|  |  |  |  |
| --- | --- | --- | --- |
| 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 | **WIP** |
| Owner | **Dave Jarvis** | Version | **0.4** |
| Author | **Stephen Elgar** | Version issue date | **27/03/2018** |

**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 |

Reviewers

This document must be reviewed by the following people:

|  |  |  |  |
| --- | --- | --- | --- |
| Reviewer name | Title / Responsibility | Date | Version |
| Amir Mehrkar | Digital Interoperability Platform (DIP)  Clinical Lead |  |  |
| Raman Behl | Clinical Lead |  |  |
| David Jarvis | National Record Locator Service (NRLS) Project Manager |  |  |
| Mike Walker | DIP Head of Programme |  |  |
| Adam Hatherly | Domain D Technical Architect |  |  |
| Will Weatherall | NRLS Technical Architect |  |  |
| Hadleigh Stollar | NRLS Programme Manager |  |  |

Approved by

This document must be approved by the following people:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Name | Signature | Title | Date | Version |
| Amir Mehrkar |  | Clinical Lead |  |  |
| Raman Behl |  | Clinical Lead |  |  |
| Mike Walker |  | DIP Head of Programme |  |  |

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 – eg 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 | Role identified in the Data Protection Act for the organisation processing data under instruction from a Data Controller |
| 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 – ie 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 |

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](#_Toc504075206)

[1.1 Purpose of Document 5](#_Toc504075207)

[1.2 Legal, Regulatory Framework 5](#_Toc504075208)

[1.3 Consultation & Assessment Approach 6](#_Toc504075209)

[2 National Record Locator Service 6](#_Toc504075210)

[2.1 Background - Digital Interoperability Platform 6](#_Toc504075211)

[2.2 National Record Locator Service Actors & Components 8](#_Toc504075212)

[2.3 National Record Locator Service Information Flows 11](#_Toc504075213)

[3 Impact on Privacy & Related Risks 13](#_Toc504075214)

[4 Privacy Risk Management 13](#_Toc504075215)

[4.1 Publishing and Consuming Suppliers & Organisations 13](#_Toc504075216)

[4.2 Data-Sharing Agreements 13](#_Toc504075217)

[4.3 NHS Digital Responsibilities 14](#_Toc504075218)

[4.4 Risk Mitigation Controls 14](#_Toc504075219)

[5 Conclusions 17](#_Toc504075220)

[6 Appendix A –– IG hazard analysis 18](#_Toc504075221)

[7 Appendix B – Application of access control model 20](#_Toc504075222)

[8 Appendix C – GDPR compliance for NHS Trusts & NHS Digital 22](#_Toc504075223)

[9 Appendix D - Consultation questions 23](#_Toc504075224)

[10 Appendix D – “Mock up” screen shots of information flows 25](#_Toc504075225)

# Introduction

## Purpose of Document

National Record Locator Service (NRLS) is one of several capabilities of the Digital Interoperability Platform (DIP), this document considers potential information security and confidentiality risks for this capability and how they are mitigated. The current patient record on Personal Demographic Service (PDS) contains the registered GP. With the National Record Locator Service, a note of care events will be added. As with GP Connect in which the registered GP is used, these will enable a query-based view of the patient record returned to the point of care through the local patient record system. Only the locator is held centrally.

The document is a Data Protection Impact Assessment (DPIA). A DPIA has already been prepared for all DIP capabilities.



This document 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 required 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 not yet complete. This version of the DPIA is prepared to enable consultation with NHS Trusts that are planning to be early implementers – see questions in Appendix D.

## Legal, Regulatory Framework

DPIA are a tool which help organisations identify the most effective way to comply with the new version of the Data Protection Act in prospect in May 2018 indicated by the General Data Protection Regulation (GDPR). GDPR guidance is not complete but it is understood that most of the 1998 Act remains relevant. For the most part this document refers to the existing Act but compliance with the new one is also stated. The format of this document includes the approach of a Privacy Impact Assessment and addresses Common Law Duty of Confidentiality obligations 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’.

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 are stated in Appendix C.

## 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

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 for NRLS 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

Consultation with National stakeholders is planned as part of preparation of data sharing framework for direct care as opportunity arises

