South, Central and West
Commissioning Support Unit

# Berkshire Interoperability

## Procuring A Person Held Record And Health / Social Care Portal

## Information Sharing

## IG Principles & Supporting Collateral

**Version:** Version 0.6

**Date:** 4th August 2015

**Status:** Draft for discussion

# Purpose

Since 2012, the National Health Service (NHS) in England has undergone fundamental restructuring in terms of commissioning of services. The NHS mandate published during this year, set out the NHS Commissioning Board's 5 key objectives to improve care, outcomes and experience, including the introduction of the "Friends and Family" test and booking appointments on-line. Underpinning the plans for improvement are strategies to make digital the default in the future and to improve the sharing and use of information between health providers.

In Berkshire we have been actively listening to our local residents, to the clinicians across the local NHS landscape and the care professionals in social care. They have consistently told us that the lack of shared information is hampering their ability deliver on person centred coordinated care. In addition, local residents tell us that they want to take a more active role in their own health care in partnership with their health and care professionals.

Currently there is limited data sharing among organisations. Information is stored within silos, with each organisation aware of their own data but lacking an overall, person centric view of the whole. This lack of interoperability means there is no one single view of the individual.

The range of service areas and the required support structures suggest that the challenge of delivering co-ordinated care should not be underestimated. It requires an integrated service model to deliver joined up care across different provider boundaries, where providers operate under different service objectives and performance criteria. Key to this is the sharing of essential information required to provide individuals with a holistic package of care.

However, to really transform the system and put people in control of their own care and data, we need to liberate their data and give it to them in a format that is completely accessible. The only way to really do this is by providing individuals access to their own data via a person held health and social care record portal (PHP)

In terms of interoperability, this leads to the two main objectives that Berkshire need to achieve:

- **Interoperability and information exchange between organisations**.
    - This would allow the flow of data to be sent between two or more organisations for the benefit of coordinating service provision across care pathways improving patient care and data analysis.
- **Having a person held health and social care record (PHR) for the citizens of Berkshire.**
    - Across commissioners and health and social care providers, so that the individual holds and manages their care and gives consent to providers of care to view their record based on an agreed data set. Providers thereby work together to provide high quality care.

The purpose of this document is to support these objectives by ensuring they are implemented in conjunction with the best practice principles associated with Information Governance.

This document is split into three sections, they are:

- **IG principles**: The IG principles that form the core of safe sharing of information across the organisations involved.
- **Supporting collateral**: The compliance evidence and detailed understanding that supports and ensures these principles are being adhered to.
- **Cross reference mapping**: A mapping between the principles and the supporting collateral to ensure there is no ambiguity in terms of what needs to be in place to satisfy best practice is being followed.

## Information Governance principles

The role of the IG steering group is to support the needs of the business in adhering to the national guidelines while ensuring information is managed in accordance to the rules and regulations in place at the time and according to best practice.

| Number | Description |
|---|---|
| 1 | Every use of personal confidential data must be fair and lawful and each organisation sharing confidential information must ensure that the organisation complies with legal requirements. |
| 2 | Health and Social Care professionals will only view personal data for individuals with whom they have a legitimate relationship and will only have access to the areas of the record that are appropriate to their role |
| 3 | Identifiable information will be shared only for the provision of care or if there are legal or regulatory requirements to do so (subject to appropriate legal and ethical approval process) and there will be no commercial use unless the data is anonymized |
| 4 | Where use of personal confidential data is considered to be essential, the inclusion of each individual item of data should be considered and justified so that the minimum amount of personal confidential data is transferred or accessible as is necessary for the provision of care |
| 5 | Data should be adequate, relevant and not excessive for the purpose of sharing; should be accurate and kept up to date; and should not be kept for longer than is necessary or required. Data will be stored and deleted / destroyed in accordance with a data retention schedule. |
| 6 | Consent to view a record will be assumed when a referral to a service has been made and will also be confirmed when possible at the point of care. |
| 7 | There must be full auditability of who has viewed what record and audit will be the responsibility of the organisation where viewing is taking place. Everyone with access to personal confidential data should be aware of their responsibilities and everyone handling personal confidential data must be fully aware of their responsibilities and obligations to respect an individual's confidentiality in accordance with the Data Protection Act. |

| | |
|---|---|
| 8 | Partners will not be held responsible for another organisation's data or their end-users. Any data breaches or inappropriate accesses will be reported in accordance with the project's Incident Management Reporting Procedures. |
| 9 | The rights of the individual data subjects should be clearly communicated including the ability to dissent from sharing their data and how the data subject's rights under the 1998 Data Protection Act will be met. Partners are responsible for managing their own Subject Access Requests in accordance with their own policies and procedures. |
| 10 | The Individual's personal data and the data repository in which it is stored should be the subject of appropriate technical and organisational measures against unauthorised or unlawful processing, accidental loss or destruction. |
| 11 | Secondary use of the information, e.g. risk stratification[1], will be available only to those system users with the correct role(s) to run such queries. |
| 12 | Data ownership of the data repository supplying the Portal will reside jointly with the sharing organisations together acting as data controllers in common. Any data transferred from the Portal into a partner organisation's own care management system takes on an "independent life" and becomes the responsibility of that partner. Organisations must ensure that in doing so the data copied is essential, justified and accurate. |

