CONNECTED HEALTH CITIES:

GUIDANCE ON DATA USE AND DATA SHARING

Document Management

Revision History

Version	Date	Summary of Changes
0.1	01/08/2016	First draft for internal review

Reviewers

This document must be reviewed by the following people:

Reviewer name	Title / Responsibility	Date	Version

Approved by

This document must be approved by the following people:

Name	Signature	Title	Date	Version

Contents

Foreword

The guidance document brings together relevant national advice and guidance to assist the Connected Health Cities to implement appropriate Information Governance Controls that meet current legislative and national policy requirements when establishing data sharing arrangements in support of the projects that are sponsored by the Connected Health Cities.

Introduction

Background

1. Connected Health Cities is a pilot project for Health North which aims to use patient and population data to generate innovations that can deliver more effective and efficient health and social care.
2. Obtaining agreement to share data is often beset with challenges as organisations providing the data seek to assure themselves that such data sharing and processing is both lawful and ethical and that the receiving organisation will manage and protect the shared data appropriately and use it only for the agreed purpose.

Purpose of Document

3. The purpose of this document is to provide guidance for Connected Health Cities partners on how to address key information governance issues related to information sharing for Connected Health Cities Projects between partner organisations.
4. The guidance has therefore has been designed to support data sharing for the purposes of care pathway analysis, research and direct patient care. It is targeted at anyone involved in considering the data sharing requirements associated with Connected Health Cities projects.
5. Adoption of this guidance by those requesting that data be shared for a Connected Health Cities project will provide a consistent and standardised approach to Information Governance issues and provide assurance to those organisations providing data that appropriate controls have been put in place and that data sharing is lawful and ethical.

Review

6. This guidance and the associated Data Sharing Contract and Data Sharing Agreement will be reviewed by Connected Health Cities on an annual basis or because of a change to either applicable legal frameworks or national policy.
7. Any proposed changes will be notified to partners in writing in advance of their implementation.

Interaction with Current Local Arrangements

8. The guidance provides advice on the steps to be taken when establishing data sharing arrangements for projects that are supported by Connected Health Cities.
9. These arrangements supplement rather than replace existing local arrangements for data sharing and are to be used between all partner organisations for Connected Health Cities projects only. However, they should be broadly consistent with local data sharing arrangements and agreements.
10. The arrangements require organisation level sign up and approval by local Caldicott Guardians and/or Senior Information Risk Owners. However, it is intended that approval should be straightforward as the Caldicott Guardian and Senior Information Risk owner can be assured that appropriate controls are in place when the guidance has been followed.

11. Early engagement with local Caldicott Guardians and IG leads at organisations involved in the proposed data sharing arrangements is recommended.

Definition of Purpose

12. For each data flow within a project it is essential to determine the purpose for which the data is to be shared:

    i Direct Care

    ii Research

    iii Other purposes including care pathway analysis, service planning and service evaluation

13. Clarity about all expected purposes for data sharing should be established at the outset for each data sharing arrangement. If there is more than one purpose for sharing the data the requirements set out within this guidance will need to be met for each purpose. If there is a change in purpose during the course of a project, these considerations must be reviewed and any changes established.

Direct Care

14. Deciding on whether the proposed activities should be considered as being for direct (individual) care purposes is not always straightforward.

15. The Caldicott2 Review[1] defined direct care as a clinical, social or public health activity concerned with the prevention, investigation and treatment of illness and the alleviation of suffering of individuals. It includes supporting individuals' ability to function and improve their participation in life and society. It includes the assurance of safe and high quality care and treatment through local audit, the management of untoward or adverse incidents, person satisfaction including measurement of outcomes undertaken by one or more registered and regulated health or social care professionals and their team with whom the individual has a legitimate relationship for their care.

16. Activities (and any data sharing in support of such activities) can be described as direct (individual) care purposes only where they are carried out by a regulated health or social care professional and their teams, with whom the patient has a legitimate relationship. Any data that is shared must be relevant for the care, must be kept confidential and can only be shared if the patient has been informed and has not objected. A key issue will be whether the health or social care professional that it is proposed the data should be shared with has a legitimate relationship with the patient and whether the patient is aware that the data is being shared. This is of particular importance for clinical networks that propose to share data across organisational boundaries.

17. A patient has not been given an opportunity to object to data sharing if they are unaware that it is taking place.

1.

[1]https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/192572/2900774_InfoGovernance_accv2.pdf

18. The Health and Social Care's, HSCIC's, guide to confidentiality and associated reference document can assist in determining whether the proposed activity should be considered to be direct (individual) care.

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

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

19. If there is any doubt about whether the proposed activities can be considered as direct (individual) care further advice should be sought from the local Caldicott Guardian or the local IG lead.

Research

20. There is no clear definition of what constitutes research, it can take many forms, from clinical trials of drugs through to qualitative research studies.

21. Generally, research is considered to be the attempt to derive new knowledge by addressing clearly defined questions with systematic and rigorous methods. The Health Research Authority provides a tool to assist researchers in determining if their project should be considered to be research.

    http://www.hra-decisiontools.org.uk/research/

22. Where the purpose is determined as research the project will require ethical approval and an application must be made through a Research Ethical Committee (REC). There are a range of bodies which have roles in regulating different aspects of health research. More information can be found on the HRA website.

    http://www.hra.nhs.uk/research-community/before-you-apply/determine-which-review-body-approvals-are-required/

Other purposes

23. There are many other purposes for sharing data. Those of most relevance to the CHCs include audit, service planning, service evaluation.

24. Audits are designed to find out whether the quality of a service meets a defined standard.

25. Service Planning aims to improve health service delivery and/or system performance to better meet the health needs of a population. It comprises the process of aligning the delivery of existing health services to meet the changing patterns of need and use of services.

26. Service Evaluation is designed to answer the question "what standard does this service achieve"?

Specification of the Data Requirements

Identification of the type of data required.

27. A key issue in determining the type of data that is sufficient for the purpose will be the protection of the privacy and confidentiality of the patient.

28. For direct (individual) care purposes, it is likely that **personal confidential data** (personally identifiable data) will need to be shared: that is data which identifies the patient. Safe and effective care can usually only be provided where the health or social care professional who has a legitimate relationship with the patient can identify the patient they are providing care to.

29. However, for all other purposes including research, which benefits the community rather than an individual patient, it may be possible to use anonymous grouped data or de-personalised data (where data has been de-identified with appropriate controls on processing) rather than personal confidential data as set out in the following diagram from the HSCIC's Guide to Confidentiality.