# 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.

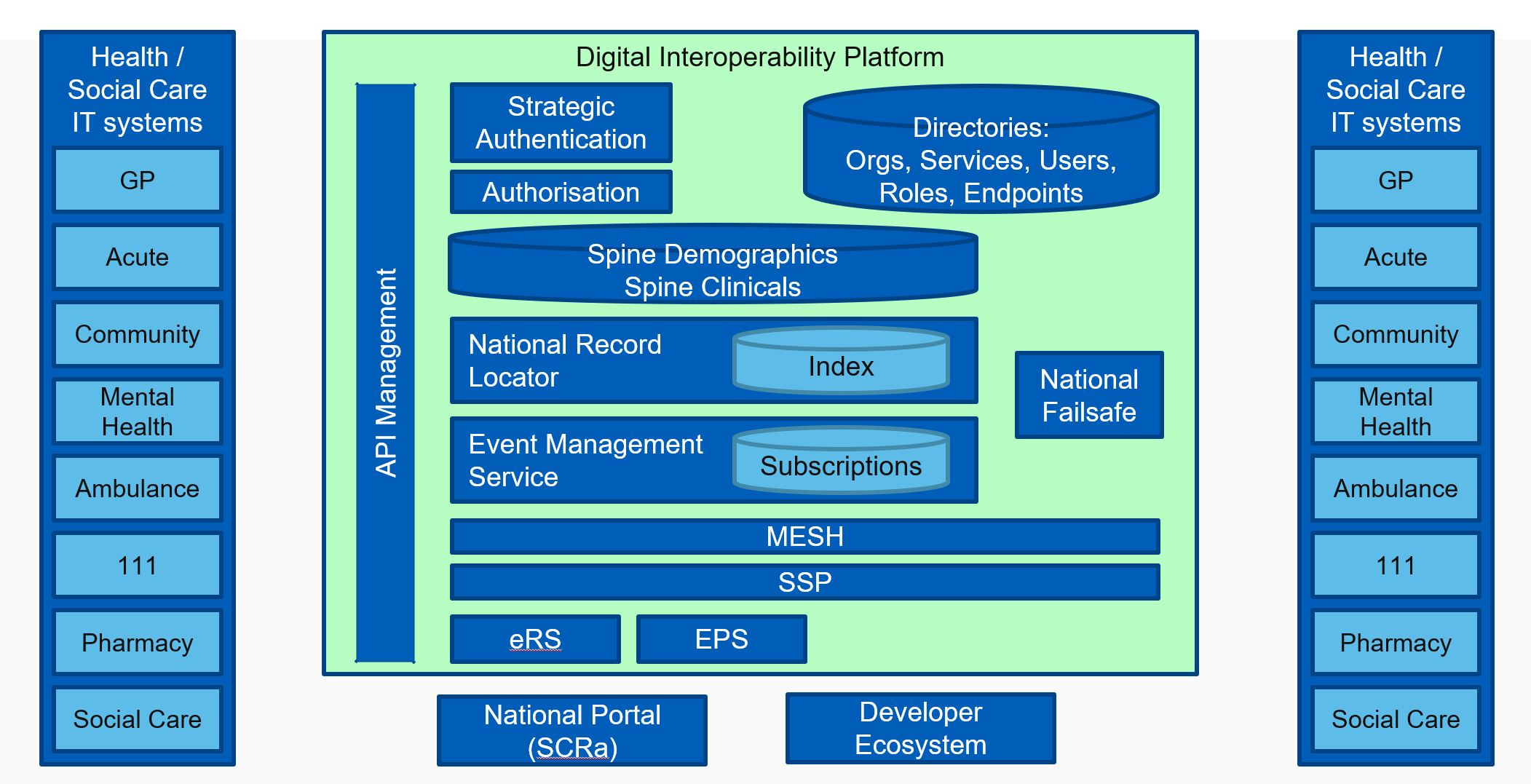


Figure 1 – Digital Interoperability Platform

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 an additional 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

A 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.

