Health & Social Care Data Flows: Information Governance - Preparing for Transition - What You Need to Know

The Health and Social Care Information Centre (HSCIC) is England's national source of information about health and social care.

www.ic@nhs.uk

Contents

1. Introduction

1.1 Why have we produced this manual?

We have been asked by several health and social care bodies to provide guidance to support the significant changes to the information governance arrangements for commissioning data flows from 1 April 2013. The Health and Social Care Act 2012 (HSCA) provides a model where the expectation is that personal confidential data[1] (PCD) will be managed centrally (for purposes other than direct care) in order to protect confidentiality. Additionally, the current s.251 approval held by the NHS Health and Social Care Information Centre (HSCIC) for the processing of Secondary Uses Service Data on behalf of Primary Care Trusts (PCTs) will no longer be in place.

This manual provides guidance about the arrangements that you will need to put in place to be able to continue processing PCD lawfully for purposes **other than direct care**[2] from 1 April 2013[3]. It also explains the arrangements that you will need to put in place to be able to process de-identified data e.g. pseudonymised[4] or weakly anonymised[5] data as an Accredited Safe Haven (ASH). De-identified data are data that cannot be lawfully published due to the risk of individuals being identified but which does not immediately identify individuals where appropriate management and technical controls are in place.

It contains information relevant to organisations across health and social care[6] namely:

- Clinical Commissioning Groups (CCGs)

---

[1] This term describes personal information about identified or identifiable individuals, which should be kept private or secret. For the purposes of this document '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.

[2] In some cases, there are local data processing arrangements in place for direct care, for example where Local Authority Public Health staff are currently processing data on behalf of health or social care providers (who are the data controllers). In such cases, there must be appropriate legal arrangements in place, including contractual data processing agreements in order to comply with the Data Protection Act 1998 (DPA). It should be noted that contracts between NHS organisations are **not** considered to be valid contracts under the DPA.

[3] The Health and Social Care Act 2012 (HSCA 2012) requires the NHS Health and Social Care Information Centre (the HSCIC) to publish a code of practice to be followed in relation to the collection, analysis, publication and other dissemination of confidential information concerning, or connected with, the provision of health services or of adult social care in England. This Code of Practice will support your information governance activities in the longer-term by describing the overarching principles that will apply in health and social care.

[4] In pseudonymised data individuals in a dataset are distinguished by using a unique identifier, which does not reveal their 'real world' identity.

[5] Anonymised data is data which is rendered into a form which does not identify individuals and where identification is not likely to take place.

[6] Although social care is not undergoing national re-organisation, this manual will be enable social care organisations to understand their responsibilities surrounding information handling.

- Commissioning Support Units (CSUs)
- Data Management and Integration Centres (DMICs)
- Local Authority Public Health (LAPH) including Health and Wellbeing Boards
- Health and Social Care Providers, including private sector provider organisations
- The NHS Commissioning Board (NHSCB), including Regional Offices and Area Teams
- Registries, for example cancer registries
- Primary care organisations including GPs and out of hours services
- The Office for National Statistics (ONS)
- The Health and Social Care Information Centre
- Others, e.g. the Department of Health (DH), Monitor, Care Quality Commission (CQC).

It will be of particular interest to people in the following roles:

- Information users and information managers
  - Data and information managers
  - Information analysts
  - Public health intelligence teams
  - Local Authority public health teams
- Information governance leads and information governance managers
  - Caldicott Guardians
  - Senior Information Risk Owners
  - IT Security Officers
  - Information Governance Managers and Officers
- Medical Directors
  - Clinical Information Officers
  - Directors of Public Health

1.2 How will it benefit you?

This manual will help you identify the required governance arrangements for PCD and de-identified data flows to and from your organisation. By providing a single point of reference, this manual will enable you to:

- Identify and classify your data flows
- Follow the law and best practice
- Support business continuity
- Establish a dialogue with those with whom you will exchange data from April 2013
- Increase the potential for collaborative working across health and social care
- Reduce variability of data management solutions across the country and ensure greater harmonisation

1.3 Which data flows are covered by this manual?

This manual aims to cover the mandatory and principal voluntary[7] health and social care data flows to and from your organisation that will need to be in place from 1st April 2013, namely:

- Flows from local organisations to national bodies such as the DH, HSCIC, CQC; and
- Common local flows between health and social care organisations.