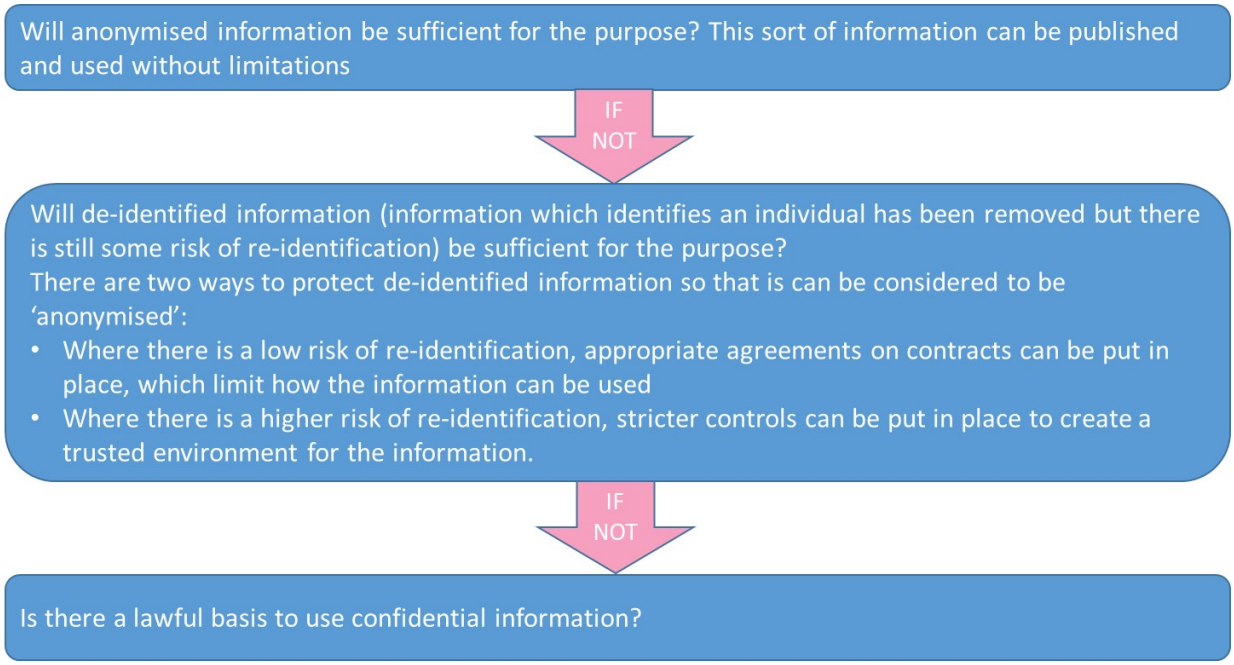

Figure 3: Identification of the type of data required from the HSCICs Guide to Confidentiality

30. **Anonymous grouped data** is data where the risk of a patient being identified is minimal. This is aggregated data where the small numbers have been suppressed.

31. It is the responsibility of the data provider to ensure that data is effectively anonymised before it is shared. For advice on how to anonymise data see the Information Commissioner's Office Anonymisation: Managing Data Protection Risk Code of practice.

https://ico.org.uk/for-organisations/guide-to-data-protection/anonymisation/

32. Because Anonymous Grouped Data is not detailed it may not always be sufficient for the purpose. However, it may be possible to use data that is **De-personalised data** (patient level data that has been de-identified or pseudonymised with appropriate controls on processing) rather than **personal confidential data (personally Identifiable data)**.

33. **De-identified data** is data where the patient identifiers have been removed: **pseudonymised data** is data where individuals are distinguished by using a unique identifier or pseudonym which does not reveal the 'real world' identity of the patient.

34. There is still some risk of re-identification when using data that is de-personalised. These risks include the accidental identification of an individual by those accessing the data or deliberate re-identification by 'motivated intruder' within the receiving organisation or by someone hacking the database. Unless there are robust controls associated with how the data is stored and can be used it must be considered to be personal confidential (personally identifiable) data. However, the privacy of the patient is protected through these controls. [See Section: Secure Systems – Page 26]

35. Only as a last resort should personal confidential (personally identifiable) data be used and this will require an appropriate legal basis. [See Section: Lawful Basis for Data Sharing and Processing – Page 12]

Identification of the amount of data to be shared

36. Where patient level data (Personally Identifiable or De-personalised data) is required it is essential to assess and justify the amount of data that is relevant for the purpose. Consideration should be given to both:

    - The number of patient records that will be required.
    - The number of data fields that will be required.

37. Data should only be shared about those patients that will be involved in the project. So, for example, providing access to a database of all patients where only some are involved in the project is not acceptable.

38. In addition, the data fields to be shared should only be those that are relevant to the project. Sharing the whole patient record where only certain aspects of their care is relevant to the project is not acceptable.

39. The data sharing arrangements should be explicit about the amount of data that will be shared.

Data Quality

40. Data sharing arrangements should be established so that data quality can be maintained to the standard required for the purpose.

41. Any known data quality issues should be declared by the data provider when the data is shared.

Lawful Basis for Data Sharing and Processing

42. Any data sharing that involves the sharing or processing of **personal confidential (personally identifiable) data** requires a lawful basis to enable the organisation that is providing the data both to comply with the Data Protection Act and to meet their duty of confidentiality.

Data Protection Act

43. The Data Protection Act sets out eight key principles for processing personal data.

I. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless –
(a) at least one of the conditions in Schedule 2 is met, and
(b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

II. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

III. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

IV. Personal data shall be accurate and, where necessary, kept up to date.

V. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

VI. Personal data shall be processed in accordance with the rights of data subjects under this Act.

VII. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

VIII. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

44. The conditions set out in Schedules 2 and 3 to the Data Protection Act are known as the "conditions for processing". Organisations processing personal data need to be able to satisfy one or more of these conditions.

45. Further information can be found in the Information Commissioner's Office Guide to Data Protection.

https://ico.org.uk/for-organisations/guide-to-data-protection/

46. Those projects that have already undertaken a Privacy Impact Assessment [See Section: Privacy Impact Assessment – Page 21] will have established that their proposed data sharing arrangements comply with the principles of the Data Protection Act.

47. The first data protection principle requires, among other things, that one or more "conditions for processing" in relation to the processing of personal data must be satisfied. Many (but not all) of these conditions relate to the purpose or purposes for which the data is to be used.

48. The conditions for processing that need to be met are more exacting when the information being processed is sensitive personal data, such as information about an individual's health.

49. Being able to satisfy a condition for processing will not on its own guarantee that the processing is fair and lawful – fairness and legality must still be looked at separately.

