**NRL Data Protection Impact Assessment Annex 1 - Care Plans v2.0**

**Published 15th Oct 2020**

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, in whatever format (e.g. paper, email attachment), are considered to have passed out of control and should be checked for currency and validity.

# Purpose of this document

The NRL facilitates sharing between controllers, providing the means by which health and care organisations can share data. This document is for **information only** and describes the processing of Care Plans through the National Record Locator. The parties are processing data via the NRL are independent controllers and must meet the data protection obligations for the personal data they are processing. Therefore, the controllers must, in accordance with Article 35, carry out a Data Protection Impact Assessment for the sharing of care plans via the NRL, documenting the necessity and proportionality, risks to the rights and freedoms of individuals and the safeguards and security measures in place to protect personal data.

This processing operation is subject to a Data Sharing Arrangement which is entered into by those parties using the system. This document should be read in conjunction with the (“NRL”) Data Sharing Arrangement for Care Plans.

# Consultation with Stakeholders

|  |
| --- |
| Simon Eccles, national CCIO for the NHS, highlighted the sharing of Care Plans as one of his priorities for IT in the NHS. Further to this, the NHS Long Term Plan[[1]](#footnote-2)[1], published in January 2019, also raises similar objectives; “Ensure that clinicians can access and interact with patient records and Care Plans wherever they are”.  The NRL was identified as a means of meeting these objectives and following a period of discovery an implementation phase of work was approved by the NRL Project board on 24th January 2020. This implementation phase will see the sharing of Care Plans, mainly centred around end of life care, with the same Ambulance and 111 service taking part in NRL phase 2. Engagement is continuing at the same time with other potential providers and consumers of Care Plans. This could see the service extend further but at this stage it will remain within the scope of end of life type Care Plans being shared with ambulance and 111 services.  Simon Eccles approached the Integrated Care Programme directly and requested that NRL facilitates the sharing Care Plans, including the ability to view them on the SCRa. The [Long Term Plan](https://www.longtermplan.nhs.uk/wp-content/uploads/2019/08/nhs-long-term-plan-version-1.2.pdf) provides us with a strategic objectives to and Care Plans are mentioned a number of times within the Long Term Plan, listed beneath where relevant to sharing:  Practical priorities will drive NHS digital transformation  • Ensure that clinicians can access and interact with patient records and Care Plans wherever they are.  Chapter Five sets out a wide-ranging and funded programme to upgrade technology and digitally enabled care across the NHS. These investments enable many of the wider service changes set out in this Long Term Plan. Over the next ten years they will result in an NHS where digital access to services is widespread. Where patients and their carers can better manage their health and condition. Where clinicians can access and interact with patient records and Care Plans wherever they are, with ready access to decision support and AI, and without the administrative hassle of today. Where predictive techniques support local Integrated Care Systems to plan and optimise care for their populations. And where secure linked clinical, genomic and other data support new medical breakthroughs and consistent quality of care. Chapter Five identifies costed building blocks and milestones for these developments.  5.15. Patients’ Personal Health Records will hold a Care Plans that incorporates information added by the patient themselves, or their authorised carer. Making Care Plans available to the patient and all clinicians caring for them will help ensure care is not duplicated, tests are not repeated and appropriate actions are taken in a timely manner. The PHRs will also hold data that the patient chooses to share with the NHS, including from monitoring devices such as digital scales or blood pressure cuffs. Patients who choose to join a condition monitoring programme will be able to benefit from insights from these data and will be monitored for combinations of symptoms that may indicate clinical and result in contact from a health adviser or clinician to help the individual stay well. Patients and clinicians will also be able to add information about living circumstances which may require reasonable adjustments to be made events. |

# Purpose of the processing

|  |
| --- |
| The purpose of the processing for Care Plans is set out in the Care Plans Data Sharing Arrangement (“DSA”). The Agreed purposes are set out in Annex 1 and states ‘The Shared Personal Data is processed only for the purposes of direct care and the ‘provision of health and care and treatment, medical diagnosis, provision of social care’.  The National Record Locator (“NRL”) will share personal data described as “Care Plans”, between several parties, these include but are not limited to:   * Mental health Crisis Plans * Anticipatory Care Plans * End of Life Care Plans * Urgent Care Plans (Co-ordinate My Care) * Integrated Care and Support Plan   The pointers are solely to be shared between the Parties for the Agreed Purposes. Those purposes are for direct care and the ‘*provision of health and care and treatment, medical diagnosis, provision of social care*’ |

