|  |  |  |  |
| --- | --- | --- | --- |
| Document filename: | **National Record Locator Service Data Privacy Impact Assessment** | | |
| Project / Programme | **Digital Interoperability Platform** | Project | **National Record Locator Service Data** |
| Document Reference |  | | |
| Product Manager | **Hadleigh Stollar** | Status | **Final** |
| Owner | **Dave Jarvis** | Version | **1.0** |
| Author | **Stephen Elgar** | Version issue date | **05/07/2018** |

**National Record Locator Service**

**Data Privacy Impact Assessment**

Document management

Revision History

|  |  |  |
| --- | --- | --- |
| Version | Date | Summary of Changes |
| 0.1 | 12/12/17 | First draft based on DIP DPIA |
| 0.2 | 19/01/18 | Second draft based on comments from IG staff in Trusts to change format to that of conventional Privacy Impact Assessment |
| 0.5 | 18/05/18 | Fifth draft based on comments from NHS Trust staff and from discussions internal to NHS Digital |
| 0.6 | 15/06/18 | Based on comments from NHS Digital Solutions Assurance team, changes to Data Controller relations position and assumption on Data Sharing Agreement |
| 0.7 | 19/06/18 | Updated screen shots and diagrams |
| 1.0 | 05/07/18 | Final – minor corrections for accuracy and confirmation of NHS Digital as a Joint Data Controller with the NHS organisations that publish and view pointers, addition of LHRC context |

Reviewers

This document must be reviewed by the following people:

|  |  |  |  |
| --- | --- | --- | --- |
| Reviewer name | Title / Responsibility | Date | Version |
| Dr Amir Mehrkar | Digital Interoperability Platform (DIP)  Clinical Lead | 19/06/18 | V0.7 |
| Dr Adrian Burke | Clinical Lead NRLS | 19/06/18 | V0.7 |
| David Jarvis | National Record Locator Service (NRLS) Project Manager | 19/06/18 | V0.7 |
| Mike Walker | DIP Head of Programme | 19/06/18 | V0.7 |
| Adam Hatherly | Domain D Technical Architect | 19/06/18 | V0.7 |
| Will Weatherall | NRLS Technical Architect | 19/06/18 | V0.7 |
| Hadleigh Stollar | NRLS Programme Manager | 19/06/18 | V0.7 |

Approved by

This document must be approved by the following people:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Name | Signature | Title | Date | Version |
| Dr Amir Mehrkar |  | Digital Interoperability Platform (DIP)  Clinical Lead | 05/07/18 | 1.0 |
| Dr Adrian Burke |  | Clinical Lead NRLS | 05/07/18 | 1.0 |
| Mike Walker |  | DIP Head of Programme | 05/07/18 | 1.0 |

Glossary of Terms

|  |  |
| --- | --- |
| Term / Abbreviation | What it stands for |
| API | Application Programming Interface – the set of technical components enabling information to be exchanged (interoperability) between systems |
| Capability | The description for a set of business requirements being delivered by NRLS APIs |
| Care Record Element | This describes a ‘section’ or type of information held in the patient’s record – e.g. Diagnoses, Allergies and Sensitivities |
| Data Controller | Role identified in the Data Protection Act, for the persons/organisations carrying legal responsibility to ensure that the data in their control is governed in accordance with the act |
| Data Processor | * A processor is responsible for processing personal data on behalf of a controller. If you are a processor, the GDPR places specific legal obligations on you; for example, you are required to maintain records of personal data and processing activities. You will have legal liability if you are responsible for a breach. |
| Data Subject | Patient whose record has been requested and is transferred using NRLS APIs |
| FHIR | Fast Healthcare Interoperability Resources – open standard for healthcare data models and transfer resources <https://www.hl7.org/fhir/overview.html> - part of the API specification |
| FoT | First of Type – i.e. the initial deployments of the NRLS capabilities |
| GPSoC | ‘GP Systems of Choice’ Framework <http://systems.digital.nhs.uk/gpsoc> |
| IAO | Information Asset Owner |
| IGA | Information Governance Alliance – information and guidance organisation for the Health and Care sector |
| NDCM | GPSoC National Data Controller Model project |
| RTM | Requirements Traceability Matrix – specifying more detailed requirements, and supporting traceability of requirements delivery |
| SSP | Spine Security Proxy – the set of NHS ‘Spine’ functions which provide security & validation of Consumer - Provider API interactions |
| TOM | NHS Digital Solutions Assurance ‘Target Operating Model’ – the set of requirements which Commissioning/Deploying organisations and Consumer Suppliers must meet to be assessed as technically conformant and deployed |
| NRLS | National Record Locator Service |
| DIP | Digital Interoperability Platform |
| PDS | Personal Demographic Service |
| LHCR | Local Health Care Record exemplars; NHS England funded initiative to support sharing of information |

Document Control:

The controlled copy of this document is maintained in the NHS Digital corporate network. Any copies of this document held outside of that area irrespective of format (e.g. paper, email attachment), are considered to have passed out of control and should be checked for currency and validity.

Contents

[1 Introduction 5](#_Toc518586255)

[1.1 Purpose of Document 5](#_Toc518586256)

[1.2 Legal, Regulatory Framework 5](#_Toc518586257)

[1.3 Consultation & Assessment Approach 6](#_Toc518586258)

[2 National Record Locator Service 7](#_Toc518586259)

[2.1 Background - Digital Interoperability Platform 7](#_Toc518586260)

[2.2 National Record Locator Service Actors & Components 9](#_Toc518586261)

[2.3 National Record Locator Service Information Flows 12](#_Toc518586262)

[3 Impact on Privacy & Related Risks 14](#_Toc518586263)

[4 Privacy Risk Management 14](#_Toc518586264)

[4.1 Publishing and Consuming Suppliers & Organisations 14](#_Toc518586265)

[4.2 Data-Sharing Agreements 14](#_Toc518586266)

[4.3 NHS Digital Responsibilities 15](#_Toc518586267)

[4.4 Risk Mitigation Controls 16](#_Toc518586268)

[5 Conclusions 18](#_Toc518586269)

[6 Appendix A –– IG hazard analysis 19](#_Toc518586270)

[7 Appendix B – Application of access control model 21](#_Toc518586271)

[8 Appendix C – GDPR compliance for NHS Trusts & NHS Digital 23](#_Toc518586272)

[9 Appendix D – “Mock up” screen shots of information flows 24](#_Toc518586273)

# Introduction

## Purpose of Document

National Record Locator Service (NRLS) is one of several capabilities of the Digital Interoperability Platform (DIP). In this document potential information security and confidentiality risks of this capability are considered and how these risks are mitigated. The current patient record on Personal Demographic Service (PDS) contains the registered GP. With the National Record Locator Service, a note of the location of care records will be added to the central patient record. These will enable a query-based view of the patient record to be returned to the point of care. Only the locator is held centrally.

The document is a Data Protection Impact Assessment (DPIA) and considers:

* the information flow for the NRLS capability
* identifies the potential effects upon individual privacy
* identifies and explains how risks will be minimised
* explains how the solution complies with the legal and regulatory framework
* illustrates that care and diligence has been taken in considering this and its impacts
* informs decision makers about how the project is proceeding

Design work on NRLS Phase 1 is complete. This version of the DPIA has been prepared following consultation with NHS Trusts that are planning to take the service.