50. The conditions for processing are set out in Schedules 2 and 3 to the Data Protection Act. Unless a relevant exemption applies, at least one of the following conditions must be met whenever you process personal data:

    - The individual whom the personal data is about has consented to the processing.
    - The processing is necessary:
        a) in relation to a contract which the individual has entered into; or
        b) because the individual has asked for something to be done so they can enter into a contract.
    - The processing is necessary because of a legal obligation that applies to you (except an obligation imposed by a contract).
    - The processing is necessary to protect the individual's "vital interests". This condition only applies in cases of life or death, such as where an individual's medical history is disclosed to a hospital's A&E department treating them after a serious road accident.
    - The processing is necessary for administering justice, or for exercising statutory, governmental, or other public functions
    - The processing is in accordance with the "legitimate interests" condition

51. Because health data is sensitive personal data under the DPA, at least one of several other conditions must also be met before the processing can comply with the first data protection principle:

    - The individual whom the sensitive personal data is about has given explicit consent to the processing.
    - The processing is necessary so that you can comply with employment law.
    - The processing is necessary to protect the vital interests of:
        - the individual (in a case where the individual's consent cannot be given or reasonably obtained), or
        - another person (in a case where the individual's consent has been unreasonably withheld).

- The processing is carried out by a not-for-profit organisation and does not involve disclosing personal data to a third party, unless the individual consents. Extra limitations apply to this condition.
- The individual has deliberately made the information public.
- The processing is necessary in relation to legal proceedings; for obtaining legal advice; or otherwise for establishing, exercising or defending legal rights.
- The processing is necessary for administering justice, or for exercising statutory or governmental functions.

52. The Information Commissioners Office provide a statutory guide to Data Sharing

https://ico.org.uk/for-organisations/guide-to-data-protection/data-sharing/

Common Law Duty of Confidentiality

53. A duty of confidentiality arises when one person discloses information to another (for example a patient to their clinician) in circumstances where it is reasonable to expect that the information will be held in confidence. It is a legal obligation which is derived from case law rather than being set out in law like the Data Protection Act. It is also a requirement established within professional codes of conduct and is included within NHS employment contract as a specific requirement linked to disciplinary procedures.

54. The general position is that if information is given in circumstances where it is expected that a duty of confidence applies, that information cannot normally be disclosed without the information provider's consent.

55. In practice, this means that all patient information, whether held on paper, computer, visually or audio recorded, or held in the memory of the professional, must not normally be disclosed without the consent of the patient. It is irrelevant how old the patient is or what the state of their mental health is; the duty still applies.

56. Three circumstances making disclosure of confidential information lawful are:

- where the individual to whom the information relates has consented;
- where disclosure is in the public interest; and
- where there is a legal duty to do so, for example a court order.

57. Therefore, under the common law, a healthcare provider wishing to disclose personally identifiable data to anyone outside the team providing care should normally first seek the consent of that patient as described below.

58. If a disclosure is made which is not permitted under common law the patient can bring a legal action not only against the organisation but also against the individual responsible for the breach.

59. In certain circumstances, it may be possible to seek Section251 support. This is described below and in effect sets aside the data provider's duty of confidentiality.

Duty of Care

60. 'Duty of care' describes the obligations implicit in the roles of every health and social care worker. The duty of care requires staff to keep accurate and contemporaneous records of their work and share information appropriately with those involved in an individual's care.

61. However, an important element of the duty of care is to protect confidentiality and to respect the preferences of patients and service users about information sharing decisions. Balancing these two requirements is important and will shape how services are designed and managed.

62. In order that health and social care organisations can provide a comprehensive service they must ensure that they have identified all partner organisations that might contribute to care and put in place the necessary information sharing agreements, policies, procedures, fair processing and communications arrangements and technical measures to enable staff to share information securely and appropriately.

63. Information is shared because there is a duty of care and the default position should be that information is shared when it is likely to contribute to improved care and outcomes for an individual and where the individual is aware of the sharing and hasn't objected. Policies, procedures and systems should be designed around this principle.

64. Further information on the duty of care can be found in advice from the Information Governance Alliance:

    https://www.igt.hscic.gov.uk/Resources/The%20Duty%20of%20Care.pdf

Duty to Share

65. The Health and Social Care (Safety and Quality) Act 2015 introduces a new legal duty requiring health and adult social care bodies to share information where this will facilitate care for an individual. The Information Governance Alliance has published guidance that explains what this new legislation requires and provides a clear message that subject to the preferences of the individuals concerned, sharing for the care of individuals is a requirement, not an option. The guidance can be found at:

    http://systems.hscic.gov.uk/infogov/iga/resources/dutytoshare.pdf

Patient Consent

66. Patient consent is the approval or agreement of the patient that their data can be shared for a specific purpose or range of purposes. For consent to be legally valid the patient must be informed, must have the capacity to make the decision to provide consent and must give consent voluntarily. Therefore, a patient should know and understand how their data is to be used and shared and should understand the implications of refusing to allow the data sharing, especially where this might affect the care they receive.

67. There are two types of consent to meet the requirements of the Common-Law Duty, – explicit and implied. Implied consent as described below can only be relied upon in the context of direct or individual patient care. For all other data sharing purposes that are relying on patient consent explicit consent will be required.

68. Where patient consent cannot be gained for whatever reason (other than a lack of capacity) a statutory provision such as support under the NHS (Control of Patient Information) Regulations 2002, commonly referred to as Section 251 support is required. This is described below.

Implied Consent

69. Implied consent can only be relied upon as a lawful basis when personal confidential data is being shared for direct or individual care purposes. Implied consent is an unwritten agreement between the patient and the professionals who provide their care that allows data sharing to take place as long as the data that is shared is relevant for their care, it is kept confidential, and as long as the patient has not objected.

70. Implied consent is a form of consent which is only valid when a reasonable person would believe that consent had been given, although no direct, express or explicit words of agreement had been uttered and no other form of evidence exists. However, implied consent is being relied upon it should not be seen as an easy way out or used as a euphemism for "doing nothing".

71. For implied consent to work there has to be some action taken by the consenting individual from which their consent to the data sharing can be inferred. This might for example be by accepting a care referral, attending an appointment or not objecting when asked if they are happy for information to be viewed. The key point, however, is that when taking this action, it is reasonable to believe that the individual understands that he/she is also agreeing to information about them being shared.

72. Draft guidance on implied consent from the Information Governance Alliance can be found:

    http://systems.hscic.gov.uk/infogov/iga/consultations/iclimits.pdf

73. Even when sharing for direct (individual) care purposes reliance on implied consent has limitations and may not always be sufficient for example for:

    - Sharing the patient's whole care record rather than sharing only relevant data.
    - Sharing across organisational boundaries or with healthcare professionals that the patient may not expect to be part of the care team (and to have a legitimate relationship with the patient): the patient should be told of a proposed communication or data sharing and provided with an opportunity to object. [See Information for Patients Page 25]

74. If there is any doubt about whether implied consent can be relied upon further advice should be sought from the local Caldicott Guardian or the local IG Lead or explicit consent should be obtained.