# Data Flow Map



# Description of the Processing

|  |
| --- |
| The NRL is intended to provide a mechanism for controllers to share information across health and care organisations in a way that has not been done before. The NRL informs ‘consumers’ of the existence and the location of records. The NRL allows controllers to create a ‘pointer’ for a patient record in a number of ways. The controller determines what pointer type to create for which patients.  A pointer shows the existence and location of a record which can then be retrieved via an API and / or using contact details to request information about the record;   * Informs of the existence of a health and care record for a patient * Provides the location of a record, which allows the record to be retrieve via a standardised API * Provides contact details of the organisation which holds the record, which allows information about the record to be requested   The purpose of the NRL is to support health and care uses only. For its initial use, the NRL was restricted to the sharing of mental health crisis plans to Ambulance and 111 services. Subsequent updates to the service will support the sharing of additional types of records.  **Nature and scope of the processing:**  The NRL is to facilitate the sharing of Care Plans. Care Plans are created for the purposes informing those delivering direct care to patients of their health and wellbeing needs.  The NRL will share Care Plans by publishing pointers that indicate that a Care Plans is available and can be accessed if needed.  Organisations that hold Care Plans (the Record Publisher) will create a pointer to a patient’s Care Plans which can then be accessed by an authorised clinician, care worker and/or administrator, in any health or care setting, to support that patient’s direct care (the Permitted Recipient). The Recipients should only access such Care Plans made available by a pointer in accordance with the NRL Data Sharing Arrangement. The DSA states that pointers are created on the understanding that only organisations providing care to a patient will request access to their data.  NHS Digital will facilitate the sharing of Care Plans and will assist the controllers in meeting their data protection obligations. NHS Digital is responsible for:  • Creation and maintenance of the pointer data model i.e. the template that NRL Providers populate to publish a pointer  • Validating the pointer metadata provided by the NRL Provider to ensure that it has been populated using data that is relevant and in the correct format. This validation supports the proper functioning of the index e.g. so that pointers can be effectively searched for. If a pointer fails this validation it will not be published on the NRL index.  • Audit pointer retrieval to assist and support the controllers in meeting their responsibilities  • Support investigations e.g. into system misuse or clinical incidents  • Monitor whether access controls are operating as intended  • Fulfil subject access requests relating to the data it has shared  • Fulfil requests from Data Controllers and Caldicott Guardians detailing who has accessed patients’ health record pointers  • Provide mutual authentication process  **Context of the processing:**  The NRL provides a service that allows care records to be accessed across organisational and regional boundaries to a degree that is not currently achievable. It works by acting as a registry by pointing, or bookmarking, to show a user that a patient record exists and where it is held. The user can then use the information held on the NRL to contact the organisation where the record is held to request more information, or directly request the record if the users system is enabled to allow this.  NHS Digital has no direct relationship with the individual patients whose data is being processed (the data subjects), this direct relationship is with the employees of the NRL Provider and NRL Consumer organisations. |