## Legal, Regulatory Framework

DPIA is a tool which helps organisations to identify the most effective way to comply with the new version of the Data Protection Act (DPA) that comes into force in May 2018 indicated by the General Data Protection Regulation (GDPR). GDPR guidance is now available. Most of the 1998 Act remains relevant. This document refers to the 1998 and prospective 2018 Act. The format of this document is based on a Privacy Impact Assessment. Common Law Duty of Confidentiality obligations are considered in addition to DPA in meeting individuals’ expectations of privacy.

The Data Protection Act became law in March 2000 and required systems and assurance to be in place prior to the processing of data giving people specific rights in relation to their personal information and placing certain obligations on those organisations that are responsible for processing it. These are summarised by 8 Data Protection Principles which specify that personal data must be:

1. Processed fairly and lawfully
2. Processed for specified purposes
3. Adequate, relevant and not excessive
4. Accurate and kept up-to-date
5. Not kept for longer than necessary
6. Processed in accordance with the rights of data subjects
7. Protected by appropriate security (practical and organisational)
8. Not transferred outside the EEA without adequate protection

Information about an individual’s health should be processed as ‘Sensitive Personal Data’. Under the new DPA the phrase is ‘Special category health data’.

Health and Care sectors are also guided and challenged on important data issues by the National Data Guardian, Dame Fiona Caldicott, whose initial report highlighted the following six key principles which have been subsumed into the NHS confidentiality code of practiceplus the seventh included in the 2013 follow-up Information Governance report:

1. Justify the purpose(s) of using confidential information
2. Only use it when absolutely necessary
3. Use the minimum that is required
4. Access should be on a strict need-to-know basis
5. Everyone must understand his or her responsibilities
6. Understand and comply with the law
7. The duty to share information can be as important as the duty to protect patient confidentiality

NRLS compliance with both Data Protection and Common Law Duty of Confidentiality obligations is stated in Appendix C.

The Second Caldicott Report 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 an identified individual. 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 (identified patient safety), 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.”

## Consultation & Assessment Approach

For NRLS:

* Dec 2018 - Initial DPIA draft preparation (using NHS Digital format) for review by NHS Trusts planning to use NRLS in Phase 1
* Jan 2018 – Second draft DPIA for review by NHS Trusts planning to use NRLS in Phase 1 using a format developed for PIA
* March 2018 – Third draft DPIA prepared based on feedback from Trust staff
* May 2018 – Fifth draft DPIA prepared based on feedback and on discussions within NHS Digital

For the other DIP capabilities: -

* Jan 2017 – an initial PIA for Reasonable Adjustment flag with Learning Disability clients and professionals was completed
* Mar 2017 - an initial PIA to support GP Connect “first of type”
* Dec 2017 - initial DPIA for NHS Digital for DIP internal review
* Jan 2018 - Initial DPIA draft preparation for review by Child Health Information strategy team
* May 2018 – second draft of GP Connect DPIA for discussions with Royal College Joint IT Group

NRLS is proposed as one of the mechanisms for national sharing for [Local Health Care Record exemplar](https://www.interopen.org/2018/03/27/interopen-recognised-in-nhs-englands-invitation-for-proposals-for-local-health-and-care-record-lhcr-programme/)s. The assumption is that the NRLS and DIP services will be available to LHCR exemplars as an option to support sharing of patient information for direct care.

# National Record Locator Service

## Background - Digital Interoperability Platform

NHS Digital has been commissioned to develop and operate a Digital Interoperability Platform (DIP) to deliver a set of national capabilities or services – Figure 1. DIP patient information services will bring together care information related to the patient in near real-time at the point of care. They will support wider sharing of records along care pathways and across organisational boundaries. In association, work is progressing to standardise integration through development of interface messages (APIs) and also through simplifying the operating model.