75. NOTE: Audit of the care provided, when conducted by a member of the care team, that does not require disclosure of personal confidential data to any person that would not have the need to view the data as part of their role, can also rely on implied consent as a lawful basis for processing the

data. Patients should be informed that their data may or will be used for an audit function and should be given an opportunity to object.

Explicit Consent

76. Explicit consent can be given in writing or verbally, or conveyed through another form of communication such as signing. A patient may have capacity to give consent but may not be able to write or speak. Explicit consent is required when sharing data with staff who are not part of the team caring for the individual. It may also be required for a use other than that for which the data was originally collected.

77. A record must be kept of any explicit consent decision and processes.

78. When seeking patient consent, it is important to ensure that consent is sought for all aspects of the data sharing and for all purposes which the personal confidential data will be used for. Explicit patient consent for data to be used for one research project is not sufficient for it to be used for another. The wording of the patient consent and whether or not you wish to seek consent for multiple purposes should be carefully considered when designing the 'consent model'.

Capacity to Consent

79. In seeking consent, it is important to assess the patient's capacity to understand the information being given to them and therefore to make an appropriate decision with regards to their data being shared. It should not be assumed that because a patient lacks capacity to make a decision on a particular occasion, they lack capacity to make any decisions at all, or will not be able to make similar decisions in the future.

80. Advice on assessing capacity is provided in the Codes of Practice that accompany the Mental Capacity Act 2005 which can be found at:

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/224660/Mental_Capacity_Act_code_of_practice.pdf

Section 251 support

81. In the rare cases where patient confidential data is required but gaining explicit consent is impractical, legislation is in place that allows personal confidential data to be processed or shared for medical purposes including for example research, service planning and audit.

82. Regulations under Section 251 of the NHS Act 2006 allows for the Secretary of State for Health to make regulations that set aside the common law duty of confidentiality for defined medical purposes. The regulations that enable this power are called the Health Service (Control of Patient Information) Regulations 2002. This is commonly referred to as Section 251 support or approval.

83. Section 251 support provides a secure basis in law for the processing of personal confidential data for medical purposes other than direct (individual) care where patient consent cannot be gained. Section 251 enables the common law duty of confidentiality to be overridden and enables disclosure of personal confidential data where it is not possible to use anonymised data and where seeking consent is not practical.

84. Applications for Section 251 are made via the Health Research Authority to the Confidentiality Advisory Group. Research Applications should be made using an IRAS form, non-research applications should be made using a S251 form. Details of how to make an application can be found at:

    http://www.hra.nhs.uk/research-community/applying-for-approvals/confidentiality-advisory-group-cag/

85. Where the data is required for a research project the IRAS form enables the application to be made to a Research Ethics Committee and the Confidentiality Advisory Group using the same form. A separate application form is provided for non-research projects.

86. All processing including that which relies upon Section 251 support must adhere to the Data Protection Act

Patient Objections or Withdrawal of Consent

87. A patient may decide that they wish to object to their data being shared even for direct (individual) care purposes. A patient may also decide that they wish to withdraw explicit consent previously given for data sharing to take place. In all but the most extreme cases (for example where the data must be shared for legal reasons such as notifiable diseases) these patient objections and consent withdrawal should be honoured.

88. How such objections are managed by the project will depend on the way in which data is being shared or accessed. Where feasible it may be beneficial to adopt the local organisational processes for handling patient objections.

89. Where it is necessary to establish project specific arrangements managed directly by the project team it will be important to ensure the identity of the person registering an objection.

Data Controller

90. Any data sharing arrangements which involve the processing or personal confidential data will need to clearly state whether the recipient of the data will be acting as Data Controller or Data Processor and the recipient must be registered with the Information Commissioners Office.

The Data Protection Act defines these terms as:

Data Controller *means a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are or are to be processed*

Data Processor *in relation to personal data means any person (other than an employee of the data controller) who processes the data on behalf of the data controller.*

Processing *in relation to information or data means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data including:*

- *Organisation, adaption or alteration of the information or data*
- *Retrieval, consultation or use of the information or data*

- Disclosure of the information or data by transmission, dissemination or otherwise making available, or
- Alignment, combination, blocking, erasure or destruction of the information or data.

91. Determination of which organisation is the data controller is important as they will have data protection responsibilities and will take responsibility should there be a data breach. It may be appropriate for organisations to be joint data controllers e.g. in a clinical network supporting a specific care pathway where access to data from several organisations is allowed on a single system.

92. It is not appropriate to agree that an organisation is the data controller unless they are acting as such and are able to exercise overall control over the purpose for which and the manner in which the personal confidential data is processed.

93. The Information Commissioners Office provides further guidance on the difference between the data controller and data processor.

    https://ico.org.uk/media/about-the-ico/documents/1042555/data-controllers-and-data-processors-dp-guidance.pdf

94. The Information Governance Alliance has also provided guidance to assist in identifying the data controller(s) responsible for personal data in a shared environment. The Data Protection Act 1998 sets out clear responsibilities that must be met by data controllers, however, in complex data sharing situations it may not always be straightforward to determine who they are. In general, bodies processing data about identifiable individuals will be either a data controller for that data or a data processor. The term 'processing' refers to any activity involving the data: holding, viewing, sharing, deletion etc. Similarly, data sharing may involve an actual transfer of recorded data or simply relate to enabling information to be viewed by a third party. Further guidance can be found at:

    http://systems.hscic.gov.uk/infogov/iga/resources/datacontrol.pdf

Contractual Arrangements with Data Processors

95. In circumstances where data sharing is to occur between organisations using a system that is provided by a third party supplier (data processor) it will be important to ensure that appropriate contractual arrangements are put into place. These arrangements need to allow the additional organisations, if they retain data controller responsibility for their patients' data, to retain control and responsibility for this data. They need to assure themselves that the contract between the initial organisation and the third party supplier has sufficient robust IG controls in place to adequately protect the data.

96. Such assurance can be provided if the additional organisations have a separate contract with the third party supplier although this may not always be appropriate. If separate contracts are not appropriate the additional organisations should consider a back to back agreement with the original contracting organisation.

De-Personalised Data (De-Identified or Pseudonymised Data)

97. Where the data to be shared is de-identified or pseudonymised it is essential that appropriate controls are put in place through the Data Sharing Contract and Agreement to minimise the risk of re-identification of the patient. These controls will include:

    - An undertaking that the data will not be linked with any other data and/or
    - Role based access control to the data

98. If there is a data breach and the information becomes identifiable then the Data Protection Act would apply and the Information Commissioner's Office should be notified.

Privacy Impact Assessment

Recommended Approach

99. Delivery of the care pathway analysis and research projects supported by Connected Health Cities requires data about service users and patients to be processed. This processing can present significant risks to privacy which must be appropriately managed.