The manual does not list and provide guidance on all local data flows. Local data flows and data sharing agreements included are those flows that we understand occur across most organisations. However, the principles outlined in the manual can be applied to other local flows. We have included references within the guidance to help you identify how you should handle these other local data flows.

PCD will flow from health and care data providers into the HSCIC for national flows and the HSCIC hosted DMIC for local data flows. Onward data flows to CSUs, Local Authorities and the NHS CB Area Teams (the latter two are not shown in this diagram in figure 1 below) will be either effectively anonymised/aggregated[8] or record level pseudonymised. In certain limited cases, these recipients may require one or more identifiers (such as postcode) but this will only be supported where the recipient is accredited as a Safe Haven[9] for this purpose. CSUs will provide CCGs with business intelligence to support their commissioning responsibilities. The model assumes that CCGs will not require PCD to support their local commissioning activities though they may seek Accredited Safe Haven (ASH) status themselves if they would prefer direct access to the limited data that this would enable. Further information about the model is available on page 11.

National arrangements are being put in place to establish the lawful basis for these flows (s.251 support). Further details of the application and progress to s.251 support will be made available in the next release of this manual.

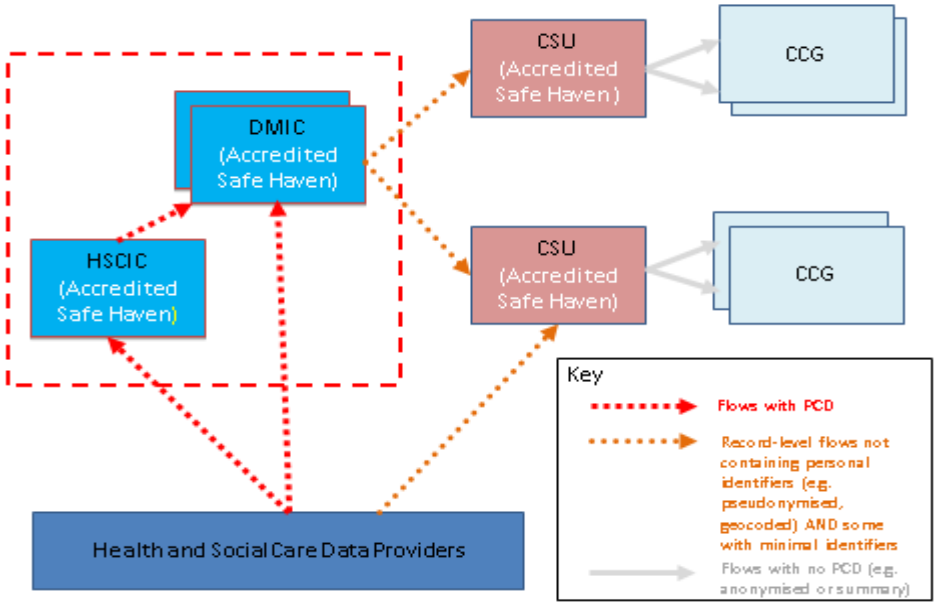
The NHSCB has aligned its model for organisational arrangements and information flows with the centralised model established by HSCA 2012. This model is illustrated in Figure 1 below.

Figure 1: The centralised model for commissioning data flows

[7] Please note, the flows included with this document are not necessarily mandatory data flows. You should not therefore take the inclusion of any particular flow as an indication that you have a right to demand this data from the data provider. You will need to ensure that there are appropriate contractual arrangements in place where relevant.

