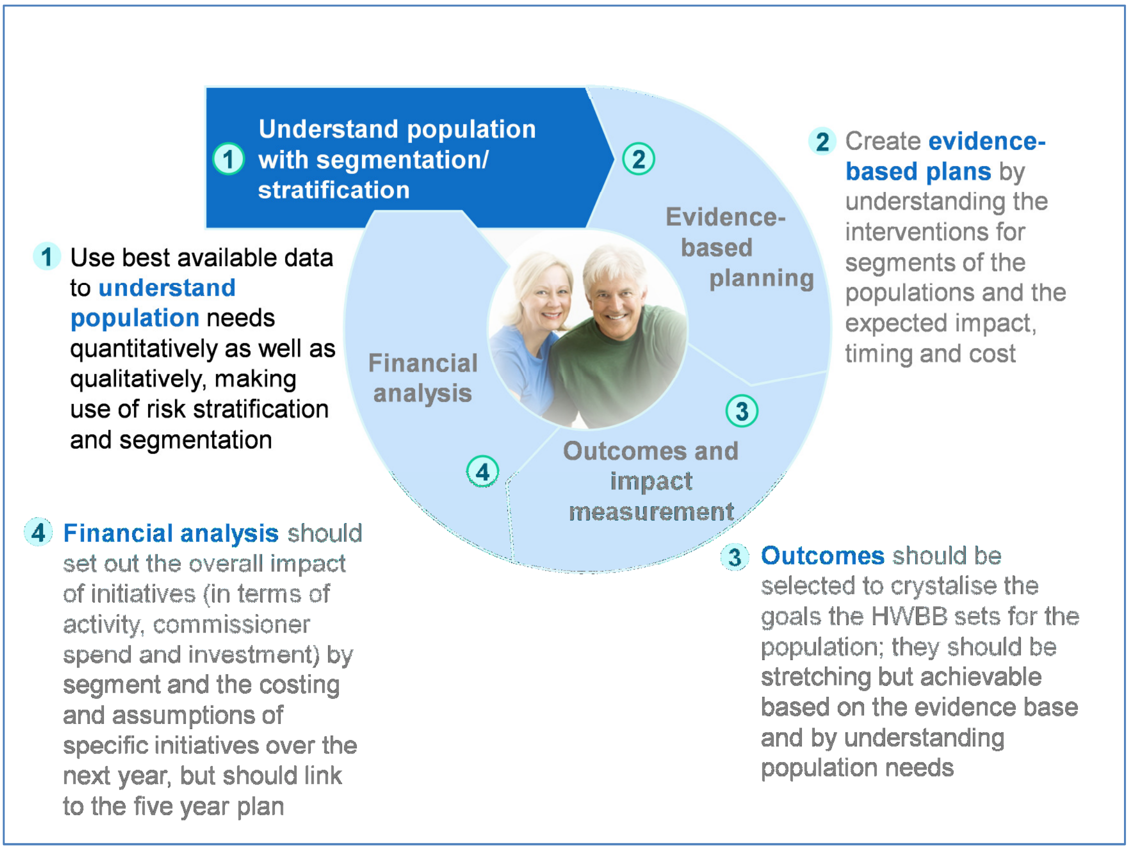
Contents

BACKGROUND

This document provides an explanation of population segmentation, risk stratification and information governance (IG). Also included in the following sections are practical hints and tips that will support the preparation of BCF plans as they pertain to population segmentation and risk stratification. This document is meant to be used in conjunction with the other documents that make-up the “how to guide.” Please refer to the document entitled “Introduction to the How To Guide” to understand how to best use this guide.

It is worth highlighting that an approach to population segmentation, risk stratification and IG issues are a vital component in robust, well-developed BCF planning. The other sections of this toolkit – such as evidence-based planning, outcome and impact measurement and financial analysis – build on population segmentation and risk segmentation theory explaining in this section.

Figure 1. Four steps for robust planning


1 Understand population with segmentation/ stratification
2
Evidence-based planning
3
Outcomes and impact measurement
4
Financial analysis

1 Use best available data to **understand population** needs quantitatively as well as qualitatively, making use of risk stratification and segmentation

2 Create **evidence-based plans** by understanding the interventions for segments of the populations and the expected impact, timing and cost

3 **Outcomes** should be selected to crystalise the goals the HWBB sets for the population; they should be stretching but achievable based on the evidence base and by understanding population needs

4 **Financial analysis** should set out the overall impact of initiatives (in terms of activity, commissioner spend and investment) by segment and the costing and assumptions of specific initiatives over the next year, but should link to the five year plan

POPULATION SEGMENTATION, RISK STRATIFICATION AND INFORMATION GOVERNANCE

What are these?

Population segmentation and risk stratification are two concepts used to help understand the needs of the population so that services can be better planned and delivered. Segmentation is grouping the local population by what kind of care they need as well as how often they might need it. Risk stratification means understanding who, within each segment, has the greatest risk of needing intense care such as a hospital admission.

Both population segmentation and risk stratification can be performed with patient de-identified data as well as patient-identifiable data. De-identified data can be used to make commissioning plans while patient-identifiable data is essential for direct patient contact by providers and in both cases is protected by robust information governance.

It is vital that population grouping exercises are compliant with information governance requirements. Please see **Appendix 1a** for a thorough discussion of **information governance requirements** as they pertain to risk stratification. This section includes detailed examples related to the BCF template.

Why are they important?

The current health and care system is often organised around services or specific conditions rather than putting individuals at the centre of care and support. This does not promote consideration of people’s needs in their totality or the most effective use of available resources. The common approach is to use clinical pathways for each condition which means patients can end up on different pathways for multiple conditions with no holistic view of their needs.

Population segmentation enables the design of new models of care as well as a more preventive, proactive approach. Most health and care professionals will already group the population intuitively for the purposes of delivering effective care (e.g. people over 75, people with long term conditions (LTCs)). Grouping is important for several reasons:

1. *Grouping helps in understanding the distinctive needs of different parts of the population.* This is an important first step to achieving better outcomes through integrated care. Understanding the characteristics of population needs should inform the choice of schemes and services to be offered.

2. *Grouping helps define the main combinations of care that people might need.* Integrated care aims to handle the complexity of people's interdependent needs. To do that, care needs to be tailored. A one-size fits all approach is inadequate. Different sets of people have different needs. Ideally segmentation would be unique to each individual, but that would require fifty million segments, so it needs to be simplified. A good segmentation approach is intuitive to professionals, does not overlap much with other groups and uses sensible categories that are tailored enough to accurately describe people's needs, but not so minute as to become unwieldy.
3. *Grouping supports prioritisation and a phased approach to implementation.* Grouping enables a focus on what's most relevant to the local population. Each local area can decide which group(s) they want to focus on first, according to local priorities and context.
4. *Grouping allows the modelling and tracking of how integrated care interventions affect different patient groups.* The groups will form the primary organising logic for new models of care, desired outcomes and the approach to measuring progress.
5. *Grouping allows new payment models to incentivise providers.* The grouping of population along with the relevant budgets allows the creation of capitated budgets and payment models. Without patient segmentation and the underlying data it is impossible to do this.

Options for grouping

There are four different options for grouping the population:

1. Utilisation risk (risk stratification)
2. Age and condition
3. Social and demographic factors
4. Behaviour

The most common are by utilisation risk (risk stratification) and by age and condition. It is recommended that HWBBs focus on these two methods as the most practical for the purpose of BCF plans.

- *Utilisation risk (risk stratification):* this method of grouping the population is based on how likely people are to use services. This is commonly done on the basis of an unplanned emergency admission in the next year using a centralised risk algorithm, such as the Combined Predictive Model (CPM) to do so.

  The advantages of this approach are that it is commonly used and based on widely available data. However, there are disadvantages too. It is very focused on acute care, the risk groupings are usually done year-on-year and may not be stable from year-to-year.

- *Age and condition:* the population is divided into groups typically first by age (e.g. children under 12, under 18, 18-50, 50-75, 75+) and then by condition (e.g. no chronic condition, chronic conditions, severe and enduring mental illness). This is the preferred approach of many international integrated care providers and payors (commissioners).

  The advantages of this approach include: it is easy to define; easy to understand; remains fairly constant over time as age and condition tend not to be reversible; and, can easily capture activity and cost data by segments given existing coding. However, the disadvantages include: there can be significant disagreements about the "right" boundaries to use in creating segments; and, that it may imply a "one size fits all" approach for each segment. It is for this reason that applying a risk stratification to the segmentation will yield a more precise understand of the needs of each segment.

Risk stratification

Stakeholders across the system want to identify people who are most at risk of deterioration or at risk of a significant care event. A range of predictive risk models can be used to stratify the population by the probability of an emergency admission in the next year. This approach is commonly used by many internationally including Care More and Kaiser.

In the UK, commissioning risk stratification is the responsibility of individual NHS bodies. In the past, the Department of Health has recommended the use of CPM and PAAR as the best predictors.

Risk stratification analysis may be supported by your local analytics service provider such as your CSU.