100. Any project supported by Connected Health Cities that intends to use personal data as defined by the Data Protection Act (see Appendix 4 - Glossary of Terms) should have conducted a Privacy Impact Assessment in line with the ICOs Code of Practice. This will include projects that intend to process data that is Anonymised in Context because there is a risk that it could become personal data.

101. If a Privacy Impact Assessment has not already been undertaken for the project itself it is recommended that a Privacy Impact Assessment is conducted with regard to the data sharing arrangements.

102. The Privacy Impact Assessment should be undertaken by, or on behalf of, the project's clinical lead or sponsor. The local Information Governance Team should be able to provide advice on conducting the Privacy Impact Assessment.

103. Any organisation that will supply or process the information should be consulted as part of the stakeholder engagement. Consultation should include the project's clinical lead, as well as the organisation's Caldicott Guardian and possibly the Senior Information Risk Owner.

104. The Privacy Impact Assessment will produce a series of recommendations to protect patient privacy. These actions must be allocated to a senior officer (who will have sufficient authority to ensure that the action is implemented) within the project or the partner organisation as appropriate.

Introduction to Privacy Impact Assessments

105. An individual's right to privacy is protected by the Data Protection Act 1988 (DPA) and within Article 8 of the European Human Rights Act. Privacy can be considered to be the right of an individual to keep data about themselves from being disclosed.

106. A Privacy Impact Assessment is a process which assists organisations to identify and minimise the privacy risks of new projects. It involves working with people within the lead organisation, within partner organisations and with the people affected. The intention is to evaluate the privacy implications of a project and assess the project's compliance with relevant legislation. Where potential privacy risks are identified it should be possible to identify actions to mitigate or reduce these risks without impacting on the objectives or realisation of the benefits of the project.

107. Completion of a Privacy Impact Assessment by Connected Health Cities projects ensures that that the proposed processes and procedures for handling personal confidential data are reviewed to ensure that they comply with legislation and best practice at an early stage in the project planning.

Where appropriate, stakeholder involvement in the PIA process increases awareness among those professionals involved in the project and creates a culture where maintaining privacy is a priority.

108. Although a Privacy Impact Assessment is not a legal requirement it is good practice and is an effective way to demonstrate how the processing of personal data complies with data protection legislation.

Conducting a Privacy Impact Assessment

109. The process of conducting a Privacy Impact Assessment has been described in a code of practice issued by the Information Commissioners Office.

https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf

110. There are two types of privacy: physical and informational. The code of practice, as with projects of the Connected Health Cities, is mainly concerned with Informational privacy: the ability of a person to control, edit, manage and delete data about themselves and to decide how and to what extent such data is communicated to others.

111. Consideration of the privacy risks of a project should be concerned with the risk of harm through the use or misuse of personal data. The code refers to risks arising such as personal data being:

- Inaccurate, insufficient or out of date
- Excessive or irrelevant
- Kept for too long
- Disclosed to those who the person it is about does not want to have it;
- Used in ways that are unacceptable or unexpected by the person it is about;
- Not kept securely.

112. The code of practice suggests that a Privacy Impact Assessment should be conducted for a range of projects or situations. Of relevance to Connected Health Cities are those that will introduce:

- A new IT system for storing and accessing personal data.
- A data sharing initiative where two or more organisations seek to pool or link sets of personal data.
- A proposal to identify people in a particular group or demographic and initiate a course of action.
- Using existing data for a new and unexpected or more intrusive purpose.
- A new database which consolidates data held by separate parts of the organisation.

Stages of a Privacy Impact Assessment

113. An overview of the Privacy Impact Assessment Process follows.

114. Documentation for the process from the Code of Practice can be found as follows:

- Appendix 1 - The screening questions which assist in identifying whether a Privacy Impact Assessment is required
- Appendix 2 - The Privacy Impact Assessment Template.
- Appendix 3 - Questions linking the PIA to the data protection principles.

115. The findings of the Privacy Impact Assessment should be summarised within Section 4 of the Data Sharing Agreement.

Overview of the PIA process	
1. Identifying the need for a PIA. The need for a PIA can be identified as part of an organisation's usual project management process or by using the screening questions in annex two of this Code.	2. Describing the information flows. Describe the information flows of the project. Explain what information is used, what it is used for, who it is obtained from and disclosed to, who will have access, and any other necessary information
3. Identifying the privacy and related risks. Some will be risks to individuals - for example damage caused by inaccurate data or a security breach, or upset caused by an unnecessary intrusion on privacy. Some risks will be to the organisation - for example damage to reputation, or the financial costs or a data breach. Legal compliance risks include the DPA, PECR, and the Human Rights Act.	4. Identifying and evaluating privacy solutions. Explain how you could address each risk. Some might be eliminated altogether. Other risks might be reduced. Most projects will require you to accept some level of risk, and will have some impact on privacy. Evaluate the likely costs and benefits of each approach. Think about the available resources, and the need to deliver a project which is still effective.
5. Signing off and recording the PIA outcomes. Make sure that the privacy risks have been signed-off at an appropriate level. This can be done as part of the wider project approval. A PIA report should summarise the process, and the steps taken to reduce the risks to privacy. It should also record the decisions taken to eliminate, mitigate, or accept the identified risks. Publishing a PIA report will improve transparency and accountability, and lets individuals learn more about how your project affects them.	6.Integrating the PIA outcomes back into the project plan. The PIA findings and actions should be integrated with the project plan. It might be necessary to return to the PIA at various stages of the project's development and implementation. Large projects are more likely to benefit from a more formal review process. A PIA might generate actions which will continue after the assessment has finished, so you should ensure that these are monitored. Record what you can learn from the PIA for future projects.

Note: PECR refers to the Privacy and Electronic Communications (EC Directive) Regulations 2003

Information for Patients

116. The first principle of the Data Protection Act requires that personal data should be processed fairly. Embedded within this principle is the need to ensure that all patients are aware of how their data is to be processed and which organisations it is being shared with, the Information Commissioner's office refers to the term 'no surprises'

117. This principle also applies to all data processing and sharing that is undertaken by the organisation. Each organisation should have a Fair Processing or Privacy Notice for patients which describes how the organisation processes and shares their information. This will normally be found on the organisation's web site.

118. The Information Commissioner's Office advises on when there is a need to 'actively communicate' a privacy notice. The circumstances include when the data being processed is sensitive information (such as health or social care information); when the intended use of the information is likely to be unexpected or when the information will be shared with another organisation in a way that the patient would not expect.

119. Because the Connected Health Cities projects are likely to introduce a novel data sharing or processing approach it is likely that active communication with patients will be required. The approach to be adopted may not be covered by the organisation's existing fair processing notice although it should also be included in it.