[8] Aggregated data is statistical data about several individuals that has been combined to show general trends or values without identifying individuals within the data.

[9] An accredited organisation with a secure electronic environment in which personal confidential data and/or de-identified 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. De-identified data can be held under contract with obligations to safeguard the data.



1.4 Historic business models

It is recognised that not all local commissioning support business models currently adhere to this model. In particular, in some areas organisational arrangements are such that:

- The flows from DMICs shown above as flowing to CSUs instead flow direct to CCGs without any form of ASH arrangements being in place
- There may be PCD flows from data providers to CSUs and/or independent sector organisations to support 'risk stratification'

Local arrangements where the processing and linkage of PCD is undertaken by a CSU or CCG (rather than in a DMIC) will fall outside the national arrangements and a local application to secure s.251 support for this processing will need to be made by the local organisation.

It is assumed that historic commissioning data will be passed from PCT control to DMIC control, under direction from the NHS CB from 1 April 2013 as DMICs (as part of the HSCIC) will be legally entitled to receive such PCD through the powers vested in them by the HSCA (see page 11 onwards).

1.5 Further advice and queries

A comprehensive reference library on the information governance and security standards that apply in health and social care (indexed by organisation) is available here: https://www.igt.connectingforhealth.nhs.uk/KnowledgeBaseOrganisationChooser.aspx

Please direct all queries on the contents of this manual and the data flows spread sheet underpinning it to **enquiries@ic.nhs.uk** with the subject 'Data Flows Manual'.

If your query relates directly to the IG Toolkit please contact **exeter.helpdesk@nhs.net** with the subject 'IG Toolkit'.

2. Using this manual

This manual is structured so that you should quickly be able to identify the information governance requirements and practical steps you need to take in your organisation for your data flows. The manual contains guidance on:

- How your organisation should handle information; (Page 6 to page 10)
- Specific data flows (presented in the spread sheet that accompanies this document).

In order to use this manual, you should:

A. Familiarise yourself with the general guidance on information governance (Page 6 to page 10)

B. Identify the data flows for your organisation using the tools (Page 10)

C. Take immediate action to ensure the measures described are in place in your organisation. You will need to ensure the arrangements described in this manual are in place on the 1st April 2013.

2.1 General Principles Regarding the Use of Confidential Information

The HSCIC will shortly be publishing a Code of Practice on the management of confidential information in line with its obligations in the HSCA. The Code of Practice will outline the general principles for handling care records, including the need to maintain accurate records, to share them when appropriate, to inform citizens about the use of records, to hold records securely and to act within the law. You will be required to comply with the Code of Practice once it is issued.

The comprehensive source of information and guidance on your detailed obligations regarding PCD is the IG Toolkit. This integrates the many different rules that cover how confidential information should be handled, including those set out in:

- The Data Protection Act 1998
- The common law duty of confidentiality
- The Confidentiality NHS Code of Practice
- The NHS Care Record Guarantee for England
- The Social Care Record Guarantee for England
- The ISO/IEC 27000 series of information security standards
- The Information Security NHS Code of Practice
- The Records Management NHS Code of Practice
- The Freedom of Information Act 2000
- The Health and Social Care Act 2012

These rules impose overlapping obligations on you to ensure the confidentiality, security and accuracy of the information you hold.

For example, Principle 1 of the Data Protection Act 1998 requires you to ensure that when you process personal data you do this in a manner that is:

- Fair, which means that you must inform data subjects (for example, service users) about how you intend to use information about them; and
- Lawful, which means that you must comply with any other legal obligations imposed on you by applicable case law and statutes. This means, for example, that you will need to ensure that your use of person confidential data does not breach common law confidentiality and is compatible with the ECHR Article 8 right to privacy (as incorporated into English law in the Human Rights Act 1998).