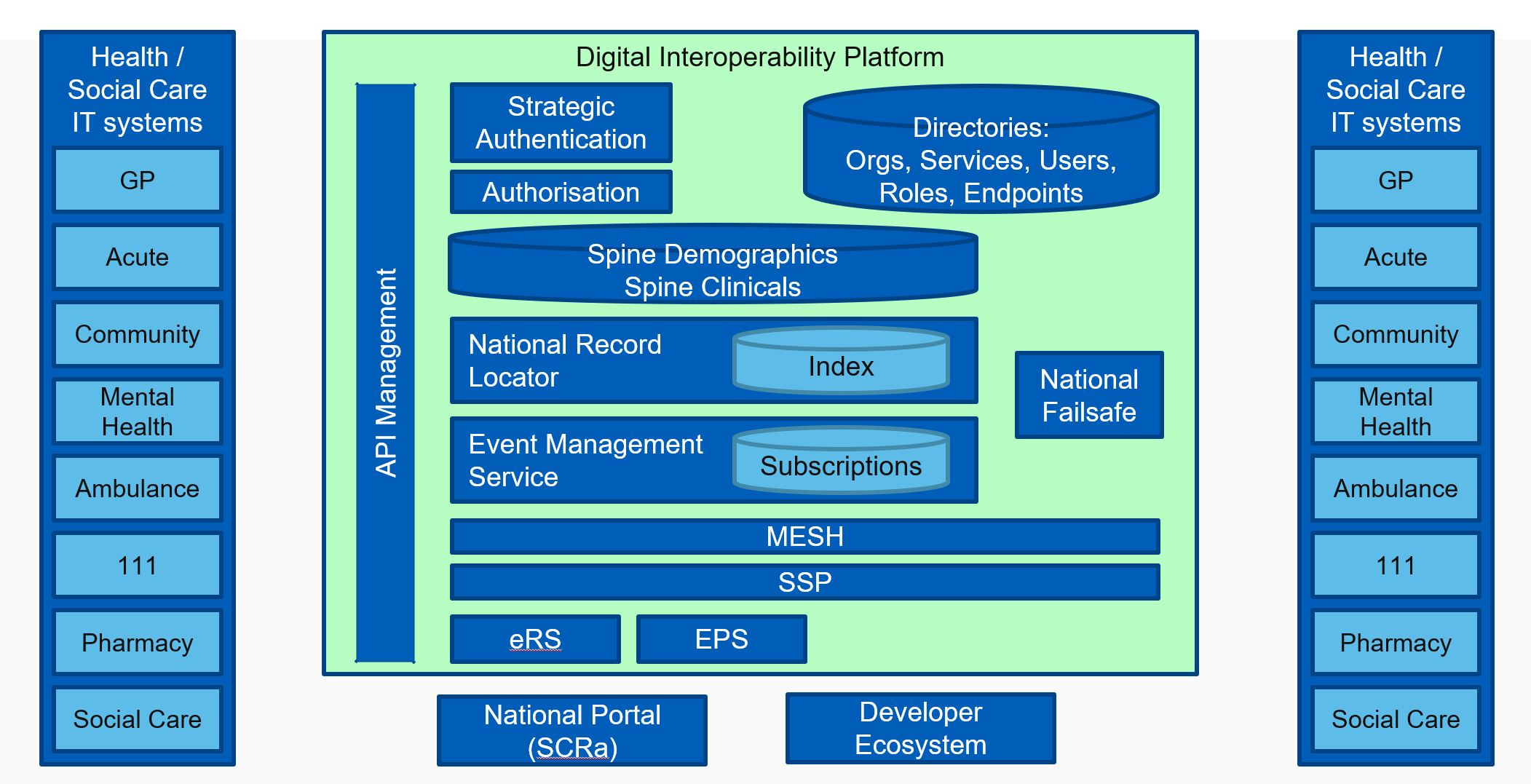


Figure 1 – Digital Interoperability Platform

The new capabilities of DIP include a National Record Locator Service, Event Management Service and Failsafe, GP Connect, National Portal and also a new Reasonable Adjustment notification which is a national patient flag. They should be seen as a technology update and extension of existing patient information services such as the Personal Demographic Service and Summary Care Record. With these capabilities patient data, for the most part, traverses the infrastructure platform rather than being held and managed by NHS Digital. These capabilities will be progressively updated both in terms of new functions, for example GP Connect is currently “view only”, there is work to add in the process of appointment booking.

In association, NHS Digital has launched a new Message Lab to be run in partnership with INTEROPen. By pooling the expertise of developers from both industry and NHS Digital, the Lab is expected to accelerate the development of open source messages designed to improve system integration across the NHS and social care. Working according to INTEROPen’s openness and transparency principles, the Lab will address real information exchange problems for patients and clinicians. The objective is to make patient information securely accessible to healthcare professionals at the point of need.

## National Record Locator Service Actors & Components

The NRLS has the potential to unify patient records across the NHS without needing to dictate where those records might be stored. This flexible and evolvable service could provide a level of interoperability in the NHS which has previously been unachievable. A record locator service could store the location of digital (and paper) records within the NHS. For digital endpoints it could hold a pointer to a record which may be retrievable via a standardised API. For paper records it could record the contact details of the organisation which holds the paper record.

**The NRLS Use Case**: an authorised clinician, care worker and/or administrator, in any health or care setting, is able to access a patient’s information to support that patient’s direct care.

**NRLS Aims**:

1. Build a national brokerage service between information consumers and information data sources
2. Complement local initiatives, including integrating into existing clinical systems
3. Provide the underpinning technical capabilities (Digital Interoperability Platform) that will facilitate integrated care

**NRLS Objectives**:

1. To provide a national index to support the health AND [social] care system (e.g. store that record exists) in a chronological order
2. To provide a record as stored/listed within the index
3. To retrieve and/or point/locate records using the Care Connect APIs
4. To provide cross border interoperability, transparency and real-time information for the purposes of direct care

For the Phase 1 implementation of NRLS, the intention is to provide Mental Health crisis plans to Ambulance and 111 teams. This use case is illustrated in Figure 2 on the next page. It shows how a record is created and accessed within the urgent and emergency care setting (and beyond e.g. within the community and primary care settings too) and how direct care can positively be influenced as a result of being able to access a patient’s record.

Table 1. NRLS Actors and Components, on page 10, lists the organisation that are involved in the information flows and their Data Controller status.

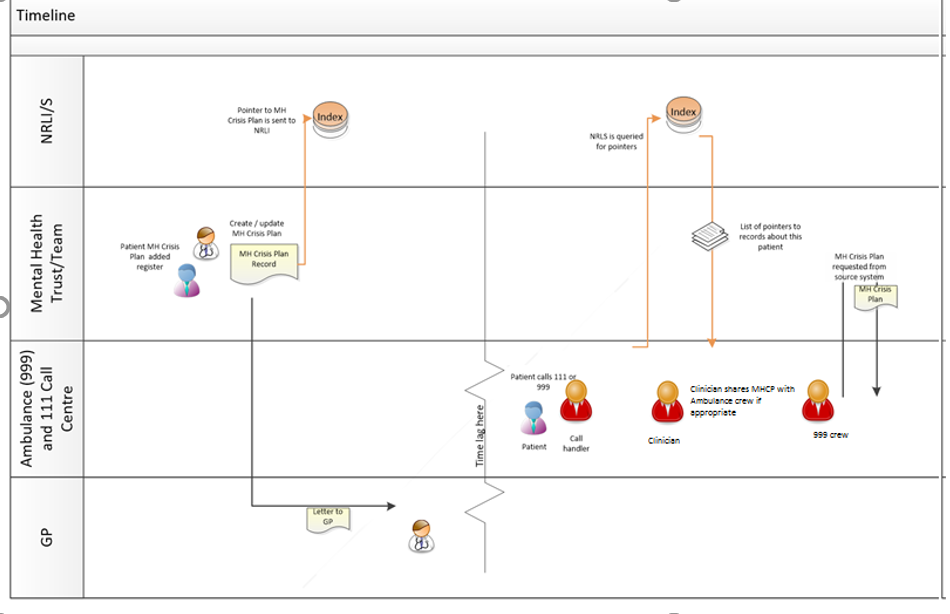


Figure 2: Example NRLS Use Case: Urgent and Emergency Care – Mental Health Crisis Plans

|  |  |
| --- | --- |
| **What/Who** | **Role** |
| Healthcare Organisation | May be a publishing or consuming organisation |
| Publishing Organisation  (Data Controller for its own systems and data and Joint Data Controller for NRLS) | The healthcare organisation deploying the NRLS capability to share a “pointer” to the record and the record |
| Publishing System  (Data Processor) | The technically accredited or commissioned (deploying) IT system publishing data via the NRLS API message |
| Consuming Organisation  (Data Controller for its own systems and data and Joint Data Controller for NRLS) | The healthcare organisation consuming to patient information shared via the NRLS APIs, reading the “pointer” and then, potentially, viewing the record. Patient data is passed from the publishing organisation on the basis of Data Controller to Data Controller exchange. |
| Consuming System  (Data Processor) | The technically accredited or commissioned (deploying) IT system consuming data via the NRLS API messages |
| NHS Digital  (Joint Data Controller) | NHS Digital provides the NRLS service, including holding the pointers and audit trail and managing the configuration that determines which organisations can use the service  NHS Digital “on boarding” process establishes governance arrangements to underpin Joint Data Controller status |
| Validation | FHIR message will be validated on receipt against technical and business rules |

Table 1. NRLS Actors and Components

Figure 1 on page 7 shows the different parts of the wider DIP. In later phases, NRLS will share many messages and functions with other DIP capabilities.

## National Record Locator Service Information Flows

The NRLS interoperability solution enables an organisation to exchange patient information at the point of care through use of record “pointers” and the capacity to pull the relevant part of the patient record from the publishing organisation to the care staff in the consuming organisation.