120. In addition, each project should consider the communication approach that will best suits their circumstances. Options to be considered should include:

    - Provision of details of the information sharing within routine patient communications such as outpatient appointment letters / discharge letters
    - Posters and information leaflets being made available to patients in clinic areas or on the wards.
    - Direct communication with patients while in clinics or as inpatients
    - Clinicians raising awareness directly with their patients.

121. Where explicit patient consent is being sought the patient information should be provided as part of the consent process to ensure that the patient is informed about the decision they are being asked to take.

122. Where implied consent or another lawful basis for processing and sharing personal confidential data is being relied upon (such as Section 251 support) the patient information must include details of what the patient can do should they wish to object to their data being processed in this way.

123. The Information Commissioner's Office provides a code of practice for fair processing which sets out good practice for designing patient information and what should be included.

    https://ico.org.uk/media/1610/privacy_notices_cop.pdf

124. Although De-personalised data (de-identified or pseudonymised data with appropriate controls in place) falls outside the Data Protection Act it is recommended that appropriate patient information is provided and privacy notices are updated to include the details of sharing.

Secure Systems

125. The seventh principle of the Data Protection Act requires that

    - Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

126. Projects that have undertaken a Privacy Impact Assessment will have considered the security implications of the data sharing from transit to security of the system in which the data is held.

127. Security of the data is the Data Controller's responsibility.

128. The Information Security Management: NHS code of practice can be found here:

    http://systems.hscic.gov.uk/infogov/codes/securitycode.pdf

129. Guidance on Secure systems can be found here:

    http://systems.hscic.gov.uk/infogov/security/infrasec/gpg/gensec.pdf

130. In addition, the Connected Health Cities Privacy Impact Assessment describes the safeguards to be put in place to create a secure data centre and provide secure data access.

    Insert URL for the CHC PIA here

Secure Data Transfer

131. When sensitive data (personal confidential, or anonymised in context) is being sent from one organisation to another the transfer method must be secure to protect the data in transit.

132. There are various options available such as encryption of data files. The Health and Social Care Information Centre has provided advice and guidance to the Digital Information Policy Unit of the Department of Health regarding security good practice in relation to the transfer of data on media such as CD, DVD and other removable media. This guidance along with other good practice information and security policy advice can be found on the Information Governance Toolkit website https://nww.igt.hscic.gov.uk/.

133. Advice on encryption good practice can be found here:

    http://systems.hscic.gov.uk/infogov/security/infrasec/iststatements/remmedia_html

134. Projects may wish to use the Secure File Transfer service. This is a web service designed to allow the secure transfer of data between NHS users. Details of the service can be found here:

    http://systems.hscic.gov.uk/infogov/security/infrasec/sft

135. A comprehensive user guide for the service can be found here:

http://systems.hscic.gov.uk/infogov/security/infrasec/sft/SFT-User-Guide.pdf

Pseudonymisation at Source

136. Pseudonymisation is a technical process that can be applied to the identifiers in a data set to replace them with pseudonyms. Pseudonymisation enables the distinction of an individual without enabling that individual identified. Pseudonymisation can be applied in a way that is either reversible or irreversible so that if it is necessary (and there is a lawful basis for doing so) for some of those involved in the project to identify the patient they will be able to reverse the pseudonym while others will not.

137. There are various open source data pseudonymisation tools available for use in health and social care which would allow the sending organisation to pseudonymise the data being shared before it is sent to the receiving organisation. If all organisations use the same pseudonymisation tool to send data to another organisation then it allows all data about the same patient to be linked on the basis of their pseudonym; avoids the need to share identifiable data; and protects patient confidentiality if appropriate controls are placed on the processing and storage of the data.

138. Further Advice and guidance on pseudonymisation at source can be obtained from the AHSN Informatics team.

Disposal and Destruction of Sensitive Data

139. The Data Controller is responsible for the security of the data up to and including its secure disposal and destruction. This applies even when the destruction of the data has been contracted out to a third party who are acting as Data Processors. Due diligence is required when appointing such third parties. Guidance on secure disposal can be found here:

http://systems.hscic.gov.uk/infogov/security/infrasec/gpg/gensec.pdf

IG assurance

140. Implementation of appropriate information security practices, policies, procedures and technical controls is supported through the IG Toolkit. All organisations processing patient personal confidential data should have achieved a satisfactory IG Toolkit score. This provides assurances that there are appropriate information governance controls within the organisation.

https://www.igt.hscic.gov.uk/requirementsorganisation.aspx?tk=422584913163530&cb=f0323b3e-baec-4d75-8ef9-cfac81d9c7d9&lnv=2&clnav=YES

Managing Data Breach Incidents

141. In the event of a data breach (or suspected data breach) during the data sharing or data access the project will be expected to follow the HSCICs guidance on Serious Incidents Requiring Investigation, in line with local arrangements.

https://www.igt.hscic.gov.uk/KnowledgeBaseNew/HSCIC%20IG%20SIRI%20%20Checklist%20Guidance%20V2%200%201st%20June%202013.pdf

Health and Social Care Information Centre (now branded as NHS Digital)

142. NHS Digital can provide a range of data services that might be required by the project from provision of national data sets to data linkage of project data to death data, hospital episode statistics etc.

143. Further details can be found here:

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

Connected Health Cities Hub

144. The Connected Health Cities Hub team can assist projects to meet understand their data and analysis requirements.

Appendix 1 - Privacy impact assessment screening questions

These questions are intended to help you decide whether a PIA is necessary.

NOTE - Answering 'yes' to any of these questions is an indication that a PIA would be a useful exercise. You can expand on your answers as the project develops if you need to.

Will the project involve the collection of new information about individuals?	**Yes / No**
Will the project compel individuals to provide information about themselves?	**Yes / No**
Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?	**Yes / No**
Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?	**Yes / No**
Does the project involve you using new technology that might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition.	**Yes / No**
Will the project result in you making decisions or taking action against individuals in ways that can have a significant impact on them?	**Yes / No**
Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records or other information that people would consider to be private.	**Yes / No**
Will the project require you to contact individuals in ways that they may find intrusive?	**Yes / No**

Appendix 2 - Privacy impact assessment template

This template is an example of how you can record the PIA process and results. You can start to fill in details from the beginning of the project, after the screening questions have identified the need for a PIA. The template follows the process that is used in this code of practice. You can adapt the process and this template to produce something that allows your organisation to conduct effective PIAs integrated with your project management processes.

Step one: Identify the need for a PIA

Explain what the project aims to achieve, what the benefits will be to the organisation, to individuals and to other parties.

You may find it helpful to link to other relevant documents related to the project, for example a project proposal.

Also summarise why the need for a PIA was identified (this can draw on your answers to the screening questions).

Step two: Describe the information flows

You should describe the collection, use and deletion of personal data here and it may also be useful to refer to a flow diagram or another way of explaining data flows. You should also say how many individuals are likely to be affected by the project.