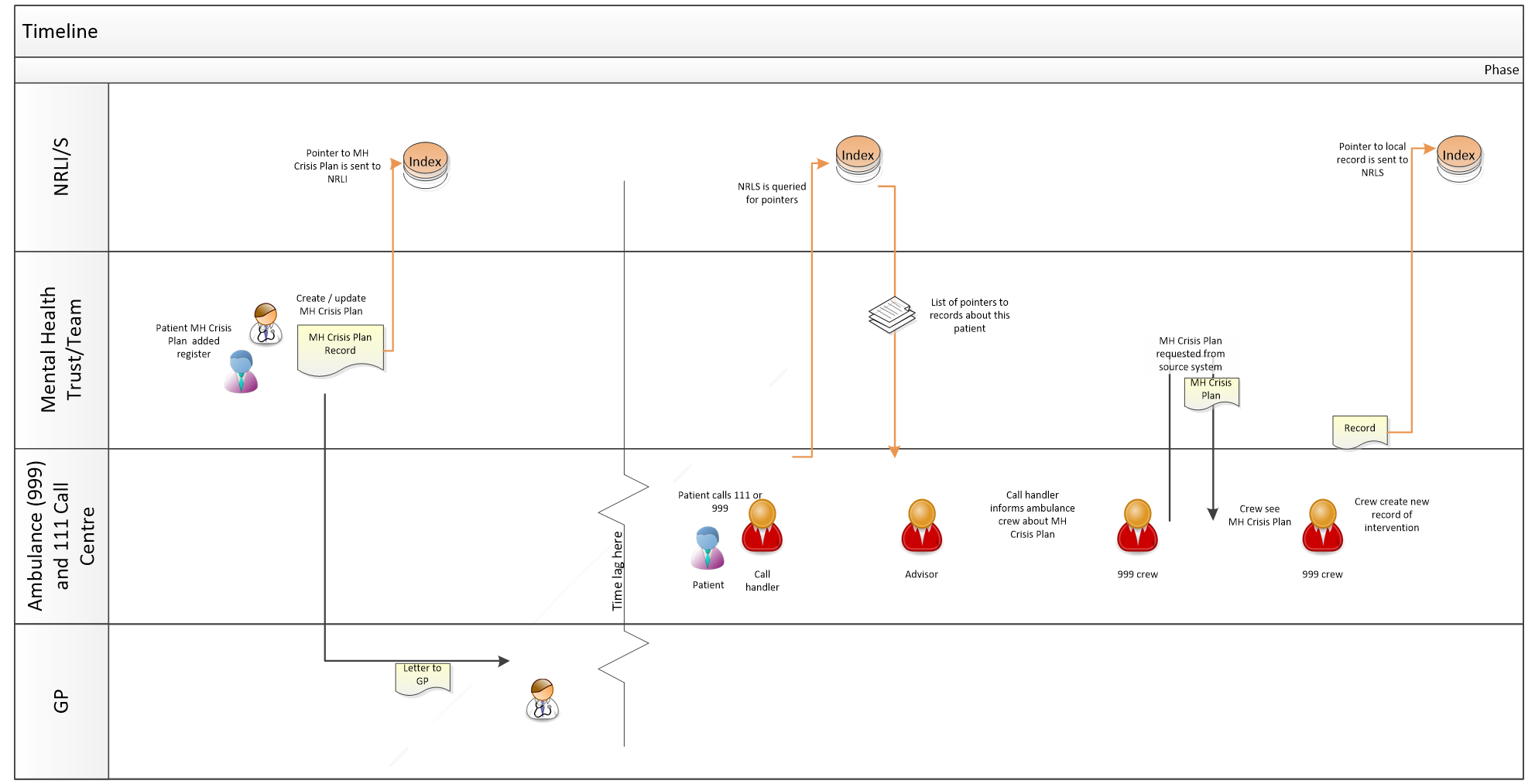


Figure 2: Example NRLS Use Case: Urgent and Emergency Care – Mental Health Crisis Plans

|  |  |
| --- | --- |
| **What/Who** | **Role** |
| Healthcare Organisation | May be a publishing or consuming organisation |
| Publishing Organisation  (Data Controller) | 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) | 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  (Data Processor) | NHS Digital provides the NRLS service |
| 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. NRLS shares 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 to the care staff in the consuming organisation.

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.

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.  *See Appendix E – screen shot* |
| 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 Appendix E* |
| 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 Appendix E* |

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.

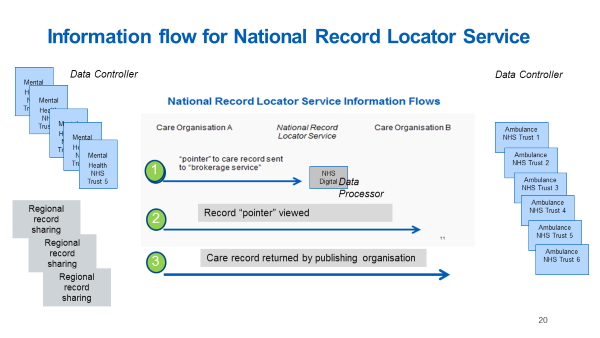


Figure 3 Information flows for National Record Service Locator

NRLS information is processed as follows:

1. Record “pointer” is published from a health care organisation to NRLS held by NHS Digital
2. Staff member employed by healthcare organisation (Ambulance) searches NRLS for a patient and returns “pointer” information and is able to view this
3. Staff member employed by healthcare organisation (Ambulance) proceeds to call record from healthcare organisation (Mental Health)

Where NRLS capabilities are enabled, all the patients receiving care from publishing organisations will potentially be affected.

Publishing, consuming organisations and NHS Digital will record the sharing of event information in their audit trails.

# Impact on Privacy & Related Risks

This DPIA has been produced because NRLS is enabling 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 described above.

## 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 use of a Data-Sharing Agreement between NHS Digital and publishing and consuming organisations.

A ‘white list’ of participating healthcare organisations is provided as part of the Target Operating Model (TOM). 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.

Work is expected on a National Framework for data sharing for direct care to which NRLS will align.

## NHS Digital Responsibilities

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 Statement, IG requirements such as for Data-Sharing agreement between Consumer and Provider organisations

## Risk Mitigation Controls

For compliance with GDPR the conditions for processing of personal and confidential patient information for direct care rest upon it being: -

* Lawful (e.g. care is undertaken by a health professional or by someone who is subject to an equivalent duty of confidentiality, there is an appropriate legal basis for the organisation, that the patients are made aware of this processing, that the organisation has appropriate security and confidentiality controls) - Article 6(c)
* For medical care purposes - Article 9(2)(h)
* There is an exemption on the right to erasure where the ‘medical purposes’ condition applies - Article (17(3)(c)

For compliance with 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

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

| **Risk** | **Description/Controls** | **Responsibility With:** |
| --- | --- | --- |
| **3.1** | 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 |  |
| **3.2** | **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, consuming organisations and registration 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 |  |
| **3.3** | **Patient identifiable and confidential information used for unassured use cases/clinical settings within direct care** |  |
| Controls | As with 3.2 | As with 3.2 |
| Result | Consuming organisation commit to use patient event information for assured use cases/clinical settings within direct care |  |

|  |  |  |
| --- | --- | --- |
| **3.4** | 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 |  |
| **3.5** | Patient record accessed by consumer systems without the necessary security framework |  |
| Controls | Consuming organisation and systems must be NHS IG 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 |  |
| **3.6** | Patient record accessed by end users without appropriate authorisation |  |
| Controls | Consuming organisations must be IG 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 |  |

|  |  |  |
| --- | --- | --- |
| **3.7** | 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, and within the context of a Data-Sharing Agreement held between the NHS Digital and all publishing and consuming organisations. | Publishing organisations  Publishing and consuming organisations  NHS Digital |
| Result | Publishing organisations commit to use of appropriate preference for sharing functions |  |
| **3.8** | 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 2. Mitigation of risks

An appropriate access control model is fundamental to mitigation of security and confidentiality risks. An additional presentation of risks and their mitigations for DIP capabilities including NRLS is provided in Appendix A. This is based on hazard analysis and is intended to position IG perspectives in the same methodology as clinical safety.