For NRLS there are 3 data flows:

|  |  |
| --- | --- |
| Data flow | Type of data |
| Creating record “pointer” | * NHS number of patient * Organisation providing care with part of the patient care record available for sharing * Date of placing of “pointer” * Date of creation of part of the patient record available for sharing   This information is not visible within NHS Digital or to any other party unless the relevant API message for viewing record “pointer” is invoked. |
| Viewing the record “pointer” | Query using NHS number provides the following information back to the staff member using the systems that invokes the API:   * Organisation providing care with part of the patient care record available for sharing * Date of creation of part of the patient record available for sharing   *See screen shot in Appendix D* |
| Pulling the record across | Patient record is available to the staff member using the systems that invokes the API:   * Part of the clinical care record prepared for sharing * Date of creation *See screen shot in Appendix D* |

Table 2. Type of in formation in NRLS data flows

This information is identifiable and contains confidential information in terms of Data Protection and Common Law.

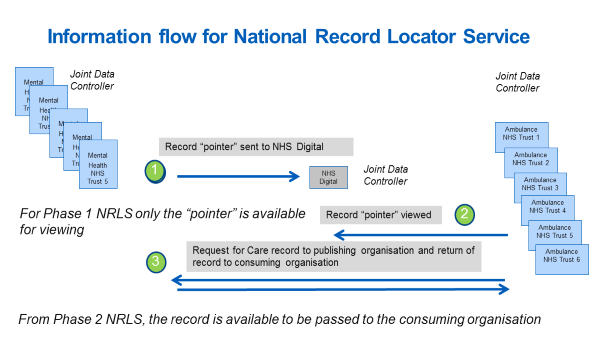


Figure 3 Information flows for National Record Service Locator

NRLS information is processed as follows:

**Phase 1**

1. Record “pointer” is published from a health care organisation to NRLS, “pointer” is held by NHS Digital
2. Staff member employed by healthcare organisation (Ambulance) transmits NHS number to NRLS for search purposes for a patient. NRLS returns “pointer” information to staff member of healthcare organisation Healthcare organisation. Contact details of the care team are present in the “pointer”

**Phase 2**

1. Staff member employed by healthcare organisation (Ambulance) proceeds to call record from healthcare organisation (Mental Health). Record is returned to the staff member of healthcare organisation (Ambulance)

There are two ways to access NRLS for Phase 1, use of a local patient information system that has been enabled to view pointers and retrieve records and use of the Summary Care Record application, sometimes termed the National Portal.

# Impact on Privacy & Related Risks

This DPIA has been produced because NRLS will enable patient identifiable and confidential event information to be shared with other systems in different care settings. Information about individuals will be sent via the Spine Security Proxy managed by NHS Digital and disclosed to organisations and users who have previously not had routine access. As a result, patient information crosses the risk management frameworks of the publishing and consuming healthcare providers and of NHS Digital.

The following risks of misuse of patient data arise through use of NRLS from legal or illegal access breaking the obligations of the Data Protection, Common Law duty of Confidentiality and Data Guardian principles:

### Patients unaware that their data may be shared onwards by the publishing organisation using NRLS capabilities for their direct care

### Patient identifiable and confidential event information used for purposes other than direct care in the consuming organisation

### Patient identifiable and confidential information used for unassured use cases/clinical settings within direct care in the consuming organisation

### Patient identifiable and confidential information retained for longer than is necessary in the consuming organisation

### Patient record accessed by consumer systems without the necessary security framework in the consuming organisation

### Patient record accessed by end users without appropriate authorisation in the consuming organisation

### Patient record-sharing dissent preference overridden

### Patient record section privacy settings overridden

Another way of considering these risks is presented in Appendix A.

# Privacy Risk Management

## Publishing and Consuming Suppliers & Organisations

These are responsible for ensuring that information which has passed to them is processed according to the required legal and regulatory frameworks.

## Data-Sharing Agreements

The Data Controllers of the publishing organisations must have confidence that the consuming organisations to which the information flows will meet the necessary legal and regulatory frameworks. This confidence will be based on the NHS Digital process for gaining agreement to use of NRLS, sometimes called “on-boarding”. A ‘white list’ of participating healthcare organisations will be managed for Phase 1 NRLS. A Data-Sharing Group is created to represent this relationship within the Spine Security Proxy (SSP) which will reject interactions where the publishing and consuming organisations are not members of the same Data-Sharing Group.

## NHS Digital Responsibilities

NHS Digital is a Joint Data Controller with participating organisations that publish and consume record pointers. NHS Digital is responsible for:

1. mitigation and management of the information security risks incurred by Spine processing (SSP)
2. assessment of technical conformance of publisher and consumer system use of the FHIR messages, including the testing of information security controls (validation)
3. assuring that Publishing and Consuming systems are meeting the necessary information governance and information security requirements
4. defining and assuring the Target Operating Model (TOM) with which Commissioning ‘approval’ must comply and which is required for live deployment; this includes the necessary framework requirements, e.g. Usage and Settings Statements and IG requirements

## Risk Mitigation Controls

Whilst the risks identified previously can never be eliminated completely, they are addressed and minimised through the following controls:

| **Risk** | **Description/Controls** | **Responsibility With:** |
| --- | --- | --- |
| **4.1** | Patients unaware that their data may be shared using NRLS for their direct care |  |
| Controls | As part of the “on boarding” processes, participating publishing and consuming organisations will be required to notify their patients of the information sharing potential and the constraints within which this will take place | Publishing and consuming organisations |
|  | The publishing and consuming organisations will be required to confirm these activities to NHS Digital Solutions Assurance as part of the deployment authorisation`  The exact methods, content, and extent of the notification to patients to be confirmed following consultation | Publishing and consuming organisations  Registration organisation (NHS Digital) |
| Result | Patients made aware of potential that their information will be shared according to the defined framework |  |
| **4.2** | **Patient identifiable and confidential information used for purposes other than direct care** |  |
| Controls | All NRLS documentation and guidance states that this information sharing is for the purposes of direct care only  Publishing and consuming organisations will need, as part of the NHS Digital Target Operating Model (TOM), to define Usage and Settings for approval by NHS Digital and publishing and consuming organisation Information Asset Owners | Consuming organisations  NHS Digital |
| Result | Consuming organisation commit to use patient event information for direct care purposes only |  |
| **4.3** | **Patient identifiable and confidential information used for unassured use cases/clinical settings within direct care** |  |
| Controls | As with 4.2 | As with 4.2 |
| Result | Consuming organisation commit to use patient event information for assured use cases/clinical settings within direct care | Consuming organisations |

|  |  |  |
| --- | --- | --- |
| **4.4** | Patient identifiable and confidential information is out of date and/or retained for longer than is necessary |  |
| Controls | Consuming organisation are committed to the NHS Records Management Code of Practice which includes retention schedules for all types of records.  This commitment is reflected in the “on boarding” documents and process. | Consuming organisations  NHS Digital |
| Result | Consuming organisation commit not to hold patient event information for longer than is necessary |  |
| **4.5** | Patient record accessed by consumer systems without the necessary security framework |  |
| Controls | Consuming organisation and systems must be NHS Data Security and Protection Toolkit compliant, and meet national requirements for Technical (Endpoint) Security  The NRLS TOM assurance process for publishing and consuming organisation requires suppliers to evidence their Information Security Management System (ISMS) and compliance with the standard BS ISO/IEC 27001:2005 BS7799-2:2005 | Consuming organisations  NHS Digital |
| Result | Consuming organisation commit to use of patient event information within acceptable access control functions |  |
| **4.6** | Patient record accessed by end users without appropriate authorisation |  |
| Controls | Consuming organisations must be NHS Data Security and Protection Toolkit compliant.  Consuming organisations systems must incorporate appropriate User Authentication and Authorisation controls either compliant with national RBAC requirements, or local equivalent  Evidence of this to be submitted as part of the TOM to NHS Digital Solutions Assurance.  NRLS will align where possible to other solutions being developed, for example the Strategic Authentication programme. | Consuming organisations |
| Result | Consuming organisation commit to use of patient event information within acceptable access control functions |  |