Consultation requirements

Explain what practical steps you will take to ensure that you identify and address privacy risks. Who should be consulted internally and externally? How will you carry out the consultation? You should link this to the relevant stages of your project management process.

You can use consultation at any stage of the PIA process.

Step three: Identify the privacy and related risks

Identify the key privacy risks and the associated compliance and corporate risks. Larger-scale PIAs might record this information on a more formal risk register.

Appendix 3 can be used to help you identify the DPA related compliance risks.

Privacy issue	Risk to individuals	Compliance risk	Associated organisation / corporate risk

Step four: Identify privacy solutions

Describe the actions you could take to reduce the risks, and any future steps which would be necessary (eg the production of new guidance or future security testing for systems).

Risk	**Solution(s)**	**Result:** is the risk eliminated, reduced, or accepted?	**Evaluation:** is the final impact on individuals after implementing each solution a justified, compliant and proportionate response to the aims of the project?

Step five: Sign off and record the PIA outcomes

Who has approved the privacy risks involved in the project? What solutions need to be implemented?

Risk	Approved solution	Approved by

Step six: Integrate the PIA outcomes back into the project plan

Who is responsible for integrating the PIA outcomes back into the project plan and updating any project management paperwork? Who is responsible for implementing the solutions that have been approved? Who is the contact for any privacy concerns that may arise in the future?

Action to be taken	Date for completion of actions	Responsibility for action

Contact point for future privacy concerns

Appendix 3 - Linking the PIA to the data protection principles

Answering these questions during the PIA process will help you to identify where there is a risk that the project will fail to comply with the DPA or other relevant legislation, for example the Human Rights Act.

Principle 1

Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless:

a) at least one of the conditions in Schedule 2[2] is met, and

b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

Have you identified the purpose of the project?

How will you tell individuals about the use of their personal data?

Do you need to amend your privacy notices?

Have you established which conditions for processing apply?

If you are relying on consent to process personal data, how will this be collected and what will you do if it is withheld or withdrawn?

If your organisation is subject to the Human Rights Act, you also need to consider:

Will your actions interfere with the right to privacy under Article 8 of the European Human Rights Act?

Have you identified the social need and aims of the project?

Are your actions a proportionate response to the social need?

1.

[2] The conditions set out in Schedules 2 and 3 to the Data Protection Act are known as the "conditions for processing". Organisations processing personal data need to be able to satisfy one or more of these conditions. See https://ico.org.uk/for-organisations/guide-to-data-protection/

Principle 2

Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

Does your project plan cover all of the purposes for processing personal data?

Have you identified potential new purposes as the scope of the project expands?

Principle 3

Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

Is the quality of the information good enough for the purposes it is used?

Which personal data could you not use, without compromising the needs of the project?

Principle 4

Personal data shall be accurate and, where necessary, kept up to date.

If you are procuring new software does it allow you to amend data when necessary?

How are you ensuring that personal data obtained from individuals or other organisations is accurate?

Principle 5

Personal data processed for any purpose or purposes shall not be kept for longer than necessary for that purpose or those purposes.

What retention periods are suitable for the personal data you will be processing?

Are you procuring software that will allow you to delete information in line with your retention periods?

Principle 6

Personal data shall be processed in accordance with the rights of data subjects under this Act.

Will the systems you are putting in place allow you to respond to subject access requests more easily?

If the project involves marketing, have you got a procedure for individuals to opt out of their information being used for that purpose?

Principle 7

Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

Do any new systems provide protection against the security risks you have identified?

What training and instructions are necessary to ensure that staff know how to operate a new system securely?

Principle 8

Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country of territory ensures and adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Will the project require you to transfer data outside of the EEA?

If you will be making transfers, how will you ensure that the data is adequately protected?

Appendix 4 – Glossary of Terms

Term	Description
Access control	A means of ensuring that the resources of a data processing system can be accessed only by approved people in approved ways
Aggregate(d) data/information	Data derived from records about more than one person, and expressed in summary form, such as statistical tables.
Anonymisation	The process of rendering data into a form which does not identify individuals and where there is little or no risk of identification (identification is not likely to take place).
Anonymised data	Data in a form that does not identify individuals and where identification through its combination with other data is not likely to take place.
Anonymised in Context	Data in a form that does not identify individuals and where identification through its combination with other data is not likely to take place because of the controls placed on how it can be used.
Audit	An official inspection, or evaluation, e.g. that the organisation's processes are being complied with.
Caldicott Guardian	A senior person responsible for protecting the confidentiality of patient and service user information and enabling appropriate information sharing.
Common Law	The law derived from decisions of the courts and case law, rather than Acts of Parliament or other legislation.
Confidentiality	Ensuring that information is not made available or disclosed to unauthorised individuals, entities or processes.
Confidentiality Advisory Group	A group that provides independent expert advice to the Health Research Authority (for research applications) and the Secretary of State for Health (for non-research applications) on whether applications to access patient information without consent should or should not be approved under Section 251 of the NHS Act (2006). The role of CAG is to review applications and advise whether there is sufficient justification to access the requested confidential patient information. Using CAG advice as a basis for their consideration, the HRA or Secretary of State will take the final approval decision
Consent	The approval or agreement for something to happen after consideration. For consent to be legally valid, the individual must be informed, must have the capacity to make the decision in question and must give consent voluntarily. This means individuals should know and understand how their information is to be used and shared (there should be 'no surprises') and they should understand the implications of their decision, particularly where refusing to allow information to be shared is likely to affect the care they receive. This applies to both explicit and implied consent.

Term	Description
Data	Qualitative or quantitative statements or numbers that are (or are assumed to be) factual. Data may be raw or primary data (e.g. direct from measurement), or derivative of primary data, but are not yet the product of analysis or interpretation other than calculation.
Data breach	Any failure to meet the requirements of the Data Protection Act, unlawful disclosure or misuse of personal confidential data and an inappropriate invasion of people's privacy.
Data Controller	A person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.
Data Linkage	The merging of information or data from two or more sources with the object of consolidating facts concerning an individual or an event that are not available in any separate record.
Data processor	Any person (other than an employee of the data controller) who processes the data on behalf of the data controller.
Data Protection Act 1998 (DPA)	The main UK legislation which governs the handling and protection of information relating to living people.
Data sharing	The disclosure of data from one or more organisations to a third party organisation or organisations, or the sharing of data between different parts of an organisation. Can take the form of systematic, routine data sharing where the same data sets are shared between the same organisations for an established purpose; and exceptional, one off decisions to share data for any of a range of purposes.
Data sharing contracts/ Agreements	Set out a common set of rules to be adopted by the various organisations involved in a data sharing operation.
Data subject	An individual who is the subject of personal data.
De-identification	**G**eneral term for any process of removing the association between a set of identifying data and the data subject. It is used here specifically to mean the removal of patient identifiers from data. This may be partial (where only some of the identifiers are removed) or complete (where all patient identifiers are removed).
De-identified	Information which identifies an individual has been removed, but there is still some risk of re-identification.
Direct identifier	Name, address, widely-used unique person or record identifier (notably National Insurance Number, NHS Number, Hospital Number), telephone number, email uniquely identify the individual.
Disclose/ Disclosure	The act of making data available to one or more third parties.
Duty of Confidence	A duty of confidence arises when one person discloses information to another (e.g. patient to clinician) in circumstances where it is reasonable to expect that the information will be held in confidence. It – a. is a legal obligation that is derived from case law;