# Describe the legal basis for the processing (collection, analysis or disclosure) of personal data?

|  |
| --- |
| **NHS Digital’s legal basis for sharing:**  NHS Digital provides the means of **sharing** by establishing and running the services that make up the Digital Interoperability Platform (“DIP”). The DIP is to provide capability to enable health and care organisations to share and access information. The National Record Locator (“NRL”) is one of these capabilities. The Direction states:    *‘Direction is given to NHS Digital (Establishment of Systems: Digital Interoperability Platform Directions 2019*[***[i]***](file:///I:/Strategic%20IG/Integrated%20Care-LHCR/NRL/NRL%20legal%20basis%20and%20Fairness%20of%20processing%20.docx)*), in accordance with Regulation 32(1) of the Regulations, to exercise the following systems delivery functions of the Secretary of State:*    *• to develop and operate such IT applications, IT infrastructure and IT systems as are necessary to deliver the Digital Interoperability Platform in accordance with the functionalities set out in the supporting technical specification(s) or any subsequent amended version of the same document.*  Pursuant to sections 254(1) and 254(6) of the Health and Social Care Act 2012, NHS Digital is further directed, to collect and analyse such information as is necessary to develop and operate the Digital Interoperability Platform. This allows NHS Digital to collect the information necessary to support the functioning and management of the National Record Locator. This includes the data collected and maintained by NHS Digital make up the national index of pointers, for the controllers purposes and data on the usage of the NRL for audit and monitoring purposes to ensure appropriate usage of the system, evidencing the processing and support the controllers in their obligations.  **Health and Social Care Organisation’s legal basis for sharing:**  Controllers must, in order to meet the legal obligations in data protection legislation, identify the legal basis and purpose for the processing of Care Plans via the NRL and document this in their Data Protection Impact Assessment (“DPIA”).  The Data Sharing Arrangement sets out the legal basis for each party that publishes and receives Care Plans on the NRL. It sets out that the record publishing controllers are responsible for ensuring they have obtained consent from the patient for the creation of the Care Plans; where the patient does not have capacity they must ensure that consent has been obtained from those with Lasting Power of Attorney, or a clinician has undertaken a best interest assessment.  The Data Sharing Arrangement sets out that the legal basis for the processing of care Plans is for the delivery of health and care in the exercise of the official authority of the controllers party to the agreement. Consent is given under Article 6(1)(a) for the creation of the Care Plans and the sharing is processed under the conditions set out in Article 6(1)(e) and Article 9(2)(a) & (h), processing for the purposes of health and care.  The Common Law Duty of Confidence is met by the Parties by ensuring that patients are informed, have given consent for the creation of a Care Plans to be created for the purposes of informing health and care organisations of their care needs. Patients have a right to dissent to the creation and processing of a Care Plan, upon such a request an assessment will be made by a clinician as to whether the processing is in the best interests of the patient. |

# Demonstrate the fairness of the processing

|  |
| --- |
| The Data Sharing Arrangement sets out that each controller would be responsible for demonstrating that the processing is fair and processed in a way that people would reasonably expect. Furthermore, the controllers must consider whether the processing may have any unjustified or adverse effects on them and document this in their DPIA’s.  The publisher has a responsibility to ensure that the data subject is made fully aware and consented to the creation of a Care Plans and the terms of the arrangement are described to the data subject. Controllers must respond to any withdrawal of consent and ensure it is acted upon where appropriate. |

# What steps have you taken to ensure individuals are informed about the ways in which their personal data is being used?

|  |
| --- |
| NHS Digital informs data subjects of the processing of Care Plans through publishing information on its website.  The Data Sharing Arrangement sets out that each of the controllers are responsible for ensuring that they meet the obligations under the GDPR for transparency along with the other rights of the data subject. |

# What categories of data are to be collect and processed

| **Data Categories**  [*Information relating to the individual's*] | **Yes** |
| --- | --- |
| **Personal Data** |  |
| Name | x |
| Address | x |
| Postcode | x |
| DOB | x |
| Age | x |
| Sex | x |
| Marital Status | x |
| Gender | x |
| Living Habits |  |
| Professional Training / Awards / Education |  |
| Income / Financial / Tax situation / Financial affairs |  |
| Email Address |  |
| Physical Description |  |
| General Identifier e.g. NHS No | x |
| Home Phone Number |  |
| Online Identifier e.g. IP Address/Event Logs |  |
| Website Cookies |  |
| Mobile Phone / Device No / IMEI No |  |
| Location Data (Travel / GPS / GSM Data) |  |
| Device MAC Address (Wireless Network Interface) |  |
| Banking information e.g. account number, sort code, card information |  |
| Criminal convictions / alleged offences / outcomes / proceedings / sentences |  |
| *Spare – add data item (as necessary)* |  |
| *Spare – add data item (as necessary)* |  |
| **Special Category Data** |  |
| Physical / Mental Health or Condition | x |
| Sexual Life / Orientation |  |
| Religion or Other Beliefs |  |
| Trade Union membership |  |
| Racial / Ethnic Origin |  |
| Biometric Data (Fingerprints / Facial Recognition) |  |
| Genetic Data |  |

# Describe if the personal data is to be shared with other organisations and the arrangements you have in place

|  |
| --- |
| The sharing of Care Plans on the National Record Locator (“NRL”) will be subject to the NRL Data Sharing Arrangement for Care Plans.  The Parties shall only provide Personal Data to each other under the arrangement;   * to the extent necessary to perform their respective obligations; * in compliance with the Data Protection Legislation; and * for the Agreed Purposes as set out in Annex 1 of the NRL Care Plan DSA*.* |