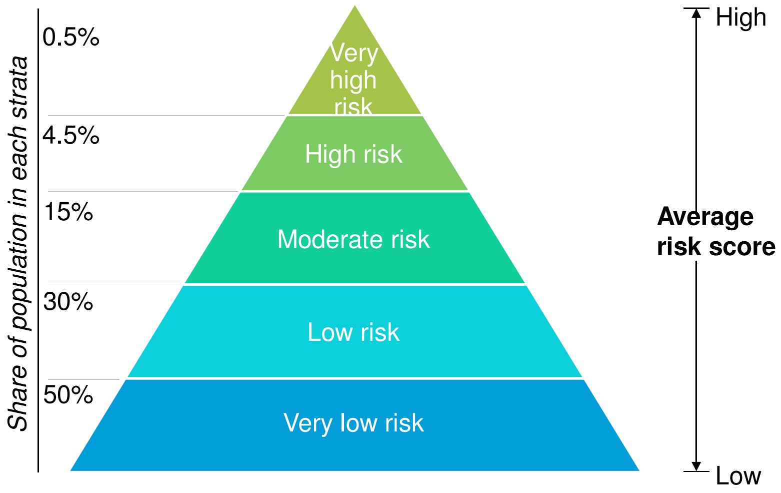
A list of **risk stratification approved Organisations** can be found at: http://www.england.nhs.uk/ourwork/tsd/ig/risk-stratification/

The two highest predictors of risk based on CPM are previous acute admissions and age. CPM distributes the population based on the risk score by allocating a pre-determined share of the population to each strata.

A regression can be run on the data to identify the factors that determine whether a certain event, like a non-elective admission, will occur. Determining those factors allows an assessment of the probability that such an event will occur to a given patient. This allows for specific patients or patient cohorts to be prioritised for proactive preventative care.

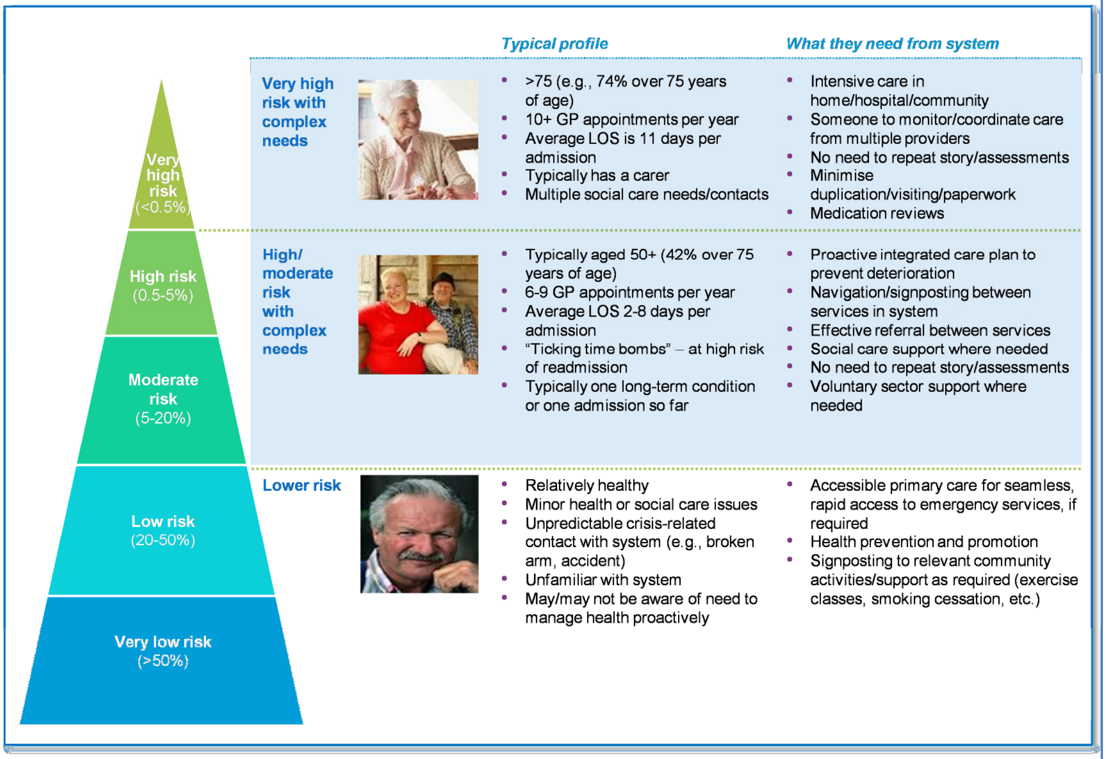
This can either be done using a person identifiable data set with explicit consent, or through using pseudonymised data that is then re-identified by clinicians entitled to hold it so that they can assign risk scores to their patients.

Figure 2. The risk stratification pyramid.
Running data through a risk stratification tool will provide an output that shows the number of people in each risk strata. The shares of population in the example below come from an example CCG – these rates will be different for different localities.



SOURCE: CCG Example, 2014.

Figure 3. An example of how risk stratification informs the targeting of care. Understanding who specifically is in each risk strata will enable an understanding of their requirements from the system as a whole, rather than what they need at one point in time for the treatment of a specific condition.



	Typical profile	*What they need from system*
Very high risk with complex needs	• >75 (e.g., 74% over 75 years of age) • 10+ GP appointments per year • Average LOS is 11 days per admission • Typically has a carer • Multiple social care needs/contacts	• Intensive care in home/hospital/community • Someone to monitor/coordinate care from multiple providers • No need to repeat story/assessments • Minimise duplication/visiting/paperwork • Medication reviews
High/ moderate risk with complex needs	• Typically aged 50+ (42% over 75 years of age) • 6-9 GP appointments per year • Average LOS 2-8 days per admission • "Ticking time bombs" – at high risk of readmission • Typically one long-term condition or one admission so far	• Proactive integrated care plan to prevent deterioration • Navigation/signposting between services in system • Effective referral between services • Social care support where needed • No need to repeat story/assessments • Voluntary sector support where needed
Lower risk	• Relatively healthy • Minor health or social care issues • Unpredictable crisis-related contact with system (e.g., broken arm, accident) • Unfamiliar with system • May/may not be aware of need to manage health proactively	• Accessible primary care for seamless, rapid access to emergency services, if required • Health prevention and promotion • Signposting to relevant community activities/support as required (exercise classes, smoking cessation, etc.)

SOURCE: CCG example, 2014

Segmenting by age and condition

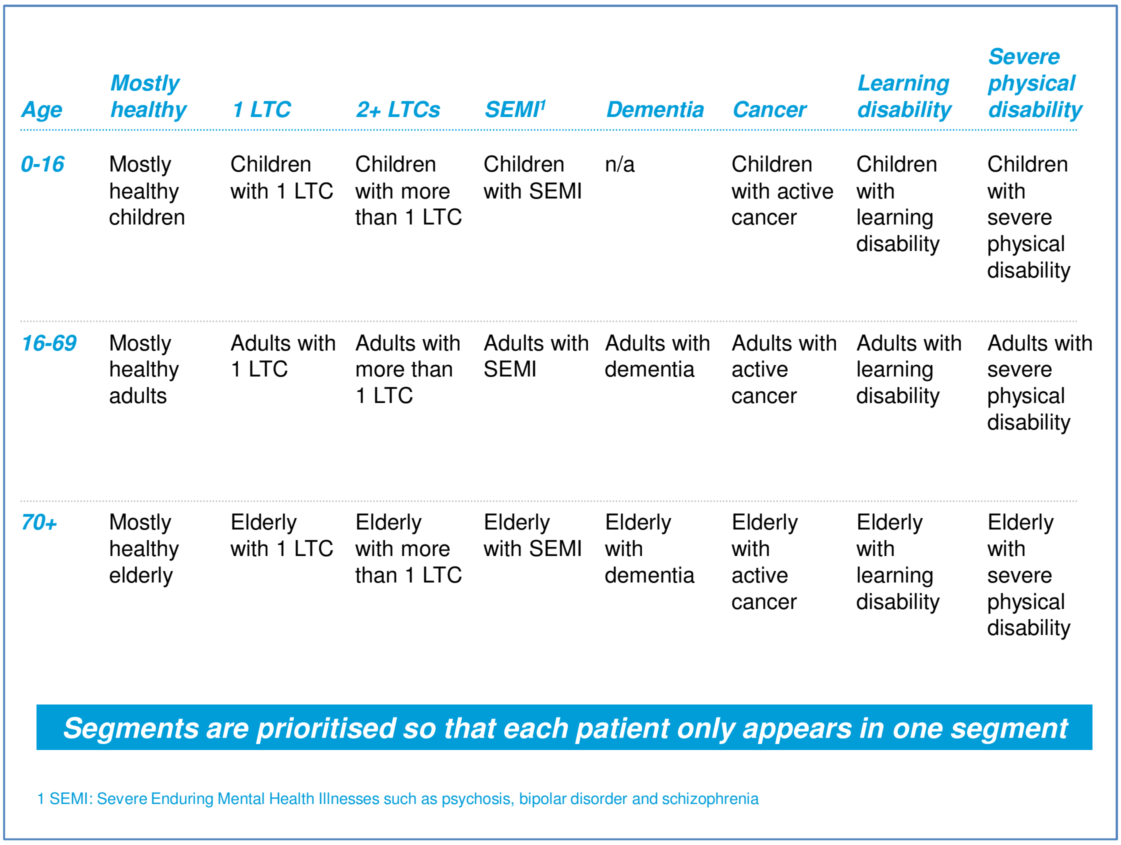
As an alternative to risk stratification, the approach taken by many international case examples including ChenMed and New York Care and in the UK pioneered by North West London, is to segment the population based on age and type of health condition.