The IG Toolkit will help you to navigate this complex area of law and guidance by providing a checklist for the information governance and security requirements tailored for your organisation. The full list of IG Toolkit requirements by organisation type is available at: https://www.igt.connectingforhealth.nhs.uk/requirementsorganisation.aspx

The great majority of organisations are already working with the IG Toolkit (https://www.igt.connectingforhealth.nhs.uk) at the moment and should continue. Anyone new to the IG Toolkit should contact the IG Toolkit helpdesk (through exeter.helpdesk@nhs.net) who will help you get set up under the correct view.

Details of your obligations, including supporting guidance and references, are available online in the IG Toolkit. These fall into three broad categories:

I. **Your management structures and responsibilities**, including:
   - Establishing responsibility and accountability for Information Governance and Security in your organisation, and clarifying who owns individual data flows. Establishing an IG Board, forum or steering group with appropriate authority to deal effectively with IG issues.
   - The appointment of a Caldicott Guardian[10] - a senior person responsible for protecting the confidentiality of patient and service-user information and enabling appropriate information-sharing.
   - The appointment of a Senior Information Risk Owner i.e. a member of the Executive Team, separate from the Caldicott Guardian, who is responsible for overseeing the development and implementation of your Information Risk Policy and for owning your information risk management process.
   - Raising awareness and providing training to staff, particularly on issues surrounding the sharing and use of person confidential data and on information risk management.
   - Having appropriate policies and procedures in place for information handling, including your overarching IG Policy, Data Protection Act 1998, Confidentiality

[10] http://www.connectingforhealth.nhs.uk/systemsandservices/infogov/caldicott

Policy, Organisation Security Policy, Information Lifecycle Management Policy and Corporate Governance Policy.

- Ensuring there are appropriate contractual arrangements with staff, suppliers, data users and other organisations surrounding the appropriate handling, transmission, use and any other processing of data.

II. **Your arrangements surrounding maintaining confidentiality and complying with data protection law**, including:

- Having clear arrangements in place to inform service users about the uses to which their information might be put through general communications to service users as well as targeted communications for specific groups or to support specific initiatives. This is a requirement to ensure the “fair processing” provisions in the Data Protection Act 1998 are met.
- Providing clear guidance to staff about how information should be handled, including the legal framework and the circumstances under which confidential information can be disclosed; the systems and processes for protecting personal information; who to approach for advice; and possible sanctions for breach of confidentiality or data loss.
- Regularly conducting audits to ensure policies and procedures are being followed.
- Ensuring that confidentiality is protected through the use of pseudonymisation and anonymisation techniques when appropriate

III. **Your arrangements for establishing and maintaining appropriate information security**, to ensure information assets are appropriately protected, such as:

- Conducting formal information security risk assessments to ensure your organisation identifies, implements and manages controls to monitor and reduce the risk to the organisation, its person confidential information and critical Information Assets.
- Having appropriate incident management and reporting procedures to deal with loss of patient/service user data, a breach of confidentiality or other effect on the confidentiality, security or quality of patient/service user information. All incidents and near-misses should be reported, recorded and appropriately managed so that where incidents do occur, the damage from them is minimised and lessons are learnt from them.

2.1 New Arrangements

Table 1 below provides additional details on the new arrangements surrounding CCGs, CSUs, DMICs and Local Authority Public Health teams.