# How long will the personal data be retained?

|  |
| --- |
| Once a record is retrieved by the permitted recipient, they must not retain the pointer or the Care Plan that it refers to beyond the retention period relevant to the care they have provided. Further detail is provided in the NRL Business Requirements.  Pointers can be deleted if and when necessary. When a pointer has been deleted on the NRL the following rules apply:   * The pointer can’t be retrieved via the NRL API e.g. the pointer won’t be returned to an NRL Consumer in response to a search * Process is irreversible i.e. it can’t be undeleted * Pointer can’t be subject to any other processing e.g. update   NHS Digital retains the pointer indefinitely for medical / legal audit purposes only. It would therefore only ever be accessed directly through the database by NHS Digital personnel with appropriate security clearance and IG approvals, assessed on a case by case basis.  NRL and SSP audit data is retained for the life of the patient plus 30 years.  The necessity of keeping this data for this period is subject to review by the programme and this has been documented in the DPIA. |

# Where you are collecting personal data from the individual, describe how you will ensure it is accurate and if necessary, kept up to date

|  |
| --- |
| It is the Record Publisher’s obligations to ensure that the personal data are kept accurate and up to date. The responsibility is set out in the DSA as follows:   * Populating the data contained in the pointer using the template provided by NHS Digital; * Ensuring there is a lawful basis for processing; that the patient has given consent for the creation of the Care Plans; that a description of this arrangement is given to the data subject; * Determining the personal data that can be accessed and manner and form in which a record can be retrieved either by providing an API or contact details to the record; * Ensuring accuracy of the pointer e.g. that it refers to the correct patient and record and contains the correct information; * Validating the patient’s NHS number on the Personal Demographics Service as part of this process; * Ensuring accuracy of the contact details the pointer refers to e.g. that correct phone number is provided; * Maintaining the pointer to reflect any changes to the record the pointer refers to e.g. when a record is updated or reaches the end of its retention period. NHS Digital provide guidance to support this; * Maintaining the pointer to reflect changes to a patient’s PDS data e.g. change of NHS number; * Auditing pointer publication (or any subsequent amendments or deletion) to meet the responsibilities of its controllership; and * Ensuring the data provided on each pointer is limited only to that necessary for the Agreed Purposes.   The Permitted Recipients have a responsibility to ensure that that the Shared Personal Data is kept accurate and up to data and the DSA states that the Recipient is responsible for:   * Notifying the Record Publisher of any inaccuracies in relation to the pointer or Care Plan; |