## Supporting document descriptions

| ID | Product Name | Product Description |
|---|---|---|
| A | Patient Information Programme | Full requirements, plan and timetable for informing patients and the public about what the project is doing and how it will inform and support improvements in care. Implementation of the PIP so that all individuals have been communicated with. |
| B | Data-Flow Mapping | Full description of what data is being moved between systems/organisations and how this happens. Required for PIA and ISA processes |
| C | Revised Information Sharing Agreements | Updates to show changes within the project phase 3 to include secondary uses |
| D | Revised patient consent model | Model to show that consent to view a record will be assumed when a referral to a service has been made and will also be confirmed when possible at the point of care |
| E | Patient opt-out processes | Procedure for managing patient opt-out and sharing across organisations |
| F | Privacy Impact Assessments | Required as part of the ISA process – Initial and/or full PIA and process for IG sign-off |

[1] Risk Stratification is a statistical process to identify factors before the occurrence of an event with unwanted outcomes, to develop interventions to mitigate their impact. It is considered an extension of direct care to the individual.

| | | |
|---|---|---|
| G | Role Based Access | Description of all role based access permissions to be used within the project |
| H | Subject Access Requests | Process for managed SARs under the Data Protection Act that relate to the use of data on the phase 3 solution |
| I | Data quality and accuracy checking | Process for reporting and managing comments and complaints from patients where data quality/accuracy issues are noted and for correcting these |
| J | Incident management reporting | Procedure for managing and reporting of incidents and for sharing with partner organisations for resolution |
| K | Auditing requirements | Procedure for auditing in all organisations, to show format, frequency, content and responsibilities for reporting |
| L | Data security model | Describes the secure encryption for data at rest and data being transferred.<br>Describes all certifications associated with organisations that store information outside the originator (producer) organisation network to ensure that all IGL2 and PSN compliance requirements are met |
| M | Data Retention Schedule | Procedure for the secure deletion of data and the duration of data retention in association with the information asset register |
| N | Risk Stratification Overview | Documents the process that will be imbedded to ensure that all risk stratification work is reviewed by the Berkshire IG Steering Group to ensure that identifiable information will be shared only for the provision of care. |

# Cross reference table linking principles to supporting documents

| | Supporting documentation | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Principle** | **Key legal basis or relevant guidance** | Patient Information Programme | Data-Flow Mapping | Revised Information Sharing Agreements | Revised patient consent model | Patient opt-out processes | Privacy Impact Assessments | Role Based Access | Subject Access Requests | Data quality and accuracy checking | Incident/management reporting | Auditing requirements | Data security model | Data Retention Schedule | Risk Stratification |
| Every use of personal confidential data must be fair and lawful and each organisation sharing confidential information must ensure that the organisation complies with legal requirements. | Data Protection Act 1998 Care Act 2014 | √ | X | √ | √ | √ | √ | √ | √ | X | √ | √ | √ | √ | √ |
| Health and Social Care professionals will only view personal data for individuals with whom they have a legitimate relationship and will only have access to the areas of the record that are appropriate to their role | Caldicott principles v.2 2013 | √ | X | √ | √ | √ | √ | √ | X | X | √ | √ | √ | x | √ |
| Identifiable information will be shared only for the provision of care or if there are legal or regulatory requirements to do so (subject to appropriate legal and ethical approval process) and there will be no commercial use unless the data is anonymized | Caldicott principles v.2 2013 Care Act 2014 | √ | ? | √ | √ | √ | √ | X | X | X | √ | √ | √ | x | √ |
| Where use of personal confidential data is considered to be essential, the inclusion of each individual item of data should be considered and justified so that the minimum amount of personal confidential data is transferred or accessible as is | Data Protection Act 1998 Caldicott principles v.2 2013 Care Act | √ | ? | √ | √ | √ | √ | X | X | ? | √ | √ | √ | x | √ |