Table 1: New arrangements for DMIC/CCG/CSUs and Local Authority Public Health

Organisation	New Arrangements
Clinical Commissioning Groups, Data Management and Integration Centres and Commissioning Support Units	The business model for CCGs CSUs and DMICs, as designed by the NHSCB, is illustrated in Figure 1. Under this model: • DMIC staff will be seconded to and managed by the HSCIC. As part of the HSCIC, DMICs will be legally entitled to receive and process PCD through the powers vested in them by the Health and Social Care Act 2012 as directed by the Secretary of State or the NHS Commissioning Board. • No organisation, including DMICs, should pass PCD **for a purpose other than direct care** to other bodies without the appropriate legal cover in place. This means that no care provider or DMIC will be able to pass confidential data to CSUs or CCGs for commissioning support without consent or appropriate s.251 support for the relevant purposes and data flows. A national application for s.251 support for limited access to person confidential information for a specific list of business purposes by ASHs is currently being developed by the NHSCB and will be shared at forthcoming Regional Workshops. • The NHS CB business model does not anticipate that CCGs will require PCD but that they will receive the outputs of analyses and business intelligence from CSUs. However, if CCGs rather than CSUs are undertaking the purposes included within the s. 251 support they will need to ensure they meet the standards of an ASH in order that they can receive the data. Where local business models have adopted a different approach they will need to make separate arrangement for obtaining s. 251 support.
Local Authority Public Health	A national application for s.251 support for limited access to PCD for a specific list of business purposes by ASHs is currently being developed. This will include the flows to LAPH and to Public Health England.

In this time of transition, you will also need to consider whether any of your existing arrangements need to be reviewed including:

- Whether any systems changes are needed
- Ensuring you comply with the NHS IG Statement of Compliance in your new organisation
- Whether you need to inform data suppliers/receivers of any contact detail changes

The National Information Governance Board (NIGB) Transition Guidance includes an action checklist to help you ensure that appropriate governance is in place during the transition period (http://www.nigb.nhs.uk/pubs/guidance/NIGB%20Transition%20Guidance%2015%20November%20web%20version.doc - see References)

2.3 Data flows

The national data flows are presented as a spreadsheet containing the following information:

- The common name and description of the data flow.
- The sender and recipient of the data: NB some data flows span several organisations in a number of steps. Each step is represented as a separate row in the spreadsheet.
- Whether the flow can contain PCD, should be row-level, aggregate, etc.
- Whether the flow is nationally or locally defined.
- The legal basis for any person confidential flows under the NHSCB commissioning model.

Please note that the set of data flows in the spreadsheet is not a complete list of all national data flows. It currently includes those for which we have the full details. We have some incomplete details about other data flows and we will continue to gather intelligence on these and publish them in the next iteration of this spreadsheet.

In order to identify the flows relating to your organisation, you should do the following:

1. Select the flows relevant to your organisation type using the filtering mechanism in Excel
   EITHER
   To **see the flows coming to your organisation type (inbound flows)** use the drop-down filter in the dark blue cell in the headed row labelled “To” (To select your organisation type, clear all the checkboxes in the organisation type list other than your own, which should remain checked).Excel will then display only the rows where you are the data recipient
   OR
   To **see the flows you will be sending (outbound flows)** use the dropdown filter in the dark blue cell in the header row labelled “From” (To select your organisation type, clear all the checkboxes in the organisation type list other than your own, which should remain checked.) Excel will then display only the rows where you are the data sender

2. You can then apply further filters to display:
   a. Flows to or from particular organisation types
   b. Flows with a particular level of anonymisation
   c. Either local or nationally defined flows

3. When you have completed the search, remember to **clear all the filters** before starting a new search.

If you have any questions about any such flows, then please contact us, using the contact information on page 5.

3. Legal basis for data flows in the NHSCB commissioning business model

3.1 Processing Data in DMICs

Please note that although PCD is referred to in a number of the flows, people should ensure that they use the minimum amount of identifiable information possible to enable that flow, in line with guidance and legislation such as the Caldicott Guardian Principles and the Data Protection Act 1998.

The NHSCB has made arrangements with the HSCIC to ensure that the responsibility and authority for such processing will rest with the HSCIC. The key purposes for which DMICs require PCD are data quality assurance and data linkage.

Those staff from DMICs who process PCD within the DMIC are to be seconded into the HSCIC and therefore will:

- Operate under the HSCIC IG and information security policies; and
- Process data in an ASH established within the DMIC infrastructure.