# How are individuals made aware of their rights and what processes do you have in place to manage such requests?

|  |
| --- |
| The Data Sharing Arrangement sets out that each of the controllers shall be responsible for their own compliance with the transparency obligations in Articles 13 and 14 of the GDPR and informing individuals of their rights in respect of the sharing of Care Plans via the NRL.  Each controller shall give full information to any Data Subject whose Personal Data may be Processed under this arrangement. This also includes giving notice that, on the termination of this Arrangement, personal data relating to them may be retained by or, transferred to one or more of the Permitted Recipients.  **NHS Digital and rights of the Data Subject**  Under the lawful basis for processing that applies to NHS Digital’s role, an individual’s rights include:   * Right to be informed * Right of access * Right to rectification * Right to restrict processing   How these rights are met by NHS Digital is explained in the subsequent sections.  **Right to be informed**  This right must be met by the controllers, the DSA sets out that both the record Publishers and Recipients who must ensure that they produce their own transparency information that meets the requirements of Articles 12,13 & 14.  As processor this right is met by NHS Digital in the following ways:  Information on the National Record Locator (“NRL”) is available on NHS Digital’s public-facing internet pages:   * <https://digital.nhs.uk/services/national-record-locator>   A transparency statement for the NRL is published on the NHS Digital website.  Further information relating to rights of individuals and how these are met by NHS Digital can be found at the links below:   * <https://digital.nhs.uk/about-nhs-digital/our-work/keeping-patient-data-safe/gdpr/gdpr-register> * <https://digital.nhs.uk/about-nhs-digital/our-work/keeping-patient-data-safe/how-we-look-after-your-health-and-care-information>   A catalogue of data controllers connected to the NRL will be made publicly available. This will enable data subjects to identify if the health and social care services they receive care from are connected to the NRL and therefore may have created pointers that refer to their health records. A data subject can then complete a subject access request to find out if any pointers have been created (see right of access section).  **Right of access**  This right must be met by the controllers, the DSA sets out that both the record Publishers and Recipients must ensure that they have a process for responding to subject access requests that meets the requirements of Article 15. Furthermore, the parties should work together to ensure that such a request is fulfilled  This right is met by NHS Digital:  **Subject Access Requests**  Individuals wishing to a request a copy of the information held by NHS Digital can make a subject access request via the organisational request process.  NHS Digital can provide the following information for all pointers relating to the subject:   * The organisation who owns the pointer and what interactions they have performed against it (create, update, supersede or delete) * Organisations who have retrieved the pointer * Organisations who have retrieved the record the pointer refers to * Time and date that these interactions took place     If a subject wishes to know more about these interactions and why they took place they will need to contact the individual organisations involved. NRL Providers and Consumers are required to audit the necessary information and have the processes in place to respond to such a request.  Link to NHS Digital SAR process:   * <https://digital.nhs.uk/about-nhs-digital/corporate-information-and-documents/publication-scheme/how-to-make-a-subject-access-request>   **Right to rectification**  This right is not met by NHS Digital:  NHS Digital is a processor in respect to the pointer. NRL Providers determine the purposes of the pointer and as such are the data controller of the pointer. Therefore, if a patient wants to challenge the accuracy of information held on the NRL they would need to do so with the NRL Provider organisation. As NHS Digital does not have a relationship with the data subject they would not be able to validate any such request.  The data controller of the pointer is required to have a process in place to rectify the data held on the pointer. Technically, the NRL provides the functionality to support this.  NHS Digital can assist data subjects in identifying who the relevant data controllers are via the subject access request process and the NRL controller catalogue as described under the right to be informed and right of access sections above.  **Right to restrict processing**  This right is not met by NHS Digital:  NHS Digital is a data processor in respect to the pointer. NRL Providers act as the data controller of the pointer. Therefore, if a patient wants to restrict access or stop any further processing of the pointer, for example due to concerns over accuracy, they would need to contact the NRL Provider organisation. As NHS Digital does not have a relationship with the data subject they would not be able to fulfill any such request.  The data controller of the pointer is required to have a process in place to restrict processing. Technically, the NRL provides the functionality to support this.  NHS Digital can assist data subjects in identifying who the relevant data controllers are via the subject access request process and the NRL controller catalogue as described under the right to be informed and right of access sections above. |