|  |  |  |
| --- | --- | --- |
| **4.7** | Patient record-sharing dissent overridden |  |
| Controls | NRLS guidance incorporated into the TOM specifies patient preference for sharing is managed by the publishing organisation.  **Implied Consent**  The publishing organisation will pass patient event information if explicit dissent is not recorded. | Publishing organisations |
| Result | Publishing organisations commit to use of appropriate preference for sharing functions |  |
| **4.8** | Patient record section privacy settings overridden |  |
|  | The publishing organisation provider system must respect any patient event information which has been marked as not to be shared | Providing Supplier |
| Result | Publishing organisations commit to use of appropriate preference for sharing functions |  |

Table 3. Mitigation of risks

An additional presentation of risks and their mitigations is provided in Appendix A, this is based on hazard analysis and positions IG perspectives in the same methodology as clinical safety.

An appropriate access control model is fundamental to mitigation of risks, detail of this model is presented in Appendix B.

GDPR compliance is listed in Appendix C and screen shots to illustrate information flows are presented in Appendix D.

# Conclusions

The NRLS service has been developed to support national sharing for direct care purposes within the constraints of the necessary Information, Security and Privacy Governance frameworks. Principles of privacy by design have been followed.

NHS England is preparing an national Information Governance Framework for Local Health Care Record exemplars and changes may be needed to the NRLS IG and access control model as this work concludes and, also, experience is gained from use of the NRLS service across the NHS.

# Appendix A –– IG hazard analysis

A set of risks are identified for DIP capabilities:

* Patients unaware that their data may be shared using NRLS for their direct care
* Patient identifiable and confidential information used for unassured use cases/clinical settings within direct care
* Patient identifiable and confidential information is out of date and/or retained for longer than is necessary
* Patient record accessed by consumer systems without the necessary security framework
* Patient record accessed by end users without appropriate authorisation
* Patient record-sharing dissent overridden
* Patient record section privacy settings overridden

To fit risk analysis with the clinical safety assurance method, these are mapped against the following, generic hazards:

* Data loss of sensitive data
* Unauthorised access to data
* System exploited

|  |  |
| --- | --- |
| **Risk** | **Hazard** |
| Patients unaware that their data may be shared using NRLS for their direct care | * Loss of sensitive data * Unauthorised access to data * System exploited |
| Patient identifiable and confidential information used for purposes other than direct care | * Loss of sensitive data * Unauthorised access to data * System exploited |
| Patient identifiable and confidential information used for unassured use cases/clinical settings within direct care | * Loss of sensitive data * Unauthorised access to data * System exploited |
| Patient identifiable and confidential information is out of date and/or retained for longer than is necessary | * Unauthorised access to data |
| Patient record accessed by consumer systems without the necessary security framework | * Unauthorised access to data |
| Patient record accessed by end users without appropriate authorisation | * Unauthorised access to data * System exploited |
| Patient record-sharing dissent overridden | * Unauthorised access to data * System exploited |
| Patient record section privacy settings overridden | * Unauthorised access to data * System exploited |

Table 4 Risks and hazards

These hazards are illustrated in Figure 4, 5 & 6. Threats (marked in blue) are mitigated by controls and consequences (marked in red) by countermeasures.