In order to conduct a valid segmentation of this nature, it is vital to include a range of relevant insights including:

1. The judgement of multiple professionals (i.e. health and social care commissioners, clinicians and other professional, public health experts, academics from the AHSN) and lay partners
2. An in-depth analysis of the integrated health and social care data set
3. A review of internationally applied grouping models.

Figure 4 illustrates one way of segmenting the population.

Figure 4. Example segmentation.
This matrix is very commonly used to segment the population. Relevant age groups are categorised along one axis, whilst the relevant conditions are categorised along the other. The number of people in each segment, along with the total cost of care, can populate this table to provide a useful profile of the population.



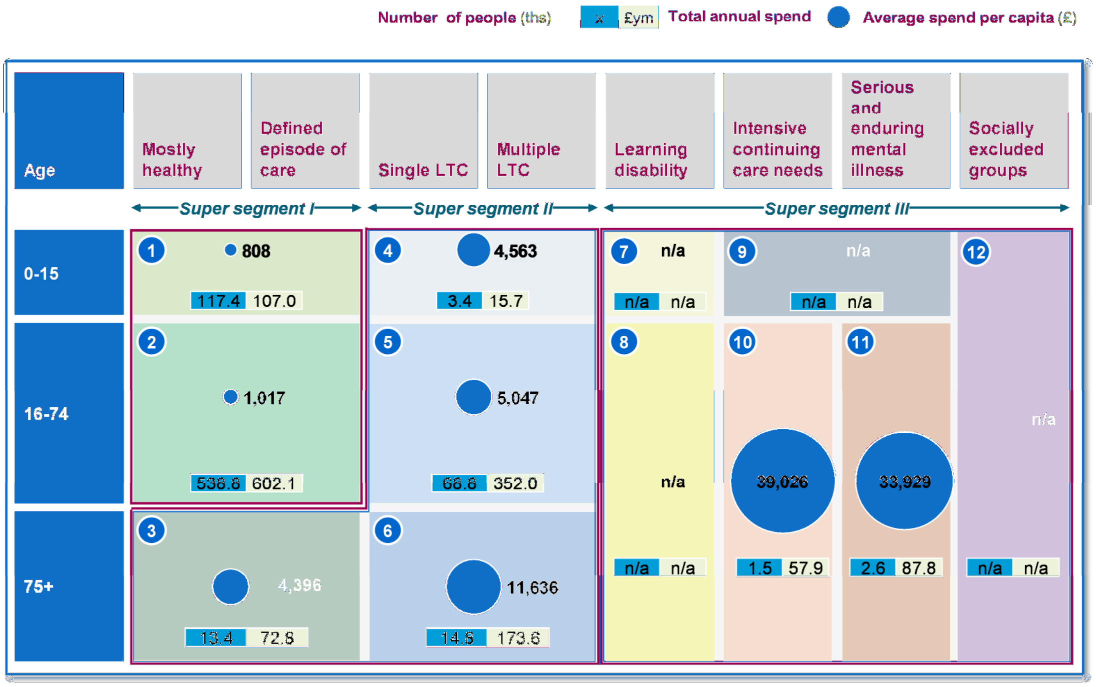
Age	*Mostly healthy*	*1 LTC*	*2+ LTCs*	*SEMI*[1]	*Dementia*	*Cancer*	*Learning disability*	*Severe physical disability*
0-16	Mostly healthy children	Children with 1 LTC	Children with more than 1 LTC	Children with SEMI	n/a	Children with active cancer	Children with learning disability	Children with severe physical disability
16-69	Mostly healthy adults	Adults with 1 LTC	Adults with more than 1 LTC	Adults with SEMI	Adults with dementia	Adults with active cancer	Adults with learning disability	Adults with severe physical disability
70+	Mostly healthy elderly	Elderly with 1 LTC	Elderly with more than 1 LTC	Elderly with SEMI	Elderly with dementia	Elderly with active cancer	Elderly with learning disability	Elderly with severe physical disability

Segments are prioritised so that each patient only appears in one segment

[1] SEMI: Severe Enduring Mental Health Illnesses such as psychosis, bipolar disorder and schizophrenia

Once an agreed segmentation is developed the whole population are allocated within it. Figure 5 provides an example of the output that can be created from making use of such data.

Figure 5. Projected 2018/19 spend per capita by segment.
The example below demonstrates what a complete segmentation could look like. With the conditions on one axis and the age on the other, the tool used to do this was able to populate the number of people, total annual health and care spend, and average spend per capita. A visual like the one below helps identify the biggest population segments and largest areas of disproportionate spend – informing the selection of a target segment.



SOURCE: CCG Example

For a detailed view of the methodology used by North West London, please see Chapter 4 of the North West London System Integrated Care Toolkit: http://integration.healthiernorthwestlondon.nhs.uk/chapter/what-population-groups-do-we-want-to-include-

What is essential for your plan?

BCF plans should demonstrate an understanding of the patient population, including an understanding of:

- Which population segments will be targeted
- Why these population segments are being targeted, i.e. the level of disproportionate care being consumed, how the segments are driving cost.

These questions can be answered through an analysis of Hospital Episode Statistics (HES), Joint Strategic Needs Assessment and QOF Registry data. With this data, it is possible to identify the proportion of the population that is elderly (75+) OR has a long-term condition. Specifically, use QOF or JSNA to assess the prevalence of major long-term conditions. Alternatively, look for specific diagnoses codes associated with major long term conditions in your HES data

Working with your CSU or your analytics team, analyse HES data to assess how many non-elective (NEL) admissions, outpatient appointments and A&E visits were associated with the elderly or people with major LTCs and what proportion of the total number of NEL/OP/A&E activity this represents. Doing this will provide you with a rough population segmentation

In addition, it is recommended that at minimum, risk stratification is conducted by plugging HES and JSNA data into PAAR++. This output will provide a rudimentary understanding of the risk strata in the local population.

Using HES, JSNA and QOF data for these exercises will provide a static, point-in-time snapshot of the local population and will not account for various person-specific characteristics such as co-morbidities. As a result, HWBBs should use regional BCF support teams to create a plan to achieve best practice population grouping and should reflect these plans in the resubmission.

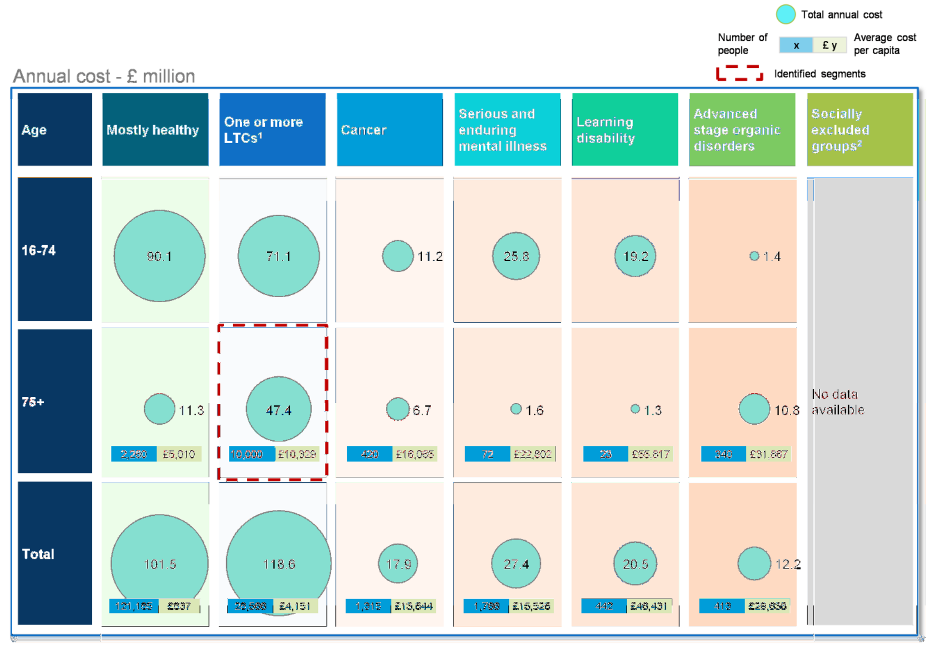
What is recommended for your plan?