| | Supporting documentation | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Principle** | **Key legal basis or relevant guidance** | Patient Information Programme | Data-Flow Mapping | Revised Information Sharing Agreements | Revised patient consent model | Patient opt-out processes | Privacy Impact Assessments | Role Based Access | Subject Access Requests | Data quality and accuracy checking | Incident/management reporting | Auditing requirements | Data security model | Data Retention Schedule | Risk Stratification |
| necessary for the provision of care | 2014 | | | | | | | | | | | | | | |
| Data should be adequate, relevant and not excessive for the purpose of sharing; should be accurate and kept up to date; and should not be kept for longer than is necessary or required. Data will be stored and deleted / destroyed in accordance with a data retention schedule. | Data Protection Act 1998 Caldicott principles v.2 2013 | √ | ? | √ | √ | √ | √ | X | X | √ | √ | X | x | √ | x |
| Consent to view a record will be assumed when a referral to a service has been made and will also be confirmed when possible at the point of care. | Caldicott principles v.2 2013 | √ | √ | √ | √ | √ | √ | X | X | X | √ | √ | x | x | √ |
| There must be full auditability of who has viewed what record and audit will be the responsibility of the organisation where viewing is taking place. Everyone with access to personal confidential data should be aware of their responsibilities and everyone handling personal confidential data must be fully aware of their responsibilities and obligations to respect an individual's confidentiality in accordance with the Data Protection Act. | Data Protection Act 1998 Caldicott principles v.2 2013 Care Act 2014 | √ | X | X | √ | √ | √ | √ | √ | X | √ | √ | √ | x | x |
| Partners will not be held responsible for another organisation's data or their end-users. Any data breaches or inappropriate accesses will be reported | Data Protection Act 1998 Caldicott | √ | X | X | √ | √ | √ | √ | √ | X | √ | √ | √ | x | x |

| | Supporting documentation | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Principle** | **Key legal basis or relevant guidance** | Patient Information Programme | Data-Flow Mapping | Revised Information Sharing Agreements | Revised patient consent model | Patient opt-out processes | Privacy Impact Assessments | Role Based Access | Subject Access Requests | Data quality and accuracy checking | Incident/management reporting | Auditing requirements | Data security model | Data Retention Schedule | Risk Stratification |
| in accordance with the project's Incident Management Reporting Procedures. | principles v.2 2013 | | | | | | | | | | | | | | |
| The rights of the individual data subjects should be clearly communicated including the ability to dissent from sharing their data and how the data subject's rights under the 1998 Data Protection Act will be met. Partners are responsible for managing their own Subject Access Requests in accordance with their own policies and procedures. | Data Protection Act 1998 Caldicott principles v.2 2013 | √ | X | √ | √ | √ | √ | X | √ | √ | √ | √ | x | √ | x |
| Individual's personal data and the data repository (s) in which it is stored should be the subject of appropriate technical and organisational measures against unauthorised or unlawful processing, accidental loss or destruction. | Data Protection Act 1998 | X | X | X | X | X | X | X | X | √ | √ | X | √ | x | x |
| Secondary use of the information, e.g. risk stratification, will be available only to those system users with the correct role(s) to run such queries. | Data Protection Act 1998 Caldicott principles v.2 2013 | √ | x | √ | √ | √ | √ | √ | x | √ | √ | √ | √ | x | √ |
| Data ownership of the data repository supplying the Portal will reside with the sharing organisations together acting as data controllers in common. Any data extracted from the Portal into | Data Protection Act 1998 Caldicott principles | x | x | √ | x | x | √ | x | √ | √ | x | √ | √ | x | x |

| | Supporting documentation | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Principle** | **Key legal basis or relevant guidance** | Patient Information Programme | Data-Flow Mapping | Revised Information Sharing Agreements | Revised patient consent model | Patient opt-out processes | Privacy Impact Assessments | Role Based Access | Subject Access Requests | Data quality and accuracy checking | Incident/management reporting | Auditing requirements | Data security model | Data Retention Schedule | Risk Stratification |
| a partner organisation's own care management system takes on an "independent life" and becomes the responsibility of that partner. Organisations must ensure that in doing so the data copied is essential and justified and accurate. | v.2 2013 | | | | | | | | | | | | | | |

## Legislation and guidance to be considered (as per ISA Appendix B):

This section seeks to reference the current regulatory and legal environment in which we are operating. The listed rules and regulations may all impact Berkshire Interoperability however the list in not exhaustive. Certain elements are mandated by regulation or legislation however in the pursuit for good practice all parties are expected to follow in accordance with their best judgement.

The rules and regulations relevant to information sharing agreements and information governance include:

- The Care Act 2014
- The Data Protection Act 1998.
- The Guide to Confidentiality in Health and Social Care.
- The NHS Care Record Guarantee for England.
- The Social Care Record Guarantee for England.
- The international information security standard: ISO/IEC 27002: 2013.
- The Information Security NHS Code of Practice.
- The Records Management NHS Code of Practice.