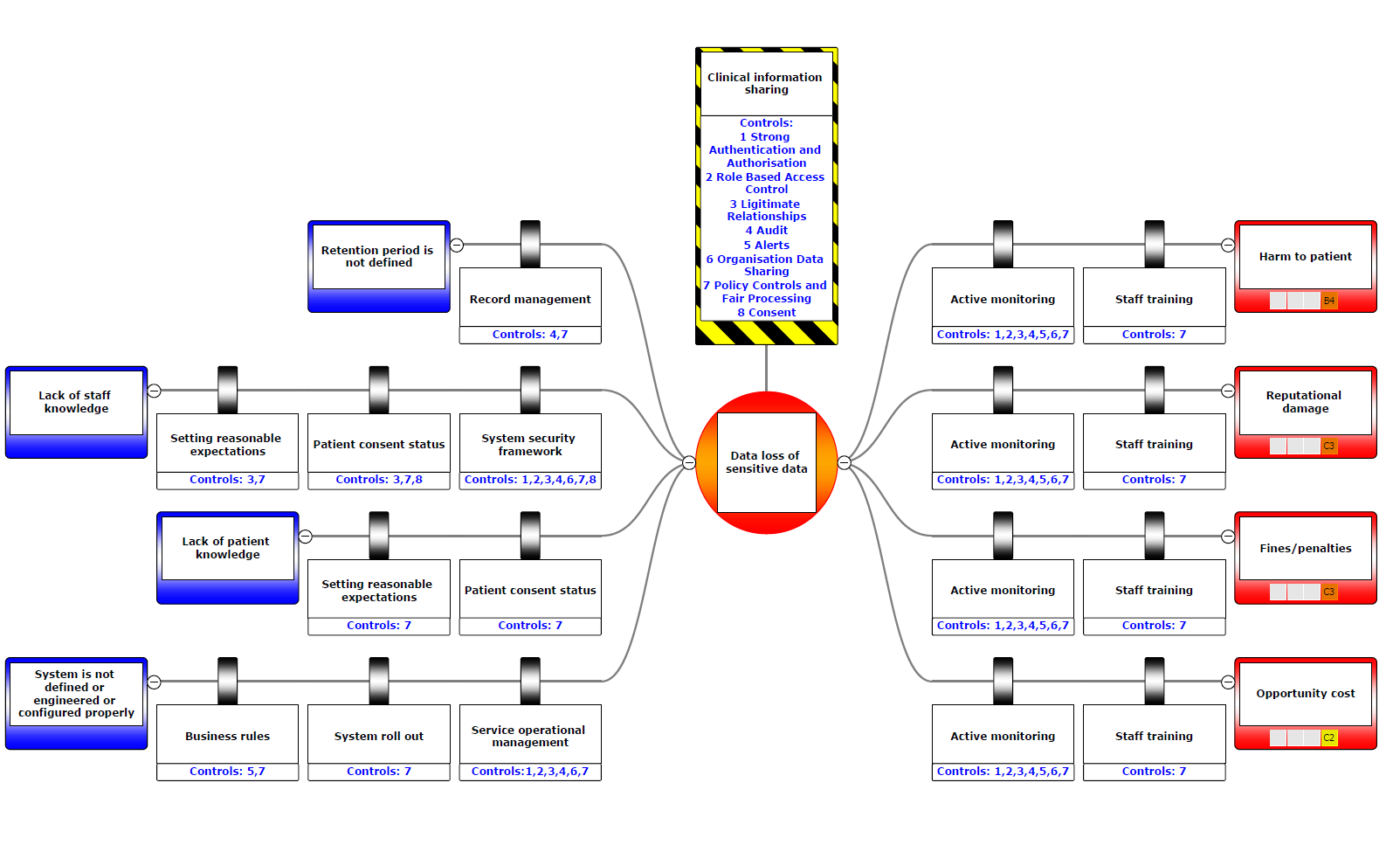


Figure 4. Hazard, Data loss of sensitive data – annotated with controls

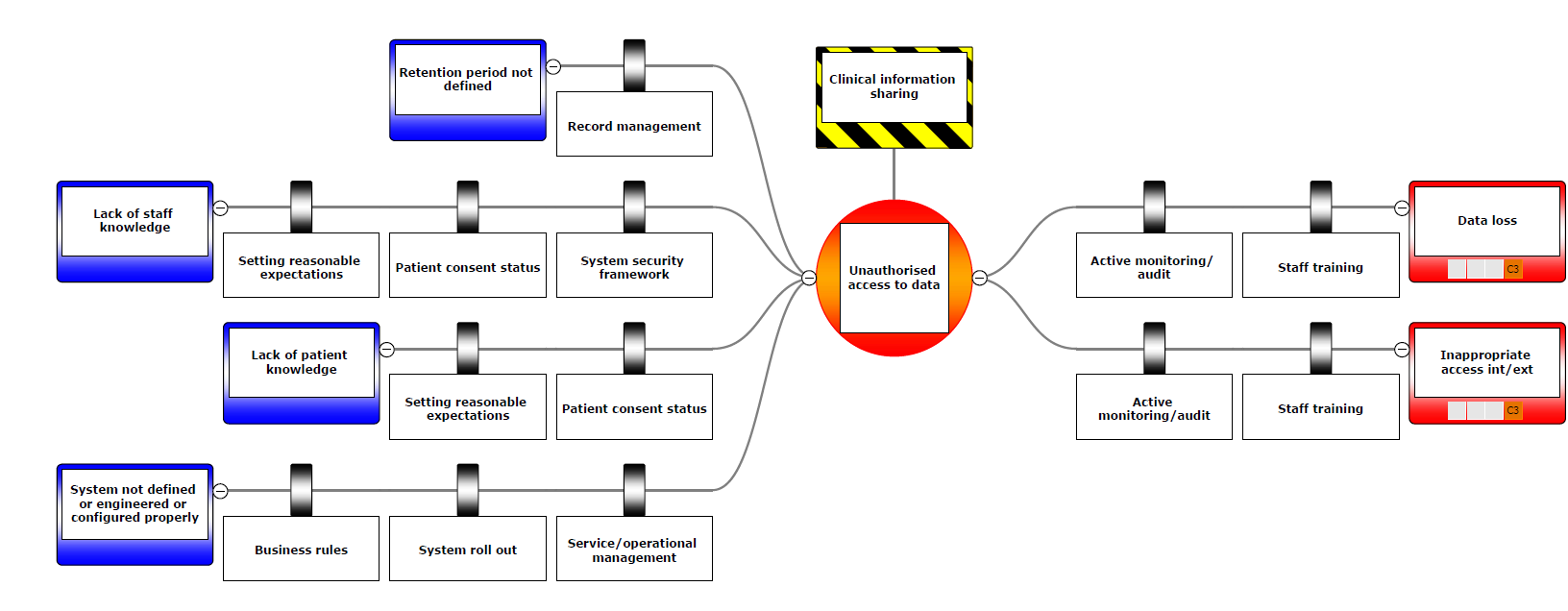


Figure 5. Unauthorised access to data

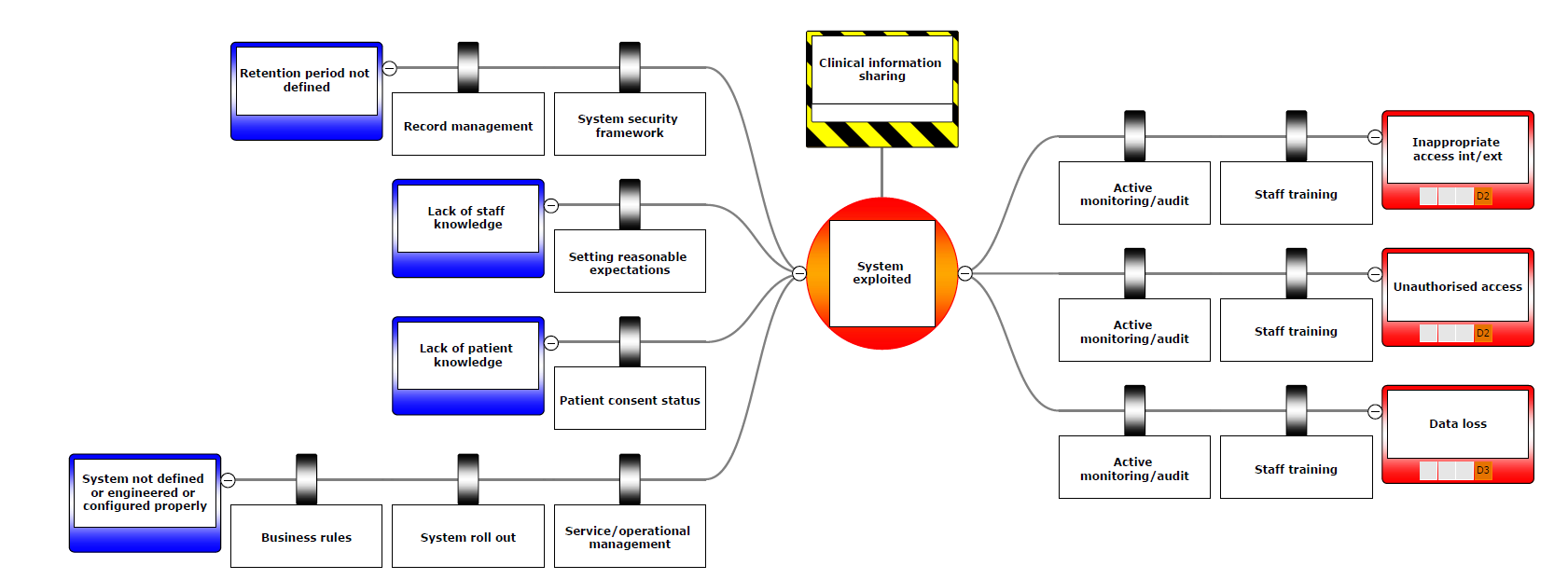


Figure 6. System exploited

# Appendix B – Application of access control model

For all DIP capabilities an access control is used to maintain confidentiality and security of patient records. The model covers people, procedures and technology:

* Strong Authentication and Authorisation
* Role Based Access Control
* Legitimate Relationships
* Audit
* Alerts
* Organisation Data Sharing
* Policy Controls and Fair Processing
* Consent



Figure 7. NHS Digital Access Controls

For some DIP capabilities, e.g. NRLS and GP Connect, patient data is transferred securely from local care provider systems to NHS Digital where it is passed to other accredited local care provider systems managed such as A&E departments, hospital pharmacies, NHS 111 and GP out of hours services and walk in centres.