# What technical and organisational controls for “information security” have been put in place?

|  |
| --- |
| Each controller is subject to their own obligations under data protection legislation and must ensure they provide adequate security and protection for personal data as set out in Article 32 of the GDPR.  ‘*Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons*’  Each controller shall therefore, implement and maintain appropriate technical and organisational measures to ensure a level of security appropriate to that risk.  Controllers sharing Care Plans on the NRL shall also maintain a record of its processing activities in accordance with Article 30 of the GDPR and shall make the record available to the other controllers upon reasonable request.  The following organisational and technical controls are provided by NHS Digital for the protection of personal data processed by the (“NRL”) Service.  **Technical & Organisational controls**  The NRL validates all interactions it receives to ensure they have come from an approved system of those permitted to share and receive the data.  The NRL also checks that the system and organisation are approved for the particular interaction type they are attempting to perform e.g. if they have only been approved as a recipient they will not be able to create and share pointers.  Additional controls are applied to NRL Consumers when they search for pointers for a patient. The pointers that are returned to them are restricted, so that organisations only receive the pointer types that are necessary for them to deliver their services. Each NRL Consumer is identified by their Organisation Data Service (ODS) code and the NRL holds a list of pointer types that they are permitted to retrieve. NRL ensures that when a Consumer requests a pointer for a patient, the NRL will find all the pointers for that patient, but then only return the pointer types that the consuming organisation should have access to.  The National Record Locator (“NRL”) is covered within the Spine Core System Level Security Policy (SLSP) (SLSP0000028). NHS Digital Staff accessing data are aware of their responsibilities and complete mandatory annual information governance training. An internal process is in place to report and manage data breaches.  Health and social care organisations can request access records via the NRL. The Interoperability Working Group will apply governance and assurance controls to ensure that only organisations that have a lawful basis and legitimate need for the data can join the NRL to access the categories of data needed. Organisation / services can only consume pointers which they are authorised to view.  Where an organisation provides several different services, it is possible that not all of those services will be able to view all pointers that an organisation can consume. Where this is the case the access control model of the patient information system provided by the supplier of the consuming organisation must ensure pointers and records are only displayed to authorised users. These are described in further detail in this section.  **Contractual Controls**  To use NRL suppliers have to provide assurance in the SCAL assessment that they meet the requirement (2 factor authentication IAL3) this forms part of the onboarding process. Suppliers that are unable to meet the required security standards will not get through the process and the providers cannot access/publish to the NRL. NRL requires 2 factor authentication using the highest level of authentication IAL 3 as per the standards defined by the Cabinet Office (link below). IAL 3 that requires physical presence of the user ie Smartcard or NHS Identity Agent.  The Data Sharing Arrangement (“DSA”) sets out the data protection responsibilities on the controllers in respect of ensuring there is adequate security appropriate to the risks in accordance with Article 32.  The processor is obliged in the Connection Agreement to ensure that its processing meets the requirements set out in the SCAL and also to ensure that the provider has entered into the terms of the DSA.  The following governance must be achieved by both suppliers and providers:   * **Suppliers** integrating with NRL achieve full assurance by completing the Supplier Conformance Assessment List (SCAL).   + This is a checklist of requirements specified by NHS Digital live services and Integrating Care programme   + These include security requirements such as user authentication and user authorisation   + To achieve assurance, suppliers have to carry out pre-determined tests and provide screen shot evidence support how their system meets the criteria.   + Suppliers must have completed the Data Security and Protection Toolkit within the last 12 months   + Suppliers must have completed a penetration test on their product within the last 12 months   + Once achieved, they receive a Test conformance Certificate (TCC) which gets sent to live services as part of the approval to integrate with NRL.   + NHS Digital controls this integration process and this cannot proceed without manual intervention from NHS Digital staff. * Once suppliers have met the SCAL criteria, they can then allow their customers (NHS providers) to use their product to integrate with NRL * To facilitate the connections between the Providers and NRL, the Providers must sign the Data Sharing Arrangement (DSA). This sets outs the obligations they must meet as a data controller using the service.   **Organisation Access Controls**   * Technically, the process described above is supported by validation of any interactions received by the NRL. The NRL checks that the endpoint where the request came from is on the list of approved endpoints (i.e. those of **Suppliers** that have gone through the above steps) and is from an approved organisation (i.e. those **Providers** who have gone through the above steps). * The NRL also checks that the system and organisation are approved for the particular interaction type they are attempting to perform e.g. if they have only been approved as an NRL Consumer they will not be able to create pointers. * Additional controls are applied to NRL Consumers when they search for pointers for a patient. The pointers that are returned to them are restricted, so that organisations only receive the pointer types that are necessary for them to deliver their services. Each NRL Consumer is identified by their Organisation Data Service (ODS) code and the NRL holds a list of pointer types that they are permitted to retrieve. This means that when an NRL Consumer requests pointers for a patient, the NRL will find all the pointers for that patient, but then only return the pointer types that the consuming organisation should have access to. This is illustrated in the left hand side of figure 4 where different pointers are returned to Consuming System 1 and Consuming System 2.     **Figure 4: NRL access controls**   * The pointer types that an NRL Consumer are permitted to retrieve is determined through the Interoperability Working Group(“IWG”). When an NRL Consumer wishes to connect to the NRL (or increase the scope of their use) they must outline which pointer types they need to retrieve and what the purpose and lawful basis for doing so are. The IWG then consider this against their standard business, clinical safety and IG criteria.   **User Access Controls**  **Authentication**  When an NRL consumer wants to retrieve either pointers or records, user authentication and authorisation also takes place. Authentication is the technical process for a person to prove who they are each time they access an online health or care service. The required authentication standard for the NRL is by use of a Smartcard or other form of NHS Identity. This is in alignment with NHS Digital security requirements that a user reading patient confidential data or clinical data on national systems (i.e. those hosted by NHS Digital) requires level 3 standard of authentication[[2]](#footnote-3).  **Authorisation**  Authorisation is the technical process of granting or denying access to a resource based on the user's identity. Technically, the authorisation model for NRL is implemented in the NRL Consumer system. It is not controlled centrally by NHS Digital. This is consistent with the approach taken for other Spine services.  NRL Consumers are required to implement Role Based Access Control (RBAC) within their system to ensure that users only have access to the types of records that are necessary for them to perform their role. This will be a subset of those the organisation is permitted to receive based on the organisation control described above. This is illustrated in the right hand side of figure 4 where the Administrator and Practitioner using Consuming System 1 have access to different pointers. NRL Consumers will have existing Registration Authority (RA) Managers who manage user access controls.  The NRL has a defined model for RBAC. In this model, access to records is determined by Record Groups, where a Record Group contains one or more Record Types. Access to each Record Group is controlled by Role Based Access Control (RBAC) codes from the [National RBAC Database](https://developer.nhs.uk/apis/spine-core/security_rbac.html) that are administered by RA Managers within Trusts.  For each Record Group there are two RBAC codes:   1. The first RBAC code will allow a user to view pointers only (for all the Record Types in that Record Group) 2. The second RBAC code will allow a user to view pointers and retrieve records (for all the Record Types in that Record Group)   The two RBAC codes support the needs of different roles. For example, many clerical roles may only need to view pointers whereas most clinical roles will need to view pointers and retrieve records. This model of access is illustrated in figure 5 beneath where each box represents a separate RBAC code.    **Figure 5: NRL RBAC model**  A user may have access to one or more Record Groups depending on the information needs of their role n.b. there is currently only one Record Group but this is expected to change as more Record Types are added to the NRL. The [NRL RBAC Mapping Table](https://developer.nhs.uk/apis/nrl/explore_rbac_mapping.html) explains which Record Types are contained within each Record Group and will be updated each time a new Record Type is added to the NRL. As a new Record Type is added to the NRL a process will be followed to determine where it fits in the RBAC model i.e. is it a record that should be available to the majority of health care professionals or does it need more specific controls?  In going through the onboarding process and signing the Data Sharing Arrangement, NRL Consumers agree to a number of responsibilities, including security controls. Organisations are required to ensure that the NRL is only used for specified purposes and where there is a legitimate relationship with the patient. They have access to audit logs to monitor for and investigate any system misuse. Organisations are also expected to remind users of their professional responsibilities when accessing and viewing personal confidential information. |