Under these arrangements the DMICs, under the control of the HSCIC, are able to receive and process PCD under the powers vested in the HSCIC through the Health and Social Care Act 2012.

In most circumstances the HSCIC (with its responsibility for the DMICs) will be the data controller (or joint data controller) of the data as defined in the Data Protection Act 1998. In rare circumstances, another organisation may request that data is collected and analysed in such a specific way that the HSCIC/DMIC may be considered to be the data processor not the controller.

4. Processing Data in CSUs or NHSCB Area Teams

It is important to recognise that as CSUs and NHS CB Area Teams are not separate legal entities from the NHSCB, they cannot themselves be data controllers or processors - this responsibility rests with the NHSCB. However, considerable delegated authority has been provided to these units and teams, enabling them to function independently, but they are not in fact legally independent.

In order to be compliant with HSCA 2012 the anticipated business model is to allow in most cases only aggregate or pseudonymised information to flow from DMICs to CSUs or NHS CB Area Teams. This data may be used as desired by the recipients subject to them working within the limitations of ASHs. However, it is also recognised that there will be a limited number of purposes that will require data that includes identifiers. The lawful basis to enable PCD to flow for these specific purposes will be established through a national application seeking s251 support.

The basis on which the support will be sought will be that:

- It is for one or more of the limited range of named purposes supported by the NHS (Control of Patient Information) Regulations 2002
- It is a temporary requirement to allow more robust arrangements to be embedded into current practices which will further reduce or remove the need to process PCD

- Any organisation undertaking such processing will be or will be working towards becoming an ASH. The full definition of an ASH will be issued through the HSCIC Code of Practice for the use of Confidential Information but an outline is provided in Appendix 1.

All data flowing from the HSCIC and DMICs should be underpinned by appropriate data sharing agreements which clarify the data controller responsibility; the purpose for which the data is be used; the information governance and information security requirements to be met and any restrictions relating to the publication or onward sharing of the data.

5. Processing Data in CCGs

It is not anticipated that CCGs will need PCD but that business intelligence (i.e. indicators and aggregate information) will flow from CSUs to CCGs. These flows should be underpinned by appropriate data sharing agreements which clarify the purpose for which the data can be used; the information governance and information security requirements to be met and any restrictions relating to the publication or onward sharing of the data.

In some cases, CCGs may not have commissioned a CSU to provide analytical support and so may need to receive data directly from a DMIC. The national s.251 support will still apply to the CCG as long as the conditions for the support are met i.e.:

- The data required and the purposes for which the data are required are consistent with those for which the national support has been sought; and
- The CCG has been accredited or is seeking to become an ASH.

The national arrangements for s251 support will **not** provide a legal basis for the CCG to receive PCD or undertake processing as if they were a DMIC themselves, nor if they elect to contract that activity to an independent third party. CCGs will be required to seek their own legal basis for such activities - if that is a requirement of their local arrangements.

Appendix 1: References

A comprehensive reference library on the information governance and security standards that apply in health and social care (indexed by organisation) is available here: https://www.igt.connectingforhealth.nhs.uk/KnowledgeBaseOrganisationChooser.aspx

In particular, we would like to draw your attention to the following references which provide useful, general guidance:

- NHS Care Record Guarantee for England: the commitment that the NHS will use healthcare records in ways that respect personal rights and promote health and wellbeing.
- Social Care Record Guarantee for England: The Guarantee explains to service users how the information they provide to social care staff is used and what control they can have over this. It complements the NHS Care Record Guarantee for England.