For the National Portal patient data is transferred securely to NHS Digital and made available through a national browser application managed as a service by NHS Digital.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| DIP IG Controls | Interaction | Timescale | Strong Authentication and Authorisation | Role Based Access Control | Legitimate Relationships | Audit | Active Monitoring and Alerts | Data Sharing Agreements (& Org Code Structure) | Policy Controls and Fair Processing | Exclusion of parts of records | Consent |
| Registry/Repository Pattern (a.k.a. National Record Locator)  NOTE: Index component only (for retrieval see National Broker). | Publish Events | Short | Local system control (TOM/CAP) | Local system control (TOM/CAP) | Based on subscription rules | NHS Digital (Splunk) & Local system audit | Not yet agreed as a requirement | Based on subscription rules | National agreement | Local system control (TOM/CAP) | Local system control – preference for sharing (TOM/CAP) |
| Med/Long | Not yet agreed | Not yet agreed | Not yet agreed | As above | As above | Based on subscription rules | National agreement | As above | Not yet agreed |
| Consume Events | Short | NHS Smartcard or use of national identity (Strategic Authentication) | Local system control (TOM/CAP) | Based on subscription rules | As above | As above | Based on subscription rules | National agreement | As above | Publishing organisation control |
| Med/Long | Strat AuthN | Strat AuthZ | Based on subscription rules | As above | As above | Based on subscription rules | National agreement | As above | Not yet agreed |

Table 5. Application of access controls for NRLS

When access to NRLS is through use of the local systems integrated with NRLS, local system will

* Use national strong authentication functions of NHS Smartcards (although local authentication is permissible for Phase 1 all access to NRLS will be through the National Portal)
* Use Role-based access control, legitimate relations and audit functions embedded within the local application

When access to NRLS is through use of the National Portal (Summary Care Record application), existing national services will be used:

* Strong authentication functions of NHS Smartcards
* Use Role-based access control, legitimate relations and audit functions embedded within the Summary Care Record application

# Appendix C – GDPR compliance for NHS Trusts & NHS Digital

The purpose of sharing patient information is direct care

In the context of GDPR, sharing is on the basis of: -

* Article 6(c) – *“lawfulness of processing “… “processing is necessary for compliance with a legal obligation to which the controller is subject”*
* Article 9(2)(h)) – “*processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards …”*
* Article (17(3)(c) there is an exemption on the right to erasure where the ‘medical purposes’ condition applies) where processing is necessary in the public interest and was originally processed under Article 9(2)(h)

Common Law Duty of Confidentiality: -

* The legal basis for sharing patient data for direct care is informed implied consent with opt out. Where the patient lacks capacity a best interest decision will be made

For both NHS Trusts & NHS Digital staff will hold the following roles:

* Privacy Officer - responsible for the organisation's Privacy Policy and Procedures
* Information Asset Owner – DPIA agreed
* Service manager – System Level Security Procedure (SLSP) agreed

The NHS Digital Transparency checklist completed for NRLS is available on request.