Term	Description
	b. is a requirement established within professional codes of conduct; and c. must be included within NHS employment contracts as a specific requirement linked to disciplinary procedures.
Fair Processing	Processing broadly means collecting, using, disclosing, retaining or disposing of personal data. If any aspect of processing is unfair, there will be a breach of the first data protection principle – even if it can be shown that one or more of the conditions for processing have been met.
Identifiable information	See 'Personal confidential data'. Information from which a patient can be identified. Their name, address and full postcode will identify a patient; combinations of information may also do so, even if their name and address are not included. Information consisting of small numbers and rare conditions might also lead to the identification of an individual.
Identification	Process of using claimed or observed attributes of an entity to single out the entity among other entities in a set of identities. The identification of an entity within a certain context enables another entity to distinguish between the entities with which it interacts.
Identifier	An item of data, which by itself or in combination with other identifiers enables an individual to be identified.
Incident	An event or occurrence.
Incident Reporting	A method or means of documenting any unusual problem, occurrence, or other situation that is likely to lead to undesirable effects or that is not in accordance with established policies, procedures or practices.
Information	Information is the "output of some process that summarises, interprets or otherwise represents data to convey meaning." Data becomes information when it is combined in ways that have the potential to reveal patterns in the phenomenon.
Information governance	How organisations manage the way information and data are handled within the health and social care system in England. It covers the collection, use, access and decommissioning as well as requirements and standards organisations and their suppliers need to achieve to fulfil the obligations that information is handled legally, securely, efficiently, effectively and in a manner which maintains public trust.
Information Security	Protecting information and information systems from unauthorised access, use, disclosure, disruption, modification or destruction.
Legitimate relationship	The legal relationship that exists between an individual and the health and social care professionals and staff providing or supporting their care.
Medical purposes	Include "healthcare purposes" plus" preventative medicine, medical research, financial audit and management of health [and social] care services"

Term	Description
Patient Identifiable Information	Any information that may be used to identify a patient directly or indirectly. Key identifiable information includes patient name, address, date of birth, full post code, images, tapes, NHS number and local identifiable codes.
Personal confidential data	This term describes personal information about identified or identifiable individuals, which should be kept private or secret. For the purposes of this guide 'personal' includes the DPA definition of personal data, but it is adapted to include dead as well as living people. '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. Used interchangeably with 'confidential' in this document.
Personal data	Data which relate to a living individual who can be identified from those data, or from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.
Privacy impact assessment	A systematic and comprehensive process for determining the privacy, confidentiality and security risks associated with the collection, use and disclosure for personal data prior to the introduction of or a change to a policy, process or procedure.
Processing	Processing in relation to information or data means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including: • organisation, adaptation or alteration of the information or data; • retrieval, consultation or use of the information or data; • disclosure of the information or data by transmission, dissemination or otherwise making available; or • alignment, combination, blocking, erasure or destruction of the information or data.
Pseudonym	Individuals are distinguished in a data set by using a unique identifier, which does not reveal their 'real world' identity.
Pseudonymisation/ Pseudo-Anonymised Data	The process of distinguishing individuals in a data set by using a unique identifier, which does not reveal their 'real world' identity
Pseudonymisation	A particular type of anonymisation that both removes the association with a data subject and adds an association between a particular set of characteristics relating to the data subject and one or more pseudonyms**.**
Pseudonym	A personal identifier that is different from the normally used personal identifier. This may be either derived from the normally used personal identifier in a reversible or irreversible way, or alternatively be totally unrelated. The term Pseudonym is usually restricted to mean an identifier

Term	Description
	that does not allow the derivation of the normal personal identifier. Such pseudonymous information is thus functionally anonymous.
Publish/Publishing	To disseminate to the public. Note that "disseminate" is sometimes given a meaning similar to that of "disclose" above, although its dictionary meaning used here is quite different: "to spread abroad" and "to disperse throughout".
Re-identification	The process of analysing data or combining it with other data with the result that individuals become identifiable. Also known as 'de-anonymisation'. The technique by which pseudonyms are reversed to reveal clear or patient identifiable data. This can be achieved by reverse application of the relevant keys through the pseudonymisation engine or by use of a look-up table containing patient identifiers and pseudonyms.
Reversible pseudonymisation	A method to enable the re-association of the identifying information and the data subject.
Role-Based Access Control	Grants a view of a patient's record depending on the role the individual was assigned when they registered for access to the NHS Care Records Service and related IT services. Authorised users are only able to access the information they need to carry out their role, e.g. a booking clerk will see less information than a doctor.
Section 251	This relates to section 251 of the NHS Act 2006 (originally enacted under Section 60 of the Health and Social Care Act 2001). It allows the common law duty of confidentiality to be set aside in specific circumstances where anonymised information is not sufficient and where patient consent is not practicable. Applications for approval to use Section 251 support are considered by the HRA Confidentiality Advisory Group.
Senior Information Risk Owner	An Executive Director or member of the Senior Management Board with overall responsibility for the organisation's information risk policy. The SIRO will also lead and implement the information governance risk assessment and advise the Board on the effectiveness of risk management across the organisation.
Sensitive personal data/information	Data that identifies a living individual consisting of information as to his or her: racial or ethnic origin, political opinions, religious beliefs or other beliefs of a similar nature, membership of a trade union, physical or mental health or condition, sexual life, convictions, legal proceedings against the individual or allegations of offences committed by the individual. See also 'Personal confidential data'.
Service user	A person who receives or is registered to receive attention, care, or treatment. The term includes patient, clients and other users of the service provided by the organisation.

Term	Description
Statistical data	Information which is held in the form of numerical data, nominal data (e.g. gender, ethnicity, region), ordinal data (age group, qualification level), interval data (month of birth) or ratio data (age in months).
Subject access request (SAR)	Under the Data Protection Act, individuals can ask to see the information about themselves that is held on computer and in some paper records, by writing to the person or organisation they believe holds it. A subject access request must be made in writing (email is acceptable) and must be accompanied by the appropriate fee, usually up to a maximum of £10. Once the applicable fee has been paid, a reply must be received within 40 calendar days.
Third party	In relation to personal data, any person other than the subject of the data, the data controller, or a data processor.