# Does the National Data Opt Out apply to the processing?

|  |
| --- |
| The National Data Opt Out does not apply to the processing for Care Plans as the processing is for direct care purposes. |

# Further Actions

* The completed DPIA should be submitted to the Office of the SIRO ([officeofthesiro@nhs.net](mailto:officeofthesiro@nhs.net)) for review
* The IAO should keep the DPIA under review and ensure that it is updated if there are any changes (to the nature of the processing and/or system changes)

# Signatories

The DPIA accurately reflects the processing and the residual risks have been approved by the Information Asset Owner:

**Information Asset Owner (IAO) Signature and Date**

**FOR OFFICE OF THE SIRO AND OFFICE OF THE DPO USE ONLY**

# Summary of high residual risks

|  |  |
| --- | --- |
| **Risk no.** | **High residual risk summary** |
|  |  |
|  |  |
|  |  |

**Summary of DPO advice:**

**Data Protection Officer (DPO) Signature and Date**

**ICO consultation outcome:**

**Office of DPO Signature and Date**

**Next Steps:**

* **DPO to inform stakeholders of ICO consultation outcome**
* **IAO along with DPO and SIRO to build action plan to align the processing to ICO’s decision**

1. [1] NHS England, *‘The NHS Long Term Plan’, NHS England,* 2019,  <https://www.longtermplan.nhs.uk/> (accessed 26th March 2020) [↑](#footnote-ref-2)
2. As per the standards defined by Cabinet Office. (2014). *Good Practice Guide No. 44 Authentication and Credentials for use with HMG Online Services* [online] Available at <https://www.gov.uk/government/publications/authentication-credentials-for-online-government-services> [Accessed 14/04/2020] [↑](#footnote-ref-3)