Management structures and organisational arrangements

- Checklist for Reporting, Managing and Investigating Information Governance Serious Untoward Incidents - January 2010 (PDF 224Kb): This guidance has been approved by all SHA IG leads and the DH Information Governance Policy Team and should be used in conjunction with the previously provided national guidance on the management of Serious Untoward Incidents (now Serious Incidents Requiring Investigation) and any local guidance on SUIs provided by the local SHA. (Due to release update in IGT V11 release June 2013)
- Resources for Caldicott Guardians, including job descriptions and information on training http://www.connectingforhealth.nhs.uk/systemsandservices/infogov/caldicott/caldresources
- NHS Information Risk Management pages: The Information Governance Policy team has published guidance aimed at those responsible for managing information risk within NHS organisations, including Senior Information Risk Owners (SIROs) and Information Asset Owners (IAOs). It reflects Government guidelines and is consistent with the Cabinet Office data handling report.
- http://www.connectingforhealth.nhs.uk/systemsandservices/infogov/security/risk/inforiskmgtgpg.pdf: The NHS Information Risk Management guidance on roles and responsibilities, including the Senior Information Risk Owner role.

Handling confidential information

- The NHS Codes of Practice, including the code of practice on handling confidential information http://www.connectingforhealth.nhs.uk/systemsandservices/infogov/codes
- Quality, Innovation, Productivity and Prevention (QIPP) - Guidance on Data Sharing Issues within Risk Stratification http://www.connectingforhealth.nhs.uk/systemsandservices/qipp/library/datasharing.pdf

- Guidelines on use of encryption to protect person identifiable and sensitive information - December 2008 (Word 99Kb): includes an explanation of the tools provided within applications provided by NHS CFH for encrypting removable media and provides guidance on potential encryption tools organisations should consider for systems under local NHS organisation control.
- Security of NHS patient data shared for research purposes - July 2008 (PDF 23Kb): The importance of effective information security has been highlighted in recent months through well publicised data handling failures in a range of different UK organisational settings. The Cabinet Office has completed a review of public sector data handling and has established a comprehensive range of minimum security standards. Consequently, NHS guidance for the protection of patient information has been extended and strengthened in order to respond robustly to these requirements.
- Information Commissioner's Office - Data Sharing Code of Practice. http://www.ico.gov.uk/for_organisations/data_protection/topic_guides/data_sharing.aspx
- HM Government (2009). Information Sharing: Further guidance on legal issues. https://www.education.gov.uk/publications/eOrderingDownload/Info-Sharing_legalissues.pdf
- Ministry of Justice (2003). Public Sector Data Sharing: Guidance on the Law. http://www.justice.gov.uk/downloads/guidance/freedom-and-rights/datasharing/annex-h-data-sharing.pdf
- Information Commissioners Office – Privacy Impact Assessment Handbook http://www.ico.gov.uk/for_organisations/data_protection/topic_guides/privacy_impact_assessment.aspx
- Information Commissioners Office – Anonymisation: Managing Data Protection Risk Code of practice http://www.ico.gov.uk/news/latest_news/2012/new-anonymisation-code-sets-out-how-to-manage-privacy-risks-and-maintain-transparency-20112012.aspx

IT Standards and Information Security

- Information Standards Board for Health and Social Care - Approved standards http://www.isb.nhs.uk/library/approved.
- The Interoperability Toolkit (ITK) provides a growing suite of national specifications to support standardisation of the information flows between IT systems. The QIPP Digital and ITK teams are developing new ITK specifications to support electronic care co-ordination. This fact sheet explains what is already available, and what is being developed. http://www.connectingforhealth.nhs.uk/systemsandservices/qipp/library/carecoordtk-fs.pdf/view?searchterm=national%20data%20flows
- Good Practice Guidelines: Transfer of batched person-identifiable data - December 2007 (Word 813Kb): covers the transfer of batched person identifiable data by means of portable electronic media, including tapes; floppy discs; removable hard discs; laptop & handheld computers; optical discs - DVD & CD-ROM; solid state memory cards; memory sticks and pen drives
- Joint guidance on protecting electronic patient information (PDF 82Kb): guidance for all health care staff, produced by the British Medical Association and NHS Connecting for Health.