- The Freedom of Information Act 2000.
- The Human Rights Act 1998.
- The Local Government Act 1972 and 2000.
- The National Health Service Act 2006.
- The Health Service (Control of Patient Information) Regulations 2002.
- Ministry of Justice guidance to legal professionals: “Public Sector Data Sharing: Guidance on the Law”
- The common law duty of confidentiality.
- The Code of Practice for the Management of Confidential Information.
- The Caldicott Principles 1997 and 2013.
- The Public Health (Control of Diseases) Act 1984.
- The Public Health (Infectious Diseases) Regulations 1985.
- The Education Act 1944 (for immunisations and vaccinations to NHS Trusts from schools).
- The Births and Deaths Act 1984.
- The Children Act 1989.
- The Family Law Reform Act 1967.
- The Mental Health Act 2007.
- The Mental Capacity Act 2005.
- The Crime and Disorder Act 1998 (with specific reference to sections 17 and 115)
- The Police and Criminal Evidence Act 1984.
- The Human Fertilisation and Embryology (Disclosure of Information) Act 1992.
- The Access to Medical Reports Act 1990.
- The Venereal Diseases Act 1917.
- The Venereal Diseases Regulations 1974 and 1992.
- The Abortion Act 1967.
- The Adoption Act 1976.
- General Medical Council: “Confidentiality: Protecting and Providing Information”

# Implications of Principles 10 and 12

As principles 10 and 12 have been developed, some immediate implications have been identified which need to be articulated to the group to ensure all partners are completely clear about the project's intentions and justifications for the proposed data repository in which the Individual's personal data will be stored for use by the Integrated Digital Record solution.

**Intentions;**

1. To create a "centralised data repository" that will store the data subject's data supplied by provider organisations. Note that NO information can or will be shared without the explicit written consent of the providing organisation. This is managed via the Information Sharing Agreements (ISA) that has and will be implemented across Berkshire. These ISA's detail exactly what information is to be shared and who it is to be shared with.
2. The "centralised data repository" will be underpinned by product "N" (Data Security Model) to provide assurances to provider organisations that appropriate technical measures against unauthorised or unlawful access, accidental loss or destruction are in place. The Data Security Model will stipulate the minimum requirements for; physical, technical and logical security, secure encryption for data at rest and data being transferred in order to demonstrate that all IGL2 and PSN compliance requirements are met. It is the projects intention to seek approval for this document via this Information Governance Steering Group to set the bench mark which all potential hosting service suppliers must meet in order to be considered. Any such hosting service supplier will need to demonstrate IGL2 and PSN compliance.
3. Provider organisations will act jointly as data controllers in common. The term jointly is used where two or more persons (usually organisations) act together to decide the purpose and manner of any data processing. The term in common applies where two or more persons share a pool of personal data that they process independently of each other.

**Justification;**

1. The National Information Bureau's Personlised Health and Care 2020 framework for action set out the NHS Commissioning Board's 5 key directives to improve care, outcomes and experience. From March 2018 all individuals must be enabled to view their care records and to record their own comments and preferences on their record, with access through multiple routes including NHS Choices. Initially, this will focus on data held by NHS providers (primary care, acute, community and mental health), but it will be progressively extended to cover other care settings, taking account of the work that local authorities are progressing in regard to personal records.

This will create the opportunity for individuals to create and manage their own personal care record. This directive is not optional - the question is not “if” but “when”.

In order to support this and other strategic local and national directives all organisations involved in the Berkshire interoperability project have been working to define a common set of requirements.

These requirements have been reviewed by each of the 17 organisations and amended to ensure they represent an accurate statement of needs across the geographic area. These requirements will be signed off and will form the basis of any future procurement.

Although there is a large number of detailed requirements one of the 3 key requirement that underpins a clear need for a person held health and social care record portal (PHP) is as follows;

| | |
|---|---|
| Requirement 3901 | The solution MUST provide a way for patients to access and view their own (combined) record. |

In order for the project to deliver this key requirement, a “centralised data repository” (CDR) must be implemented as part of the Integrated Digital Care record solution architecture. The project team has engaged with over 5 of the largest solution suppliers who have confirmed that a PHP can only be implemented in conjunction with a CDR.

2. A Risk Stratification (a statistical process to identify factors before the occurrence of an event with unwanted outcomes, to develop interventions to mitigate their impact ) capability has been identified as one of the 3 key solution requirements that underpin all others in enabling Berkshire to achieve its strategic vision and is defined below;

| | |
|---|---|
| Requirement 3617 | The solution MUST be able to produce Business Intelligence/risk stratification reporting either directly or via a 3rd party reporting system. |

In order for the project to deliver this key requirement, a “centralised data repository” (CDR) must be implemented as part of the Integrated Digital Care record solution architecture. The project team has engaged with over 5 of the largest solution suppliers who have confirmed that a Risk Stratification capability can only be realised in conjunction with a CDR.