# Conclusions

The NRLS team seeks to be responsive to ongoing work being carried out by NHS England, and NHS Digital Domain D and J, and, within the developing strategic context of the ‘Digital Interoperability Platform’, enabling information for the purpose of direct care to be shared more easily, within the constraints of the necessary Information, Security and Privacy Governance frameworks.

# 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 2 Risks and hazards

These hazards are illustrated in Figure 1, 2 & 3 on following page. Threats (marked in blue in Figures 1-3) are mitigated by controls and consequences (marked in red in Figures 1-3) by countermeasures.

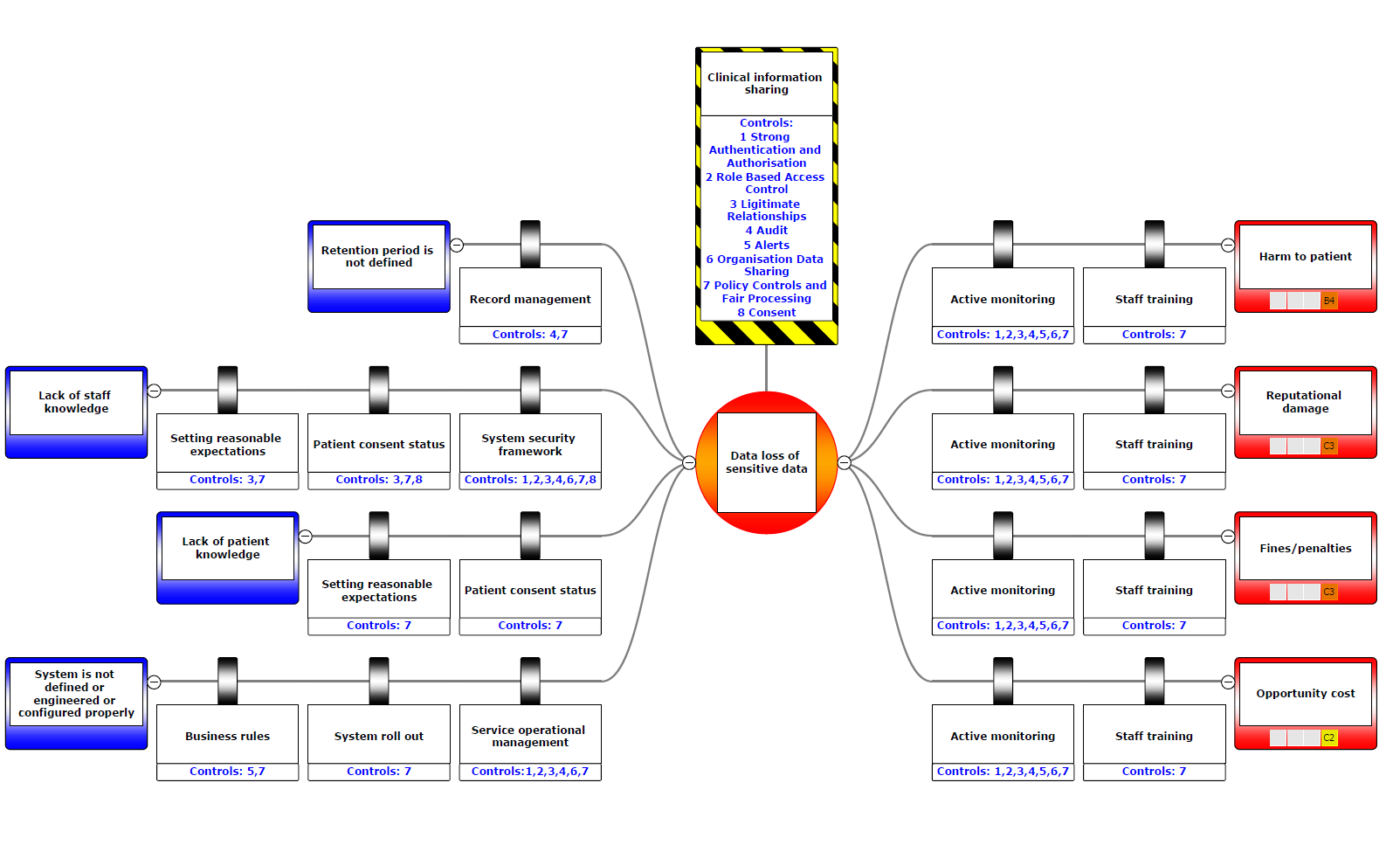


Figure 4. Hazard, Data loss of sensitive data – annotated with controls

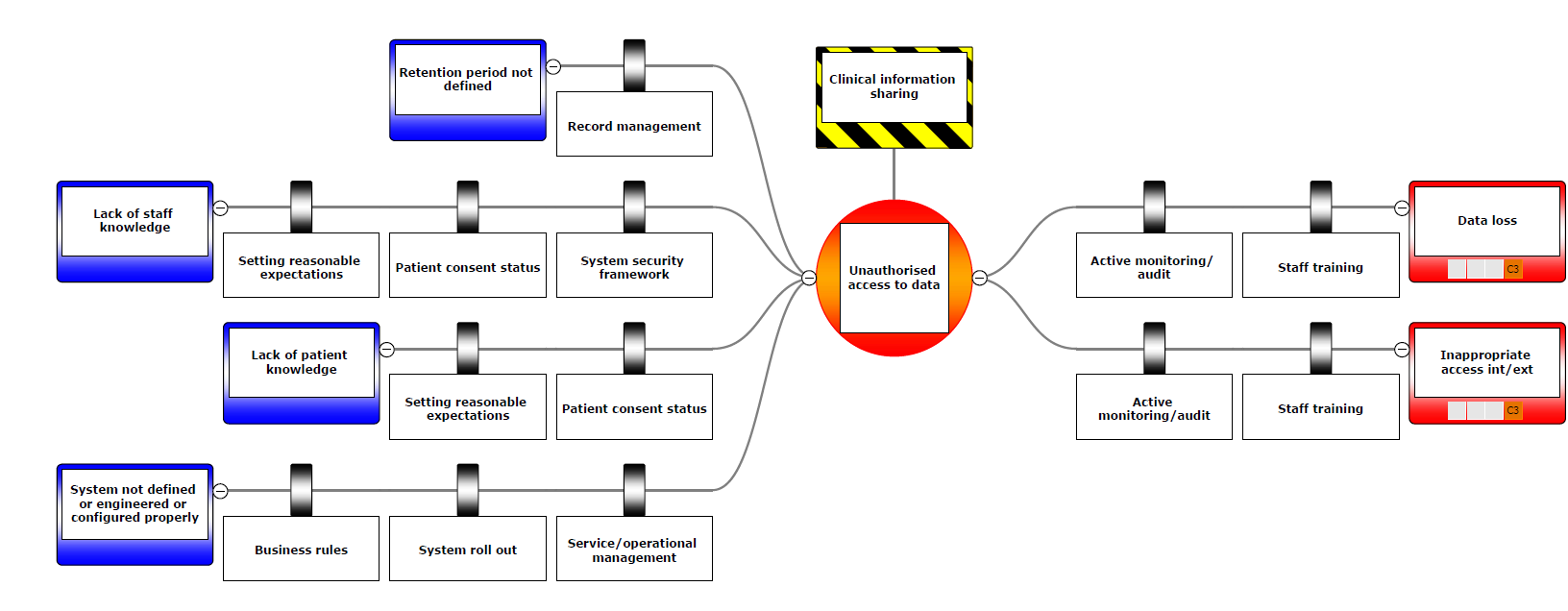


Figure 5. Unauthorised access to data

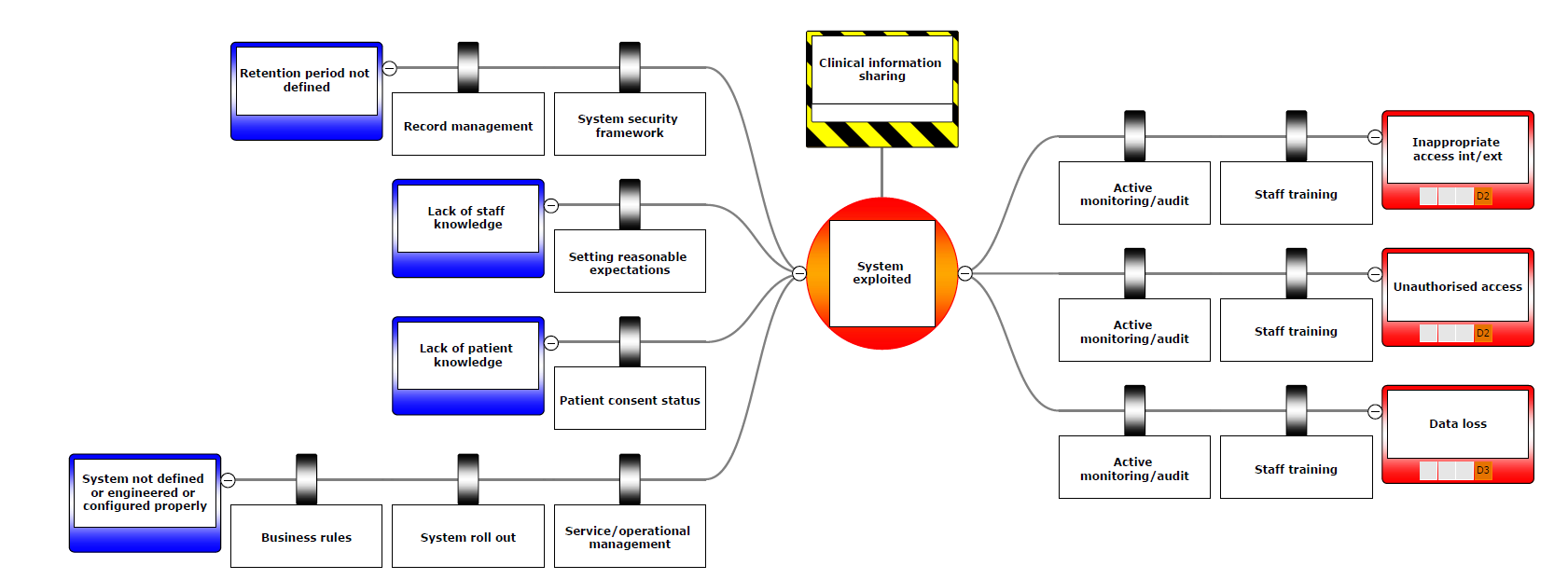


Figure 6. System exploited

# 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 NRLS, 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 3. Application of access controls for NRLS