# Appendix D – “Mock up” screen shots of information flows

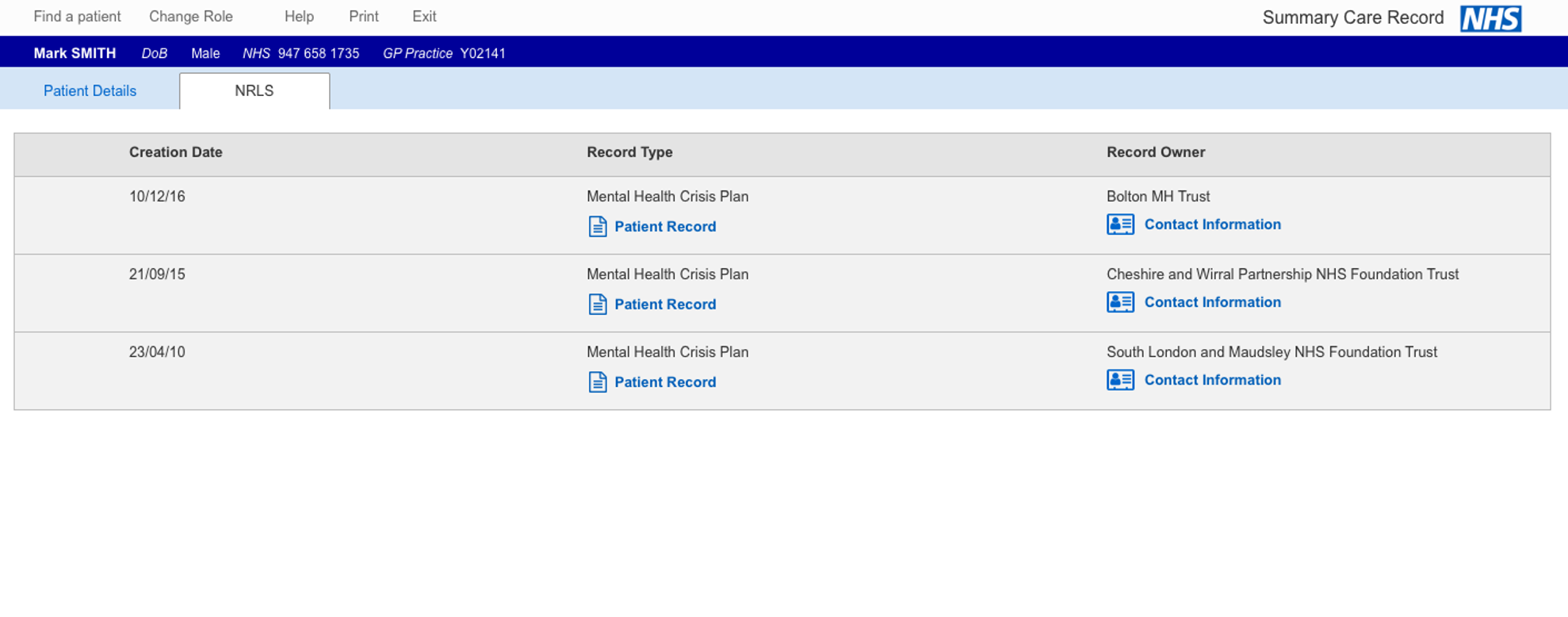


Figure 8. Phase 1 NRLS – list of records for a patient

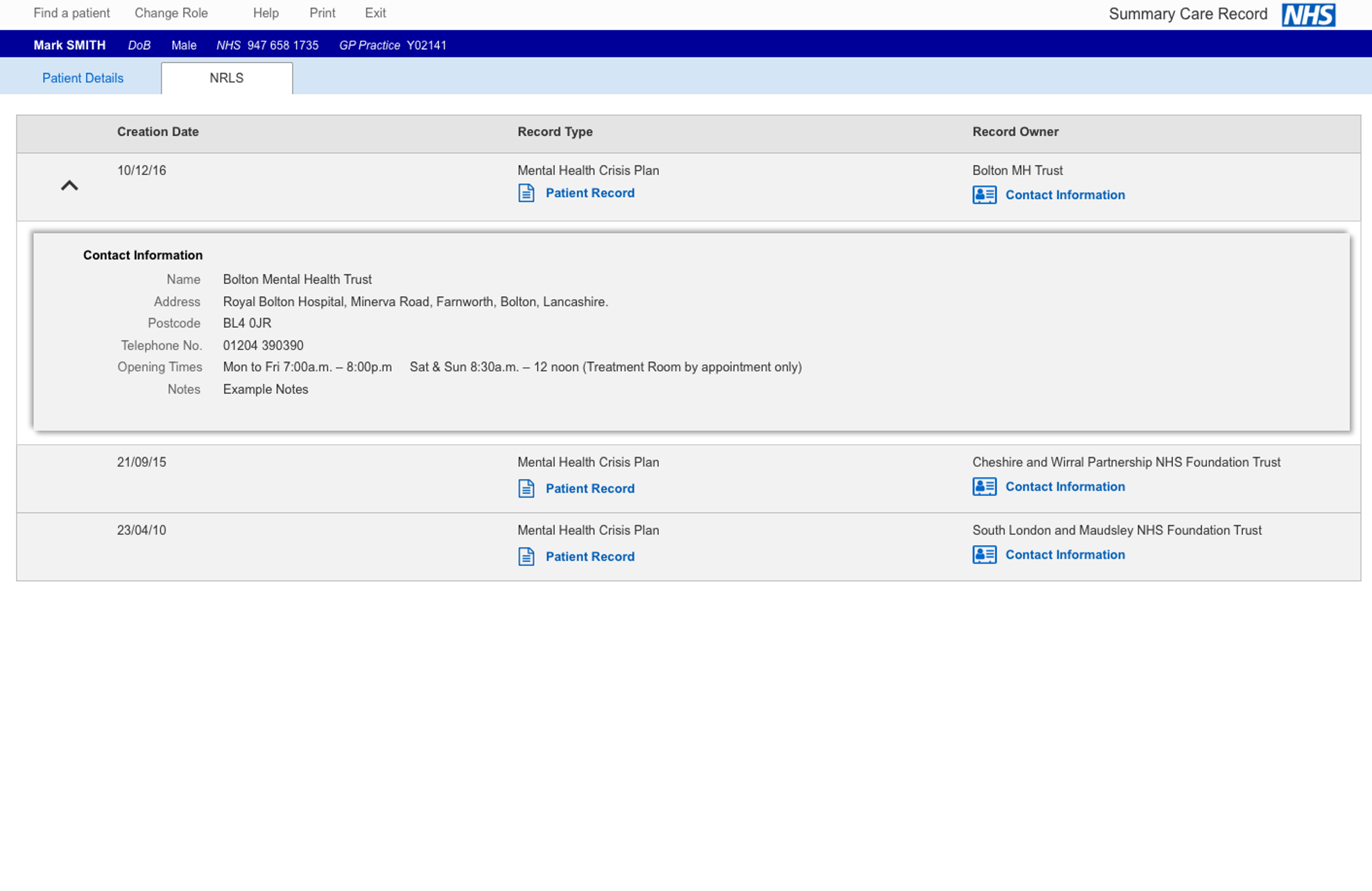


Figure 9. Phase 1 NRLS – contact details for a the care team of the patient

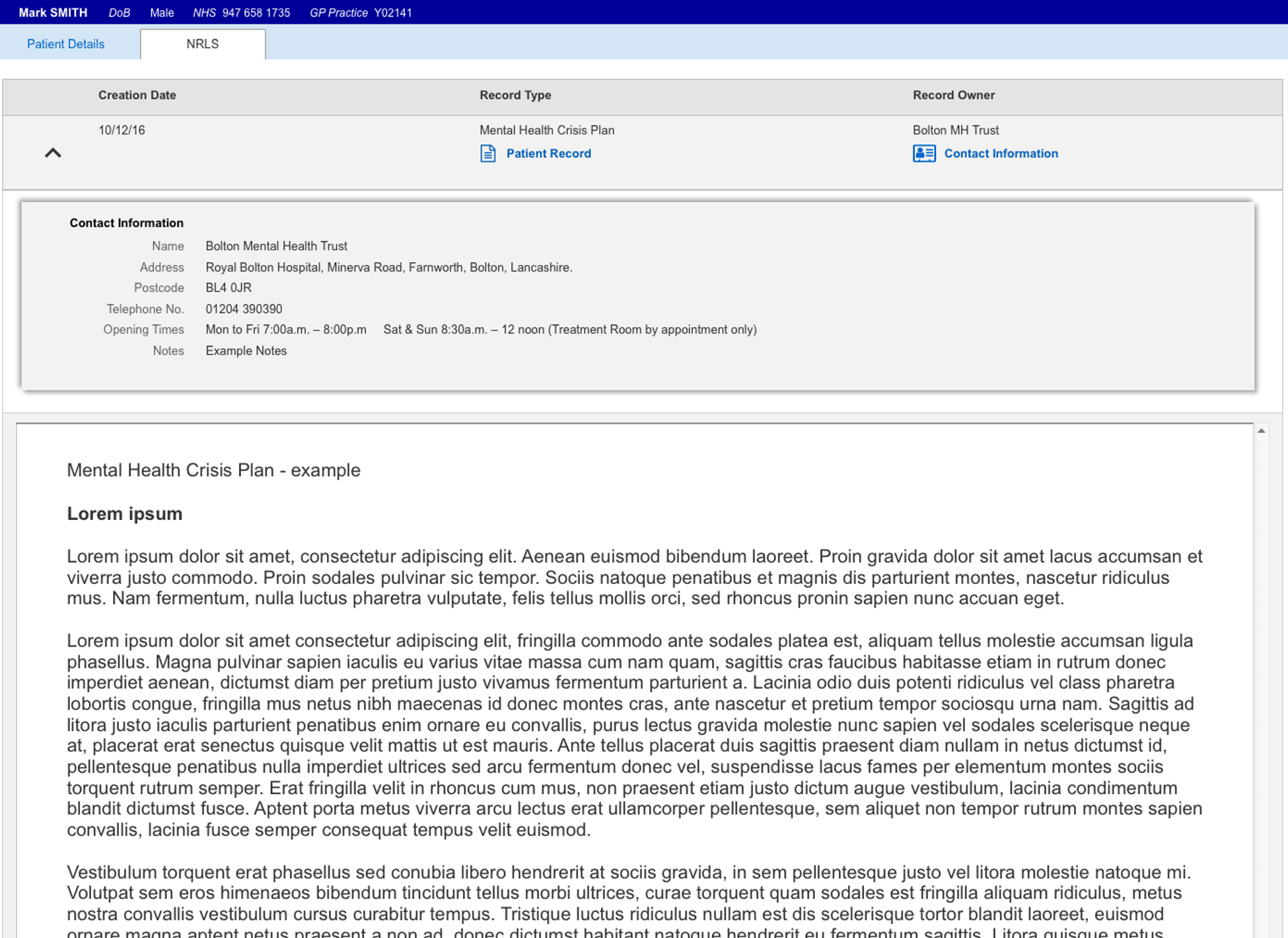


Figure 10. Phase 2 NRLS – detail of the care plan returned