To conduct a robust, dynamic population grouping exercise, a routinely updated patient-linked data set, including social care data, will provide the best data foundation for the analysis. The routinely updated and linked data will allow for dynamic segmentation, ensuring that HWBBs can update scheme offerings based on changing population needs.

Additionally, PAAR++, whilst being a helpful tool, is relatively outdated. HWBBs can improve the predictive accuracy of analyses through the use of newer, legally compliant models (e.g., QAdmissions, CPM version 2), as outlined in Appendix 1b.

BetterCareTown HWBB case study exhibit 1: Population segmentation

The output of BetterCareTown HWBB's segmentation facilitates an understanding of how the population is dispersed depending on health and care needs, as well as by the cost of care. In the example below, it is evident that those with one or more LTCs drive a disproportionate share of costs. Because this HWBB has recently implemented several interventions targeting the younger segment of those with LTCs, they have decided to focus this round of planning on those 75+ with a LTC. In the next section, we develop an understanding of how BetterCareTown HWBB used this understanding to inform their search for evidence based interventions.

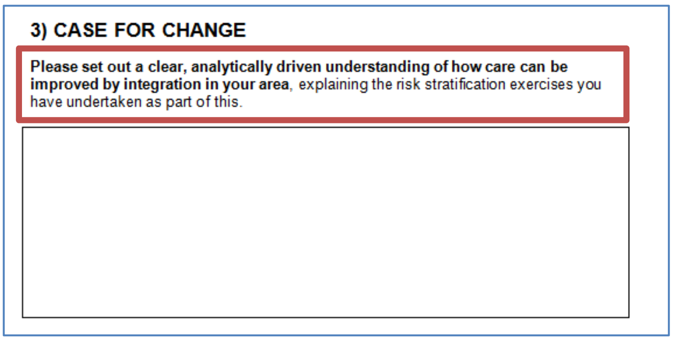


1 Including people with severe physical disabilities | 2 For example, the homeless, people with alcohol and drug dependencies

Source: Integrated data-set from H&F, ICP data warehouse, FIMS 2012/13, CCG Budget

How to use this information in the planning templates

Part 1 and part 2 of the template require the demonstration of population segmentation or risk stratification.

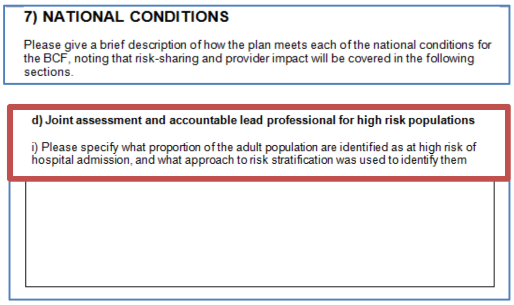


3) CASE FOR CHANGE

Please set out a clear, analytically driven understanding of how care can be improved by integration in your area, explaining the risk stratification exercises you have undertaken as part of this.

Part 1, Section 3 requires an explanation of the approach taken to segmenting or risk stratifying the population in order to understand the population's needs.

To fill this section out to a high standard, the methodology used should be described, the basic findings, and the implications for improving health and care. The best answers will use linked patient-level data over time to identify those interventions that will lead to the biggest impact.



7) NATIONAL CONDITIONS

Please give a brief description of how the plan meets each of the national conditions for the BCF, noting that risk-sharing and provider impact will be covered in the following sections.

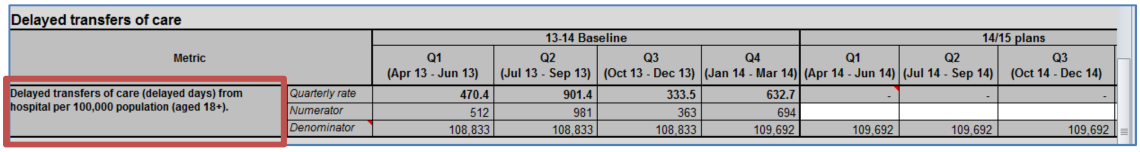
d) Joint assessment and accountable lead professional for high risk populations

i) Please specify what proportion of the adult population are identified as at high risk of hospital admission, and what approach to risk stratification was used to identify them

Part 1, Section 7d (Joint assessment and accountable lead professional for high risk populations) requires the identification of the segment of the population of highest risk of hospital admissions, as well as an explanation of the approach used to identify this group.

Part 2 requires that the population has been risk stratified specifically on tabs 5 and 6, for example:

6. HWB Supporting Metrics (i.e., Delayed transfers of care from hospital per 1,000 population, aged 18+)



Delayed transfers of care

Metric		13-14 Baseline				14/15 plans		
		Q1 (Apr 13 - Jun 13)	Q2 (Jul 13 - Sep 13)	Q3 (Oct 13 - Dec 13)	Q4 (Jan 14 - Mar 14)	Q1 (Apr 14 - Jun 14)	Q2 (Jul 14 - Sep 14)	Q3 (Oct 14 - Dec 14)
Delayed transfers of care (delayed days) from hospital per 100,000 population (aged 18+).	*Quarterly rate*	470.4	901.4	333.5	632.7	-	-	-
	Numerator	512	981	363	694			
	Denominator	108,833	108,833	108,833	109,692	109,692	109,692	109,692

Further Reading

North West London "Whole Systems" toolkit: Chapter 4 (http://integration.healthiernorthwestlondon.nhs.uk/chapter/what-population-groups-do-we-want-to-include-)

"Understanding Patients' Needs and Risk: A Key to a Better NHS", McKinsey 2013 (http://bit.ly/20prcnt)

Combined Predictive Model, King's Fund 2006 (http://www.kingsfund.org.uk/sites/files/kf/field/field_document/PARR-combined-predictive-model-final-report-dec06.pdf)

"Choosing a predictive risk model: a guide for commissioners in England", Nuffield 2011 (http://www.nuffieldtrust.org.uk/publications/choosing-predictive-risk-model-guide-commissioners-england)

Monitor is planning the release of a tool called the "Ready Reckoner." This tool provides a shortcut to segmentation by grouping population data according to typical profiles of similar localities (e.g., urban, rural). Please check their website regularly for the release of this tool

APPENDIX 1A: INFORMATION GOVERNANCE CONSIDERATIONS FOR RISK STRATIFICATION PURPOSES

This guidance is written at a point when the legal landscape is about to change.

The legal bases supporting the use of identifiable information for population segmentation and risk stratification are currently dependent upon time limited Secretary of State for Health and adult social care approvals under Regulations established in section 251 of the NHS Act 2006, which are about to expire.

New Regulations due to come into force late 2014/early 2015 will change the law[1].

The validity of this guidance is therefore limited and should only be used in connection with the BCF revised planning activity timetable.

Organisations establishing new systems to process data will need to ensure the plans can adjust to these changes.

What is it?

Information is a valuable business asset and central to every process from supporting the clinical management of individual patients, through to the management, organisation and resourcing of services.

Information Governance is a framework of statutory, mandatory and best practice standards that collectively ensure any use of information (in particular confidential information) is conducted fairly, legally and securely.

Why is it important?

Information Governance provides a clear structure to the complexity of rules that govern all use of information.

In particular, it enables personal confidential information to be used in ways that protects an individual's confidentiality and legal rights.

This is important because loss of public trust in the ability of the service to protect confidentiality risks patient's withholding important information from the clinicians and professionals treating them and a loss or reduction of quality data for care and other related purposes.

[1] Department of Health – Protecting personal health and care data: A consultation on proposals to introduce new regulations https://www.gov.uk/government/consultations/protecting-personal-health-and-care-data

There is specific information governance methodology for using data for risk stratification and population segmentation, which ensures a legal basis for that use and protects the integrity, availability and confidentiality of information.

Procedures to control access to data must ensure that only clinicians or other professionals directly responsible for a patient's care can see patient identifiable information and that data is effectively anonymised for all other purposes.

Information Governance considerations for Risk Stratification purposes

Risk stratification technology analyses relationships in historic data derived from service user (patients and clients) activity to determine which people in a population are at high risk of experiencing outcomes, such as unplanned emergency care for two purposes:.

- targeting high-risk individuals in need of additional preventive care interventions, such as the support of a multi-disciplinary team. This is referred to as "risk stratification for case- finding"; and
- analysing a population to predict the future care needs so that cost effective services can be planned and commissioned. This is referred to as "risk stratification for commissioning".

It is important not to confuse the purpose of risk stratification for case-finding with direct care[2], although it may lead to it. In the majority of cases the process will not lead to any further action i.e. not all individuals will be in need of preventative care or treatment, therefore this exercise cannot be attributed to their direct care. The point at which direct care starts is after the risk stratification process, when those highlighted as being at risk are re-identified and assessed by a health professional directly responsible for the provision of care and treatment to the individual where the patient's implied consent can be assumed[3].

If you are using risk stratification for a case-finding purpose, then you need to decide what you are going to do in response to the high-risk results. The reliance on implied consent to access confidential information for a direct care purpose only extends to qualified (regulated) social care staff who are a member of the multi-disciplinary team. You therefore will need to consider how data will be shared with non-qualified social care workers.