# 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)

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 will also be shared between NHS Trusts & NHS Digital. Template attached: -



# Appendix D - Consultation questions

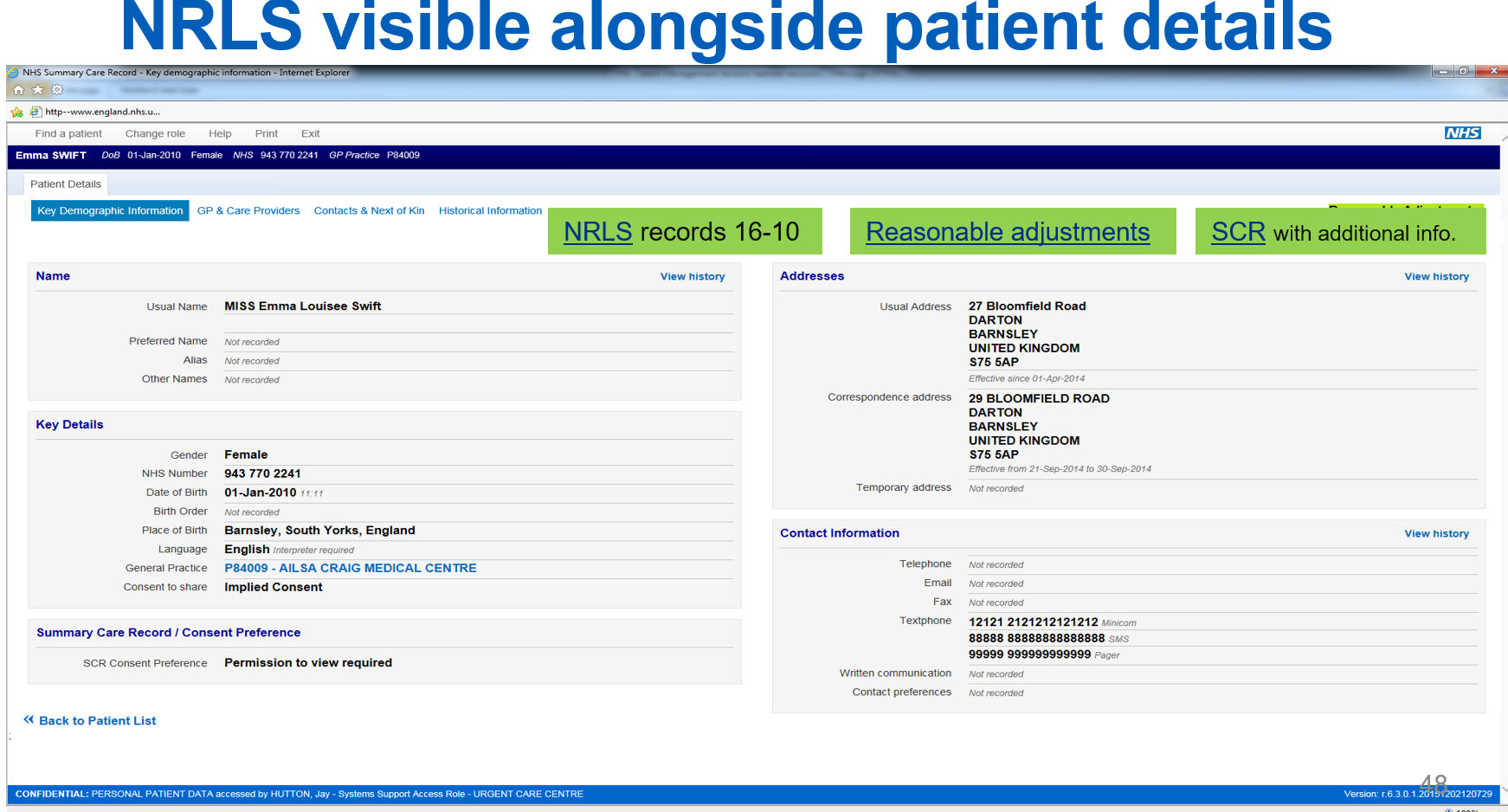
|  |
| --- |
| Questions for consultation for all DIP capabilities  Consent, is the following approach appropriate?   * Informed implied consent with opt out managed by publishing organisation * Informed implied consent with opt out mechanism managed nationally * Active consent for sharing managed by publishing organisation   Data Sharing Agreement (DSA) – which of these approaches should be followed?   * To follow good practice for DSA of existing regional partnerships * To follow expected national generic format * For NHS Digital to use national generic format to enable data to flow through DIP capabilities * To work towards a status of trusted parties as multiple point-to-point DSA are not practical for national infrastructure and services   Governance – assumption is that mechanisms for clinical oversight to be established for each DIP capability:   * These could be regional or national * Can existing groupings and mechanism be used, or should new ones be set up?   Active monitoring   * Is there support for NHS Digital to develop new services of Active monitoring?   Policy-based application of access controls in local patient information systems   * Many DIP capabilities concern messages interfaces between local patient information systems. As a result, a policy requirement for appropriate access controls in local patient information systems is an essential part of the overall approach to IG. |