- Infrastructure Security Team (N3 connection required): the Infrastructure Security Team aims to provide security information, advice and guidance which will enable organisations to see real benefits from security implementation, reduce the operational cost of insecure systems and advise on the risks relating to security controls to prevent implementation of costly and ineffective controls.
- IG Statement of Compliance: the IGSoC is the agreement between NHS CFH and Approved Service Recipients that sets out the information governance policy and terms and conditions for use of NHS CFH services through an N3 connection.

Transition arrangements including governance arrangements

- DH. 2012. Summary of Local Public Health Intelligence https://www.wp.dh.gov.uk/publications/files/2012/09/Public-health-intelligence-all-factsheets.pdf – A factsheet detailing local government requirements for public health intelligence capacity and services and outlining steps that need to be taken to secure such capacity and services such as addressing IT and information governance architecture issues.
- The Health and Social Care Act 2012
- NIGB Transition Guidance, which includes an action checklist to ensure that appropriate governance is in place during the transition period http://www.nigb.nhs.uk/pubs/guidance/NIGB%20Transition%20Guidance%2015%20November%20web%20version.doc. The action points are:
  - Map current and new information assets and both internal data flows and transfers of information externally.
  - Ensure that you understand the nature and extent of personal data you are responsible for; and your responsibilities as a data controller.
  - Be clear about which organisations are data controllers and which are data processors.
  - Ensure that there are appropriate contractual arrangements with NHS Care providers and those providing NHS funded care.
  - Ensure that there is a legal basis for processing both personal and confidential data.
  - Maintain oversight and accountability of interim arrangements.
  - Ensure that all records both health and corporate are managed appropriately particularly for organisations that are closing.
  - Ensure secure data transfer.
  - New organisations such as Clusters and Clinical commissioning groups must ensure they understand the constraints in which they need to operate during transition in relation to their accountability to PCTs, or SHAs in relation to SHA Clusters, and the need to adhere to Information governance requirements.
  - Ensure continuity of service in relation to Registration Authority functions and the administration of Role Based Access Controls, including the independent sector and local authorities.
  - Ensure you inform patients and the public about changes in how services are to be delivered and how their personal and confidential information will be processed and managed.
  - Ensure you manage consent and dissent to respect patients choices.

- Use de-identified data for secondary uses or ensure there is a secure legal basis for processing personal data.
- Ensure you manage conflicts of interest effectively.

Requirements for Accredited Safe Havens

The HSCIC is leading on work to establish clear and robust accreditation requirements for organisations wishing to become, or to host one or more, Accredited Safe Havens (ASH).

An ASH will have support in law provided under s251 of the NHS Act 2006 that will enable it to process data that might be personal confidential data in the public domain but which generally isn't PCD when processed in a controlled environment. An ASH may also process some data that might readily identify individuals if misused to deliberately attempt to identify a person (e.g. NHS Number or Postcode) but will be bound by regulations and contract or agreement to refrain from activity that risks an individual being identified and prevents the associated data from being disclosed outside of the ASH.

Requirements for accreditation are likely to include:

- appropriate techniques for de-identification of data , the use of 'Privacy Enhancing Technologies' and re-identification risk management
- a published register of data that flows into or out of the safe haven including a register of all datasets held
- clear governance arrangements that include, but are not limited to policies on ethics, technical competence, publication, limited disclosure/access, regular review process and a business continuity plan including disaster recovery.
- clear operational control including human resource procedures for information governance, including the use of role based access controls, confidentiality clauses in job descriptions, effective education and training and contracts
- achieving ISO27001 or a high level of audited performance using the NHS Information Governance Toolkit
- clear policies for the proportionate use of data including competency at undertaking Privacy Impact Assessments and the publication of these including a strong risk and benefit analysis
- a standard template for data sharing agreements and other contracts which conform to legal and statutory process
- knowledge management including changes in the law and a joined up approach with others working in the same domain
- explicit standard timescales for keeping data sets including those that have been linked, which should be able to support both cohort studies and simple 'one-off' requests for linkage.