[3] Caldicott 2 re-affirmed that implied consent is applicable only within the context of direct care of individuals. For direct care of an individual, registered and regulated social workers must also be considered part of the care team and covered by implied consent when the social worker has a legitimate relationship to the individual concerned.

This is explained further in the Health and Social Care Information Centre (HSCIC) Confidentiality guidance for health and social care. See References Section 7: Sharing information for direct care

http://www.hscic.gov.uk/media/12823/Confidentiality-guide-References/pdf/confidentiality-guide-references.pdf

Access to identifiable patient data for any other non-direct care purpose must be supported by a sound legal basis such as explicit consent or where statute or other legal duty mandates it.

Understanding the different categories of data

It is important to understand the different categories of data in order to apply the correct legal basis and information governance controls.

Personal data is defined in the Data Protection Act 1998 (DPA) as:

data which relate to a living individual who can be identified:

a) from those data, or
b) from those data and other information which is in the possession of, or likely to come into the possession of the data controller, etc.

Any processing (use) of personal data must be done in compliance with the eight data protection principles. The common law duty of confidentiality and the Human Rights Act 1998 (HRA) also apply. These are known as the “privacy laws”.

Anonymous or aggregated data is data from which an individual’s identify cannot be determined. Anonymised data falls out of the scope of the privacy laws and can be used for non-direct care (commissioning) purposes, which includes risk stratification.

Pseudonymised data falls in-between these two categories. Pseudonymisation is the process of distinguishing individuals in a data set by using a unique identifier which does not reveal their “real world” identity. When held by a person who has no means of revealing the identity of the individuals in the data set, then it is anonymised data. However, when held by a person who also holds or has access to the coded key that will allow the re-identification of the individual, it is personal data and the Data Protection Act 1998 and privacy laws engage.

Pseudonymised data is used for risk stratification in circumstances where strict controls are in place to limit access to the reversible key and prevent unauthorised re-identification.

Another definition of data is “De-identified for limited access”[4]. This is data that could be re-identified by matching it to other data or information and is therefore “personal data” by definition of the DPA. A lawful basis has to be established for its use, and disclosure is subject to regulatory codes of practice and stringent controls (i.e. governance and contractual with liabilities and penalties) to ensure it remains protected against unauthorised re-identification at all times.

Accredited Safe Havens (ASH) have been established within the health service to provide a secure environment to receive data that is potentially identifiable, but data flowing into an ASH still needs to be covered by a legal base.

Confidential patient data should only be used in cases where it is not possible to use anonymised or de-identified data; consent is not a practicable option; it is relevant and necessary for the purpose AND where there is a sound legal basis to allow or mandate that use.

The Health and Social Care Information Centre (HSCIC) Guide to confidentiality in health and social care, which is consistent with regulatory advice and professional codes of practice provides further detailed information.

http://www.hscic.gov.uk/media/12822/Guide-to-confidentiality-in-health-and-social-care/pdf/HSCIC-guide-to-confidentiality.pdf

Options for information governance compliant systems

Where it is necessary to use identifiable data for risk stratification purposes, including linkage to other data sets, this is established either through:

1. Explicit consent[5]; or
2. Using pseudonymised data within closed systems operating under controls to protect access to identifiable data limited; or
3. Regulations made under Section 251 of the NHS Act 2006[6]; or
4. Under the provisions of the Health and Social Care Act 2012,[7]

[4] Referred to as “Weakly pseudonymised data” in the NHS.

[5] Explicit consent is an unmistakeable indication of agreement given in writing or verbally, or conveyed through another form of communication such as signing.

[6] Section 60 of the Health and Social Care Act 2001 as re-enacted by Section 251 of the NHS Act 2006 allows the Secretary of State for Health to make regulations to set aside the common law duty of confidentiality requirement for consent when using data for defined medical purposes. The Regulations that enable this power are the Health Service (Control of Patient Information) Regulations 2002. Any reference to “section 251 support or approval” refers to approval given under the authority of these Regulations.

http://www.hra.nhs.uk/about-the-hra/our committees/section-251/what-is-section-251/

[7] Health and Social Care Act 2012 Chapter 2 http://www.legislation.gov.uk/ukpga/2012/7/part/9/enacted

Explicit consent.

Explicit consent is in use in some areas, but in general this is not considered to be a viable option for risk stratification purposes because of the high number of people involved and time to establish and is therefore not further considered in this guidance.

Pseudonymised data.

Systems that can pseudonymise data at the point of extraction are in use in GP Practices. These allow data to be extracted, pseudonymised, stratified automatically and returned in a non-identifiable format without it being seen by a human throughout the process. The GP has access to the coded key to re-identify data for a direct care purpose.

Anonymised data from this process can be used for risk stratification for commissioning purposes, however, its use has limitations because it cannot be linked to other data.

The following two options explain the ways in which data can be linked operating within the legal framework.

Option 1 - Risk stratification for case-finding

Section 251 approval (ref CAG 7-04(a)/2013 Risk Stratification) supports the use of patient identifiable data for risk stratification purposes by allowing data containing one strong identifier to flow into a data processor as:

1. Secondary Uses Service data derived from commissioning data sets, which is disclosed from the HSCIC under s261(4) of the HSCA via the HSCIC's Data Services for Commissioner's Regional Office (DSCRO)[8]; and
2. general practice (GP) data sets from GP systems under the instruction of GPs as data controllers.

Single strong identifiers are used for linkage purposes and can be either:

- a NHS number; or
- a full post-code;

Because this data can be re-identified by matching it to other data accessible to the data processor, controls must be in place to ensure attempts to re-identify are prohibited and confidentiality is protected.

[8] Having collected the data from commissioned service providers under HSCA section 254 Directions

The risk stratification service providers (data processors) must therefore meet information governance standards set out by the HSCIC before data can flow in accordance with the s251 approval.

Where data processing services are provided by a Clinical Commissioning Group (CCG) or Clinical Commissioning Support Unit (CSU) they have to meet Stage 1 accredited safe haven (ASH) standards. Alternatively, data can be flow to independent third parties acting as data processors where they fully meet IG Toolkit Level 2.

Where GP data is concerned, the GP Practice, as the data controller, must ensure the data is processed in compliance with the data protection principles. As a minimum, they have to inform their registered patient population about the ways in which their personal data are used (fair processing) and have written contracts in place with their data processors. These are explained further in this guidance and in Further Reading.

Valid HSCIC data sharing contracts and HSCIC data sharing agreements must also be in place.

Risk stratification operating under the section 251 approval can only be conducted by an organisation who have been approved as meeting these conditions and are listed on the Named Register of Existing Risk Stratification Suppliers.

NHS England Risk Stratification, including the Named Register of Existing Risk Stratification Suppliers and approved 3rd party organisations

http://www.england.nhs.uk/ourwork/tsd/ig/risk-stratification/

Once the information governance requirements are established, data can be extracted, cleansed, matched, pseudonymised, and analysed within the ASH and reported back as risk stratified data.

Using Role Based Access Controls (RBAC) the GP is provided with the key to reverse the pseudonymisation process to access patient identifiable risk stratified data for direct care purposes.

Anonymised data is provided for commissioning/population profiling purposes.

Further information is available at the HSCIC's website - Data flow transition page

http://www.hscic.gov.uk/dataflowstransitionmanual

Please note that at the time of writing this guidance, this Section 251 approval has not been extended to cover the disclosure of identifiable social care data.

Neither does it cover disclosures of data from commissioned health and social care service providers directly into the ASH.

Option 2 – Risk stratification for commissioning (population profiling)

Where the purpose of data processing for risk stratification concerns only population profiling, this can be done through the HSCIC.

Under the HSCA the HSCIC has statutory legal powers to provide data services to health and social care by collecting data, data cleansing, linkage, de-identification and analysis tools where they are directed or requested to, to facilitate and maximise data usage for secondary purposes where it is of public benefit.

The HSCIC can collect data:

- Under directions from the Secretary of State for Health or NHS England;
- Under a mandatory request from a principal body i.e. Monitor, CQC, NICE;
- Under a non-mandatory request from other bodies or organisations.

Directions issued to the HSCIC by NHS England allow the collection of local commissioning data[9] and historical Primary Care Trust (PCT) data "to enable CCGs and NHS England to perform their statutory functions" [10].

This means that data can be collected from various health providers, processed, risk stratified and made available to commissioners.

The HSCA Section 259 (10) states that in providing the information, the provider is not breaching the common law duty of confidentiality, but it does not override other Acts, so the data protection principles still apply.

The HSCIC can disclose pseudonymised data where they cannot be re-identified by the recipient, but cannot disclose identifiable data without a legal basis, which are provided either by directions, section 251 approval or explicit consent.

At the time of writing, directions have not been issued and s251 approval has not been granted therefore the only viable option is explicit consent from each individual concerned.

[9] Local commissioning data sets are defined as data other than Secondary Use Services (SUS) data or other national submission defined in contracts.