|  |
| --- |
| Questions for consultation for **NRLS capabilities**  **For the patient**, is the following approach appropriate?   * A patient can expect each care organisation to be able to say where and to which organisation their information is shared (Privacy Notice) * A patient can ask that their care information is not shared * A patient can ask what part of their information can be and / or has been shared with what organisation? They can then ask the recieiving organisation who has seen their information?   **For the publishing organisation**, is the following approach appropriate?  *Data Controller options:*   * The publishing organisation is the Data Controller and the consuming organisation is the Data Processor and the DSA gives a description and limitation to the exchange of patient event information (NHS Digital is a Data Processor) * Both the publishing and consuming organisations are Data Controller and the DSA gives a description and limitation to the exchange of patient event information (NHS Digital is a Data Processor) * Both the publishing and consuming organisations are Joint Data Controllers and the DSA gives a description and limitation to the exchange of patient event information (NHS Digital is a Data Processor)   *Preference for sharing event information:*   * The publishing organisation must enable patients to be aware of how their information is shared and manage dissent preference or opt out from sharing   For the **consuming organisation**, is the following approach appropriate?   * The access control model of the patient information system provided by the supplier of the consuming organisation must deliver the key IG functions of   + Authentication   + Authorisation   + Role-based access control   + Legitimate relations   + An audit trail of access and create, amend delete * A policy requirement for a consuming organisation is to ensure that a care relationship exists with a patient for whom patient record is viewed. The expectation is that the data is deleted if there is no care relationship.   For NHS Digital, is the following approach appropriate?  *Data Sharing Agreement (DSA)*   * Manages a single DSA with both publication and consuming organisations   *Clinical Governance*  Manages the set-up of a group for IG and clinical oversight |

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



Figure 8. Screen shot – searching for a patient on NRLS



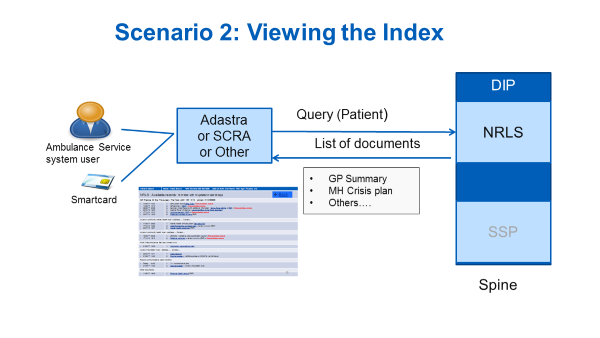


Figure 9. Screen shot – presence of NRLS-enabled record

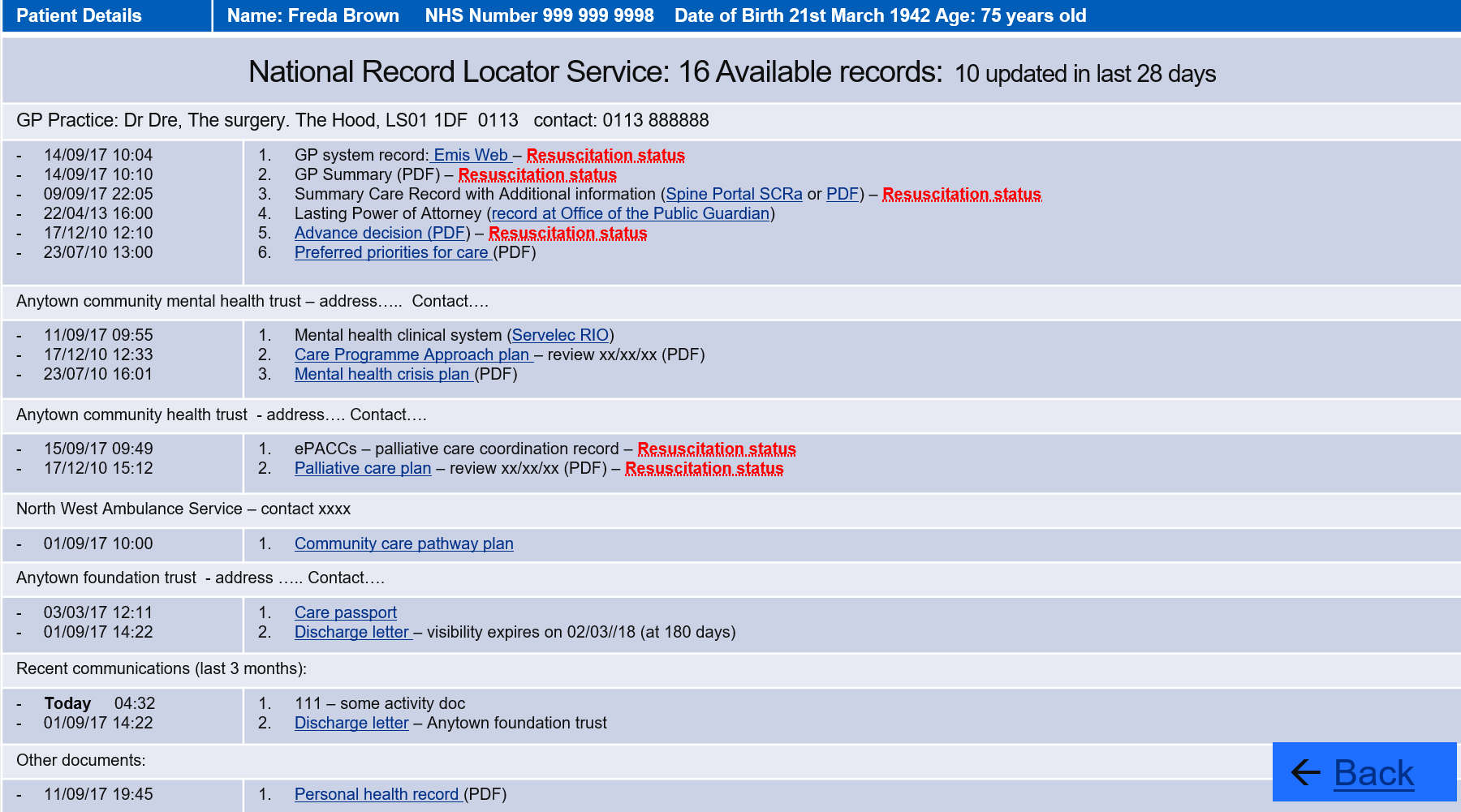
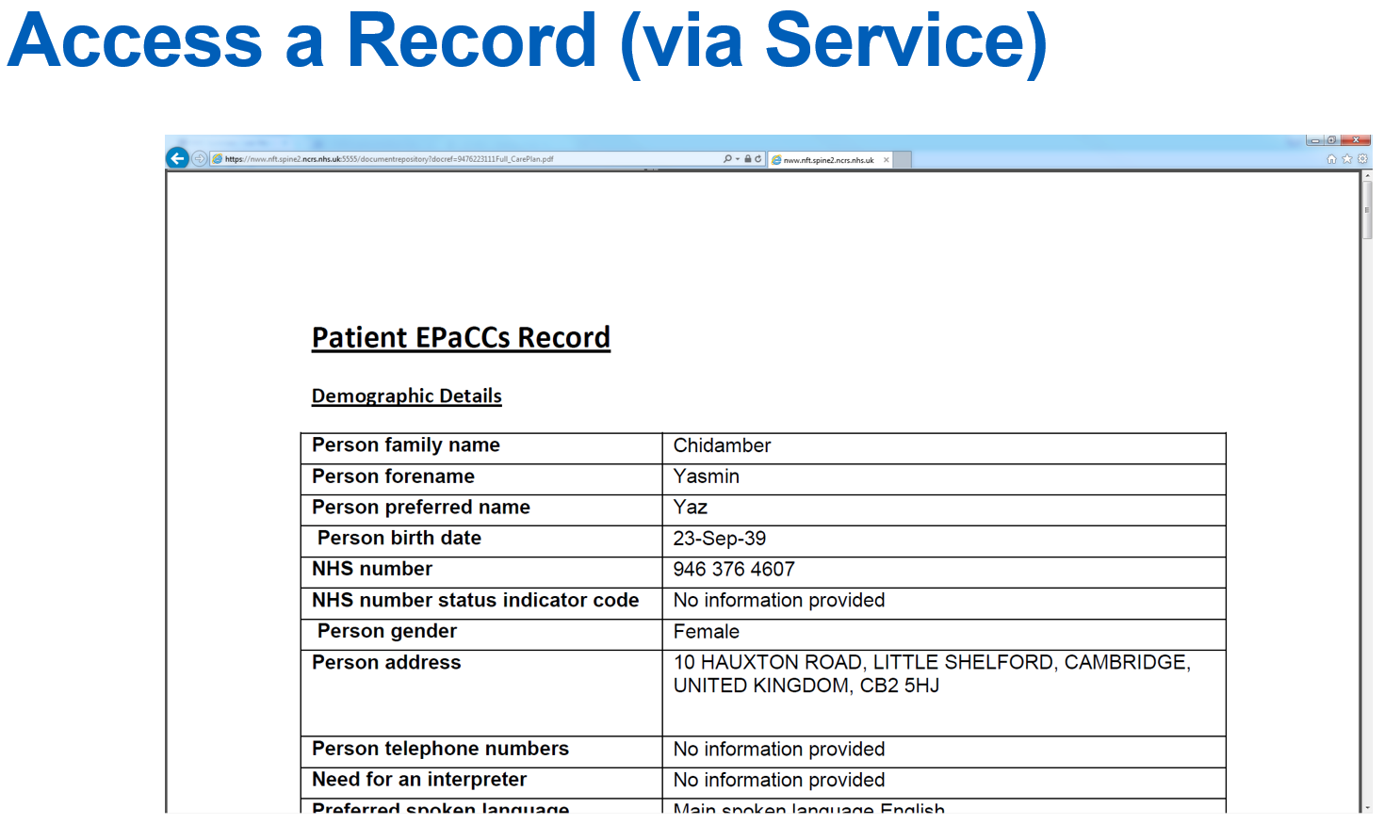


Figure 10. Screen shot – display of NRLS-enabled record



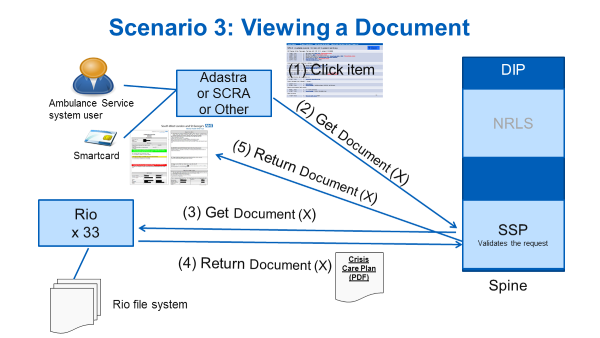


Figure 11. Screen shot – display of NRLS-enabled record