[10] The Health Care Information Centre (Establishment of Information Systems for NHS Services: Data Services for Commissioners) Directions 2013 http://www.england.nhs.uk/wp-content/uploads/2014/04/ig-expl-note-direct.pdf

Section 251 (reference CAG 2-03(a)/2013) supports the flow of data containing one strong identifier from the HSCIC's regional DSCRO into an CCG or CSU ASH to support commissioning purposes specified in the approval.

CAG 7-04(a)/2013 approval added risk stratification to the list of approved purposes.

The situation concerning the use of social care data is not as straightforward.

Whilst the HSCA provides legal powers to the HSCIC to collect adult social care data, this can only be done under directions from the Department of Health, which have not been issued.

Alternatively, an organisation can request the HSCIC to collect adult social care data under the HSCA section 255(1), subject to HSCIC discretion and in accordance with the Code of Confidentiality.[11]

This would engage HSCIC's legal powers to collect, cleanse, link to other data (e.g. health data) and pseudonymise it for analytical purposes.

However, s251 approvals do not cover the disclosure of pseudonymised adult social care data into an ASH.

This means that if you want to include social care data in data sets for risk stratification for commissioning purposes, it can only be conducted by the HSCIC or its DSCRO under a non-mandatory request and reported back in an anonymised format. Explicit consent would be required to disclose pseudonymised data.

Section 251 Information Governance conditions for processing

A Risk Stratification Assurance Statement is available in Further Reading.

The Assurance statement was established to ensure the information governance conditions of the s251 approval are met where data processing for risk stratification purposes relies on the s251 support to provide a legal basis.

A CCG or CSU operating risk stratification under the s251 conditions should have completed and returned the Assurance Statement to NHS England.

[11] The HSCIC have issued Confidentiality guidance for health and social care, but have not issued the statutory Code of Practice. A consultation process for the Code closed on 18/08/2014 and the final document will be published later in the year. http://systems.hscic.gov.uk/infogov/codes/cop/index_html

The Assurance statement can therefore be used to evidence the information governance controls are in place, or provide information to aid the completion of the BCF revised plans Narrative Template (Part 1) (7) NATIONAL CONDITIONS

Additional guidance is provided in Further Reading.

Other considerations

Data Protection

Section 251 Regulations allow the common law duty requirement for consent to be set aside to process confidential data, however, the Data Protection Act 1998 (DPA) and Human Rights Act 1998 still apply.

Where a legal basis is established under s251 support, the data still has to be processed fairly and lawfully in accordance with the data protection principles.

Further information is available in Further Reading, however in summary it is important to ensure:

The data controller and data processor roles are clearly identified;

- The data controller is liable for any breach of the Act, even when a data processor processes data on their behalf;
- Written contracts must be in place between a data controller and data processor;
- It is imperative to get fair processing right and inform people how their personal data is used, otherwise you will fail to comply with Act;
- Individuals have rights, including the right to opt-out of their personal data being used for non-direct care purposes, which they need to be informed about through fair processing communications;
- All processing is conducted in accordance to the data protection principles

A fundamental requirement of the conditions for processing under s251 is that patients have been informed (through fair processing notices and other communication materials) that their personal data is being processed for risk stratification purposes and their rights to register their dissent with their GP Practice.

If appropriate fair processing notices are not in place, this should be recorded as a risk (non-compliance with the first DPA principle) and an action plan developed to mitigate the risk.

If, however, fair processing notices are in place, this should be recorded as an example of good practice in Part 1 of the BCF revised plans.

Fair and lawful processing

The first DPA principle establishes four conditions for processing personal data. Personal data must be processed fairly and lawfully and in accordance with one of the Schedule 2 conditions and both a Schedule 2 and a Schedule 3 condition if the data is sensitive[12].

Further advice about the application of the data protection principles can be found in the Information Commissioner's Office Guide to Data Protection.

http://ico.org.uk/for_organisations/data_protection/the_guide

Fair processing

Compliance with the requirements of the DPA will be unlikely where there is a failure to comply with the first data protection principle to provide fair processing information to those people whose personal data you are collecting and using.

Fair processing requires you to be transparent – clear and open with individuals about how their information will be used (processed). This is especially important when personal data is used for purposes that would not be obvious or expected by the individuals concerned; where they have a choice as to whether or not their personal data can be used and/or where the data is sensitive and usage could be objectionable or cause them concern.

The Information Commissioner's Privacy Notices Code of Practice provides guidance in writing and communicating a fair processing notice. Consideration must be given as to how to actively communicate fair processing notices to ensure it reaches the highest possible numbers of service users.

http://ico.org.uk/for_organisations/data_protection/topic_guides/privacy_notices

The intention to process data for risk stratification purposes; to anonymise data for non-direct care purposes and an explanation of an individual's right to opt-out and how to register dissent must be included in the fair processing notice.

Contracts and data sharing agreements

The seventh data protection principle establishes certain provisions that must be in place when a data controller uses a data processor to process personal data on their behalf.

[12] Sensitive personal data is defined in the DPA as personal data relating to the racial or ethnic origin of the data subject; their political opinions, religious beliefs, membership of a Trade Union; physical and mental health condition; sexual life and the commission, alleged commission and proceedings for any offence committed.

This includes a requirement to have a written contract in place setting out what the processor can do with the data and what organisational and technical security measures should be in place to protect the data.

A written contract should therefore be in place between:

- The GP and the risk stratification service provider; and
- The GP and the HSCIC to cover the disclosure of data from the DSCRO to the risk stratification service supplier.

A Deed of contract should be established between the GP and the CCG to cover the arrangements for the CCG to commission risk stratification services on behalf of the GP.

Identifiable data, including de-identified data for limited purposes, should not be submitted directly to the data processor by another heath service provider because it (a) is not included in the s251 approval and (b) it bypasses the procedures to code opt-out preferences on GP records that prevent the data from disclosure for non-direct care purposes (see Opt-out codes below).

The HSCIC will issue data sharing contracts or data sharing agreements as appropriate to the nature and purpose of the information they are asked to disclose.

Opt-out codes

The 2013 revision of the NHS Constitution introduced a new right giving patients the option to request that their personal confidential information is not used for non-direct care purposes[13].

When an individual asks that their information is not used for non-direct care purposes (secondary purposes), a code is attached to their GP record to identify:

- Dissent from secondary use of GP personal identifiable information; and
- Dissent from disclosure of personal confidential data by the HSCIC.

The relevant codes are:

Dissent from secondary use of GP patient identifiable information: Read v2: 9NU0 or OTv3:XaZ89, or SNOWMED CT 827241000000103

[13] Established in the Health Act 2009 (Chapter 1), which came into force in January 2010 from when all providers of NHS care, either public or private, have to have regard for the NHS Constitution in everything they do. Clinical Commissioning Groups and NHS England have a duty under the Health and Social Care Act 2012 to promote the NHS Constitution. The NHS Constitution does not currently apply to Local Authorities in law.

Dissent from disclosure of personal confidential data by the HSCIC: Read v2:9NU4 or CTV3 XaaVL, or SNOWMED CT 881561000000100.

There is no provision to code dissent directly into secondary care and social care systems to prevent the data flowing into the HSCIC.

The dissent codes must not be overridden by obtaining personal data directly from a commissioned service provider for risk stratification purposes (or any other secondary use).

Section 251 approval does not override the dissent codes, therefore the HSCIC cannot disclose data that contains a strong identifier into an ASH for any commissioning purpose supported by the current approvals.

Dissent should not compromise an individual's health care needs, therefore when determining data sets for extraction for risk stratification for case finding, the inclusion and exclusion of codes needs to be taken into account.

Excluded data

There are certain categories of data that are highly sensitive and should be excluded from risk stratification processes.

The list of excluded data issued to health services by the Confidentiality Advisory Group (CAG) as part of the section 251 approval conditions is provided in Further Reading B (checklist*).*

Data matching – use of the NHS Number

The NHS Number should be used as the primary identifier for correspondence across all health and care services. Using the NHS Number makes it possible to share patient information safely, efficiently and accurately.

Where a local identifier is used this must be in addition to and not instead of the NHS Number. This has now been reinforced by the advent of the Care Act 2014 and other key policy statements.

Organisations must ensure that service user records, both paper and electronic, have an NHS Number stored on them as early as possible in the episode of care.

The National policy requirement is set out in Information Standard ISB 0149

http://www.isb.nhs.uk/documents/isb-0149/amd-136-2010/index_html

Compliance with the standard is required from 1 April 2015. Plans should be in place for using the NHS Number as the primary identifier for correspondence across all health and care services by this date. Organisations and system suppliers, however, are encouraged to comply with the standard as soon as possible.

The methods for tracing batch numbers include:

- Personal Demographics Service (PDS) – online interface using PDS – compliant systems to trace records and import the NHS number into the local patient record;
- Checking multiple records by batching them into a file for submission to the Demographics Batch Service (DBS); or
- Log onto the Spine Portal Summary Care Record Application (SCRa) to use the demographic tracing function to search individual records.

These options may be used together.

The presence of a NHS number across the various health and social care service providers enables accurate data linkage.

This can only be done by the HSCIC (or DSCRO) operating under their HSCA section 261(4) powers.

Batch tracing is available to populate databases with the NHS number.

Longer term dependency upon the NHS number will require spine enabled (N3) social care connectivity (see Interoperability and Application Programme Interfaces)

See the HSCIC Guidance to support the use of the NHS Number for further details http://systems.hscic.gov.uk/nhsnumber/staff/guidance

Interoperability and Application Programme Interfaces

The Strategy for the HSCIC 2013-2015 sets out the plans to improve interoperability through information standards and the development of data and information systems for the whole of the health and social care system.

http://www.hscic.gov.uk/media/13557/A-strategy-for-the-Health-and-Social-Care-Information-Centre---2013-15/pdf/hscic-strategy-2014.pdf

Organisational and technical security measures should be in place to protect personal data and ensure appropriate access is controlled.

The Information Governance Toolkit sets out the Department of Health Information Governance policies and standards that all organisations are required to operate to by achieving a minimum of level 2 compliance. Completion of the BCF revised plan (Template 1) requires you to explain your approach for adopting systems that are based upon Open APIs (Application Programming Interface) and Open Standards (i.e. secure email standards, interoperability standards (ITK))

The following information should assist the completion of that section:

The IG Toolkit sets out the details of the IG standards and provides links to exemplar materials such as national policy documents in the Knowledge Base. It also provides access to each organisations published self-assessment audit report.

https://www.igt.hscic.gov.uk/resources.aspx?tk=418705489316493&cb=9019ebda-caa0-425f-a7c8-413723ef0fa8&lnv=8&clnav=YES

The HSCIC Interoperability Toolkit (ITK) is a set of common specifications, frameworks and implementation guides to support interoperability within local organisations and across local health and social care communities. http://systems.hscic.gov.uk/interop/background/itk

ITK Specifications and downloads are available at http://systems.hscic.gov.uk/interop/background/specs (NB: requires Registration to download)

Application Programming Interfaces (APIs) are being developed as part of the NHS e-Referral Service solution to provide access to services and content through a well-defined and secure interface. http://systems.hscic.gov.uk/ers/supplier/apis

How do you develop a baseline and do risk stratification/segmentation for a local population?

What can you do for your plan if unable to complete the best practice guidance?

If not already in place, the information governance conditions will not be established in a two week period, therefore consideration must be given to what information currently exists that is appropriate and available for use in the BCF revised plans process. For example:

- Make the best use of the services provided by the HSCIC and regional DSCROs.
- Consider what published information is available for re-use, for example, current trends and data submitted by CCGs through UNIFY[14]
- Talk to local CCG and CSUs, to establish what information they hold that is available for use.

Information that is not identifiable but can be re-identified must not be disclosed outside the CCG or CSU ASH, therefore it must be anonymised in accordance to

[14] - See more at: http://www.local.gov.uk/health-wellbeing-and-adult-social-care/-/journal_content/56/10180/4096799/ARTICLE#sthash.lYRfYSFg.dpuf

the ISB Anonymisation Standard before it is made available to any CCG, CSU or Local Authority team. http://www.isb.nhs.uk/library/standard/128

Assurances must be provided that the data had been obtained fairly and lawfully if it is to be used for the BCF revised plans. CSUs and CCGs will have submitted a Risk Stratification Assurance Statement to NHS England to provide assurance that information governance controls are in place in order to receive data in accordance with the current s251 approval.

The Assurance statement itself will provide evidence that information governance controls were established when the data was stratified. It will also provide some other information required for the BCF revised plans, for example, the Risk Stratification service supplier; the DSCRO; what data sets were used i.e. did it include SUS data; and a Privacy Impact Assessment (if completed) would provide identified risks to include in the risk log.

How do you use this information in the planning template?

Narrative Template (Part 1)

7) NATIONAL CONDITIONS

Please give a brief description of how the plan meets each of the national conditions for the BCF, noting that risk-sharing and provider impact will be covered in the following sections.

c) Data sharing

i) Please set out the plans you have in place for using the NHS Number as the primary identifier for correspondence across all health and care services

Refer to Information Standard ISB 0149 http://www.isb.nhs.uk/documents/isb-0149/amd-136-2010/index_html

Self-assessed performance against IG Toolkit standard 11 – 421 or 11-422 (reference varies between organisational views) and evidenced in the published report https://www.igt.hscic.gov.uk/Home.aspx?tk=418705489316493&cb=3d05ac2c-920a-454d-8b9b-8f954754b591&lnv=7&clnav=YES

Identify which method for tracing is in use HSCIC http://systems.hscic.gov.uk/nhsnumber/staff/guidance

ii) Please explain your approach for adopting systems that are based upon Open APIs (Application Programming Interface) and Open Standards (i.e. secure email standards, interoperability standards (ITK))

See HSCIC for references http://systems.hscic.gov.uk/interop/background/specs

Please explain your approach for ensuring that the appropriate IG Controls will be in place. These will need to cover NHS Standard Contract requirements, IG Toolkit requirements, professional clinical practice and in particular requirements set out in Caldicott 2.

Where data was provided by a CCG or CSU, the Information Governance Assurance Statement they issued to NHS England as part of the conditions to process data under the NHS Act section 251 Regulations will provide assurance that the appropriate IG controls were in place and the data processing was conducted under a lawful basis.

Caldicott 2 recommended risk stratification should only be conducted using technology that allows data to be extracted from its source, pseudonymised, stratified automatically and returned in a non-identifiable format without it being seen by a human throughout the process. ;

Explain what controls are in place to ensure personal identifiable data is only accessible to those health and social care professionals responsible for the provision of direct care and treatment; and

Provide assurance that anonymous or aggregated data is used for all other purposes.

The NHS Standard Contract requirements specify that organisations should complete the IG Toolkit on an annual basis, achieve a minimum level 2 performance on all standards and publish their self-assessment report. Evidence can be obtained from the IG Toolkit (see Reports) https://www.igt.hscic.gov.uk/

Joint assessment and accountable lead professional for high risk populations

i) Please specify what proportion of the adult population are identified as at high risk of hospital admission, and what approach to risk stratification was used to identify them

To include the predictive tool used and whether it was:

a) an automated process that directly determined which patients should be offered preventative interventional services, or,

b) whether an appropriate clinician responsible for direct care reviewed which patients identified as high risk are offered preventative interventional services based on both the risk stratification output and other information known to them.

Whether the purpose of risk stratification was for case-finding, population profiling or both.

The source of the data and assurance that it was anonymised in accordance with the ISB standard before it was disclosed for commissioning purposes.

Further Reading A:

Information Governance Risk Stratification Assurance Statement

Including:

- **Risk Assessment Assurance Statement**
- **Checklist**
- **List of approved suppliers (note the Register is a separate document)**
- **List of excluded data items**

NHS England Risk Stratification, including list of risk stratification approved organisations

http://www.england.nhs.uk/ourwork/tsd/ig/risk-stratification/

Further Reading B:

How do you develop a baseline and do risk stratification/segmentation for a local population?

A Risk Stratification Information Governance Assurance Checklist is provided in Further Reading A. Derived from the NHS England Risk Stratification and Information Governance (which is currently being updated), it lists all requirements that need to be in place to ensure the appropriate information governance controls are met and data is being processed lawfully.

The following provides supplementary detailed information to that check list.

Ref	Checklist	Further information
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: Commissioning Support Unit (CSU) Health and Social Care Information Centre (HSCIC) regional office providing Data Services for Commissioners (Data Services for Commissioners Regional Office - DSCRO) Public health team Social care team	It may also be appropriate to include other stakeholders such as the local Clinical Commissioning Groups (CCGs), the Local Medical Council (LMC) and GPs in the development of a policy. A Privacy Impact Assessment (PIA) at the early stages of the design will enable privacy concerns to be identified, understood and addressed at an early stage. See the Information Commissioner's Conducting Privacy Assessments Code of Practice.[15]
2	Conduct an ethical review to safeguard against unintended consequences, such as the inadvertent worsening of health care inequalities.	Part of the policy development.
3	Develop one or more preventive interventions that will be offered to high-risk patients.	Part of the policy development. Consider: What are you going to do in response to risk stratification? Only qualified (regulated) social care staff can access identifiable data for a care purpose relying on implied consent. How are you going to share data with non-qualified social care staff?
4	Select a suitable predictive model. The factors that should be considered in selecting a suitable tool	Decide the purpose you need to achieve through a risk stratification process in order to select a suitable predictive model, for example, PARR 18 looks at the

[15] http://ico.org.uk/for_organisations/data_protection/topic_guides/privacy_impact_assessment

	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. 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).	likelihood of resubmission in 18 months and PARR30 30 days, whilst Combined Predictive Models looks at a wider range of factors. The following should be considered when selecting a suitable tool: the adverse outcomes to be predicted; the accuracy of the predictions; the cost of the model and its software; the availability of the data on which it is run; and future needs i.e. does it have the flexibility to develop or does it already include a wide range of data. Information governance considerations will affect the choice of model as they may need to be flexible to support current and future lawful practice. These include: whether the tool can be run using data pseudonymised at the point of extraction (pseudonymised at source); or technical controls are in place to support the flow of data containing a single identifier (referred to in the s251 approval as “weakly pseudonymised” data) from a DSCRO to an ASH ; or where identifiable data (i.e. personal confidential information) is used on an explicit consent basis, technology can take account of consent being withdrawn; and in all cases, whether the tool includes privacy enhancing technologies to restrict access and prevent unlawful access to confidential personal information.
5	Where the data are to be processed in identifiable form	Where the data are to be processed in identifiable form, including data holding

	(i.e., confidential patient information) ensure there is a legal basis to obtain and process the data for these purposes. The legal basis is currently provided by the s251 approval, but longer term arrangements to utilise pseudonymised data and re-identify only by those with a legitimate relationship with an individual should be developed or alternative legal basis sought such as consent.	one identifying element, you must ensure there is a legal basis to obtain and process the data for these purposes. The legal basis within health is currently provided by the s251 approval, but this does not apply to social care data, public health data or data directly provided to the data processor (CCG, CSU or 3rd party) – even if it is going into an ASH. Plans should already be in place to ensure data can continue to be used under a legal basis when the s251 approval expires (imminent). An awareness and training programme should commence to ensure that all relevant staff involved in the process are informed and understand their contractual and professional obligations to protect confidentiality and prevent re-identification of data by unauthorised users.
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 (only the minimum amount of data necessary to meet the purpose should be used)	Agree a defined data set to be used for risk stratification that is necessary, adequate, relevant, but not excessive for the purpose– including the extent of historical data needed to run the model (e.g. two or three years' worth of data) ensuring dissent codes and excluded data have been taken into account.
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).	Discussions with the GP as the data controller and GP data providers as the data processor are required – the provision of data must be supported in a written contract to satisfy the seventh DPA principle and under which the data processor is only to provide data in accordance with the GP's instructions and with a lawful basis.
8	Determine whether to use automated decision-taking or human review. With automated decision-taking, the outputs of the tool are used directly to determine which	Where a tool provides other clinical information (such as information derived from

	patients should be offered a preventive intervention. With human review, an appropriate clinician, with responsibility for the care of the individual patient, reviews which patients are to be offered preventive services. Their decision is based both on the risk stratification outputs and any other information known to them.	secondary care data or social care), 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.
9	Ensure that any data service providers being used for risk stratification have appropriate information governance controls in place. These controls include but are not limited to: 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). Ensuring that the data is not processed outside the European Economic Area. Please note that s251 approval is not covered for offshore processing and as such would constitute a breach of the conditions of the s251 support.	Choose a risk stratification service supplier who can provide guarantees that their organisational and technical security measures are as a minimum equivalent to those of the data controller and adequate to protect personal data. Assurance must be provided that the supplier meets the Information Governance Toolkit standards to a satisfactory level 2 or equivalent standards in ISO 27001 accredited. A Named Register of Existing Risk Stratification Suppliers meet these standards was established as a condition of the section 251 approval[16]. Retention and disposal policy and procedures should be drafted as part of the Risk Stratification Policy and included in the Data Controller/data processor contract (see 10).

[16] http://www.england.nhs.uk/ourwork/tsd/ig/risk-stratification/

		All personal data processed out of the UK must comply with both Principle 8 of the DPA and Department of Health policy. Organisations must also consider all the other Data Protection Principles before making an overseas transfer of person identifiable data. Of particular importance is the first Principle, which in most cases will require that individuals are properly informed about the transfer of their information to a country outside the UK.
10	Establish appropriate contractual arrangements with any data service providers that: Ensure there are appropriate organisational and technical measures in place to protect the data; Prevent the unauthorised re-identification, onward disclosure, or further unauthorised or unlawful use of the data and;	Principle 7 of the DPA establishes specific requirements when data is processed by a data processor on behalf of a data controller. Data protection contracts will need to be in place between each data controller providing patient data for risk stratification purposes and the data processor i.e. each GP Practice, the CCG commissioning the service and the risk stratification service provider. [17]

[17] A Data Controller is legally responsible for ensuring the processing of personal data they are responsible for is done fairly, lawfully and in compliance with the eight data protection principles.

	Include mechanisms to manage the contract and audit how the data are being used. Include a local process for managing patient objections where the data are weakly pseudonymised or identifiable. Patients may object to the disclosure or use of their personal confidential information, and/or they may object to automated decision-taking. Patients' objections must be respected. If a patient objects to the risk stratification tool being used to make automatic decisions about their care then there must be a human review of their data and of the decision made based on their risk stratification score.	The contract must include clauses to: Ensure there are appropriate organisational and technical measures in place to protect the data; Prevent the unauthorised re-identification, onward disclosure, or further unauthorised or unlawful use of the data and; Include mechanisms to manage the contract and audit how the data are being used; and Ensure the risk stratification suppliers will process personal confidential data (PCD) in the following manner: Data is received in a "de-identified data for limited access" form (i.e NHS number as the only patient identifier) or is pseudonymised on landing; AND Processing is within a "closed box" with strict role based access control; AND

- The GP or GP Practice is a Data Controller
- The Local Authority is the Data Controller for social care data
- The risk stratification service provider is a Data Processor and responsible for processing the data only in accordance with the instruction of the Data Controller and written into a contract.

The Data Processor will be a CCG or CSU processing data for risk stratification purposes in an Accredited Safe Haven (ASH); a 3rd party independent information services provider or a GP system provider, providing options to risk stratify directly using GP data as part of their clinical systems.

		Only the minimum data necessary and relevant for the purpose will be processed, with specific exclusions for sensitive information and appropriate use of the dissent codes; AND Re-identification is solely for the purpose of direct care and is made available only to those with a direct care relationship with the individual service user; AND Any publication of data other than in accordance with (iv) must be anonymised in line with the ISB Anonymisation for publication standard. AND Appropriate processes and contractual provisions are in place to securely destroy all data held in manual or electronic form once deemed it is no longer necessary for the purpose of risk stratification in accordance with agreed retention and disposal schedules. The named risk stratification supplier will provide a written procedure outlining a secure mechanism for receipt and processing of data within the risk stratification tool. These should include as a minimum the process for: • Receipt of data; • Retention periods; • Role based access controls, authorisation and maintenance; • Induction and training processes for users; • How audit trails will be maintained and confidentiality audits may be undertaken. Where SUS data is to be used, arrangements must be in place with the relevant DSCRO to provide data to the data processor for inclusion into the risk stratification programme. A separate data controller/data processor contract will be issued by the HSCIC to support this data flow. Similar arrangements need to be in place where other data controllers are included e.g. commissioned service providers and/or the local authority.

11	Develop a communications plan, including communication materials for patients (these materials may be incorporated into wider fair processing information).	You will fail to comply with the DPA if the first data protection principle to provide fair processing information to those people whose personal data you are collecting and using has not been complied with. If that is the case, you must only use anonymised data whilst action is taken to address the situation. Organisations should be open with people and explain clearly why their personal data is to be used, who it will be shared with and, where they have a choice, they are told about their options, the consequence of their decision and how to register objections. Fair processing information should be actively communicated where you are using sensitive information; or where the intended use is unexpected and likely to be objectionable; or where the information is shared with another organisation.
12	Inform patients that their identifiable or weakly pseudonymised data may be used for risk stratification purposes.	Patients have a right to object to their personal data being used for non-direct care purposes. Informing people that their data is anonymised provides assurance and demonstrates commitment to protecting confidentiality.
13	Ensure that only those clinicians who are directly involved in a patient’s care can see a patient’s identifiable risk score.	Supported by technical Role Based Access Controls (RBAC), documented policy and procedure and training. Where a tool provides other clinical information (such as information derived from secondary care data or social care), 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. An awareness and training programme should commence to ensure that all relevant staff involved in the process are informed and understand their contractual and professional obligations to protect confidentiality and prevent re-identification of data by unauthorised users.
14	Where a tool provides other clinical information (such	Where data from different sources has been matched, it could be possible to

	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.	access information from another care provider that the patient has previously requested that it is not shared with their GP.
15	Refer patients to preventive services only with their consent.	Giving people a say in how their personal information is used is an essential part of a good health care system. Ensure that patients are aware that this will include sharing their personal confidential data with those responsible for their direct care and manage their concerns.
16	Evaluate and refine the risk stratification model used and the preventive interventions offered according to its predictions.	Information that is not identifiable but can be re-identified must not be disclosed outside the CCG or CSU ASH, therefore it must be anonymised in accordance to the ISB Anonymisation Standard before it is made available to any CCG, CSU or Local Authority team.[18]

[18] ISB 1523 Anonymisation Standard for Publishing Health and Social Care Data http://www.isb.nhs.uk/library/standard/128