
Document filename: **National Imaging Registry (NIR) - Data Sharing Arrangement (DSA)**

Version issue date:
01/05/2026

Version: 1.0 FINAL

National Imaging Registry (NIR) - Data Sharing Arrangement (DSA)

This DSA is for the Beta Testing of the National Imaging Registry (NIR)

Revision History

Version	Date	Summary of Changes
0.1	10/25	First Draft. Comments provided by Legal Services.
0.2	17/11/25	Review of DPIA by Senior IG Consultant, MLCSU.
0.3	20/11/25	Production of a 'clean copy' for review by customer before moving onto review/approval stages.
0.4	25/11/25	Updated Hazard Log details incorporated into Section 13.
0.5	25/11/25	Finalisation of DSA ready for review and approvals.
0.6	11/03/26	Final IG and legal review
1.0	18/03/26	FINAL version
1.1	01/05/26	Additional comments from legal and AUP

Document Control:

The controlled copy of this document is maintained in the NHS England 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.

Data Sharing Arrangement (DSA)

This Arrangement should be agreed and signed by National Imaging Registry (NIR) Providers and Consumers in relation to the sharing of personal data.

The Providers and Consumers act as independent Data Controllers and include both public and private healthcare organisations.

Personal data processing under this Arrangement is only allowed for direct patient care purposes. It does not allow for data processing for any secondary purposes such as planning and research purposes.

By signing up to this DSA, Providers and Consumers agree:

- For their data to be shared with any onboarded Consumers nationally;
- To maintain a secure outbound network configuration (e.g. no reliance on Web Proxy Auto-Discovery (WPAD), and compliance with this requirement will be checked during the onboarding phase.

1. Background

The National Imaging Registry (NIR) is one of a number of services set up under the NHS England *Establishment of Systems: Digital Interoperability Platform (DIP) Directions 2019*. The purpose of the DIP was to 'develop and operate such IT applications, IT infrastructure and IT systems as are necessary to deliver the digital interoperability platform.'

The Secretary of State considered (in accordance with Section 254(2)(b) of the Health and Social Care Act 2012), that it was "in the interests of the health service in England or of the recipients or providers of adult social care in England" that these Directions be given. Since NHS Digital has merged with NHS England, all services set up under this Direction are now managed by NHS England.

The NIR is a federated proxy service which enables the querying of a patients imaging history and the subsequent retrieval of reports and images based upon the metadata provided in the response to the querying of patients history who live in England. Providers that hold a relevant patient record will create a pointer to that record, which can then be accessed by Consumers for the Agreed Purpose.

The NIR is an evolving service. Annex 1 (NIR Providers and Consumers) lists the types of provider and consumer organisations who currently share information through the NIR, and Annex 2 (Information Available on the NIR) lists the types of imaging and reports currently available. Additional users and types of imaging records may be added to Annexes 1 and 2 in accordance with the Change Control Process.

2. Testing

The NIR platform has been successfully tested in formal alpha testing with a small group of Trusts and will be tested with live patient data in beta testing. During this beta period additional functions and features will be deployed following NHS England's standard approach to User Acceptance testing and deployment.

During and following completion of testing: should there be any significant material changes to the nature, scope, context, or purposes of the data processing that could introduce new or

increased risks to the rights and freedoms of individuals, then this DSA (as well as the Data Protection Impact Assessment (DPIA) and any other relevant documentation) should be reviewed, updated, and be approved via Change Control Processes.

3. Purpose of this Arrangement

This Arrangement sets out the purposes, processes, and lawful bases upon which Personal Data may be processed through the NIR.

The Arrangement establishes the framework for:

- the sharing of metadata and related information to enable the safe discovery and retrieval of diagnostic imaging records;
- the roles and responsibilities of Providers and Consumers as independent Data Controllers. These are both public and private healthcare organisations;
- compliance with UK GDPR, the Data Protection Act 2018, and the Health and Social Care Act 2012; and
- the governance and assurance processes to ensure lawful, proportionate, and secure use of patient data strictly for direct care.

The terms of this Arrangement apply to all Parties documented within the Arrangement and to organisations where another responsible body (such as an imaging network) has accepted the Data Sharing Arrangement on behalf of providers in their region.

The definitions set out at Annex 3 apply to this Arrangement.

4. Parties to this Arrangement

The Parties to this Arrangement are Users of the NIR (listed in Annex 1).

Providers are Controllers of the imaging records which they share through the NIR. Consumers become Controllers for any Shared Personal Data which they receive via the NIR, and which is incorporated into their care record system(s).

NHS England is not party to this Arrangement as a User, however it is understood by the Parties that NHS England has been directed under the Digital Interoperability Platform Directions 2019 to establish and operate the NIR, and it is acknowledged by the Parties that NHS England has certain rights in relation to the NIR, as set out in the NIR Technical Specification and this Arrangement, including (but not limited to) clauses on Audit, Termination, Enforcement, and Variation of this Arrangement.

NHSE maintains audit logs related to system access. Metadata on who has accessed the NIR via the API is shared back with the end user organisations who are required to integrate into their local system and manage as part of local audit monitoring. This data can also be used for managing data subject access requests.

Notwithstanding the above, the Parties acknowledge that NHS England is responsible for the secure operation and functionality of the NIR, including management and maintenance of the registry of pointers, the security of the content of the messages traversed on the NIR service and collection of audit data about message transactions for operational support purposes. The content of the messages is not collected or stored by NHS England.

5. Data Items to be processed

See Annex 2 for more details.

6. Legal bases for personal data processing

The National Imaging Registry will fall under the Digital interoperability Platform Directions 2019 - permits NHSE to develop and operate such IT applications, IT infrastructure and IT systems as are necessary to deliver the digital interoperability platform.

NHS England 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 Imaging Registry (NIR) is one of these capabilities.

The legal basis, for the provision of this service and the processing of data in order to support the operation of the DIP is provided under:

In relation to NHSE:

- UK GDPR Article 6(1)(c) ‘*processing is necessary for compliance with a legal obligation to which the controller is subject*’;
- UK GDPR Article 6(1)(e) – Reasons of substantial Public Interest (with a basis in law) and with Conditions 11 and 18 under Schedule 1 of the Data Protection Act 2018;
- UK GDPR Article 9(2)(h) ‘*processing is necessary for the management of health or social care systems and services*’ - Supplemented by DPA 2018 Part 1 Schedule 1, paragraph 2: health or social care purposes; (f) the management of health care systems or services or social care systems or services.

For National Imaging Registry (NIR) Providers and Consumers the lawful basis is set out in Schedule 1 below.

7. Individual rights

Patients are informed of their rights through both national and local NHS and Private Imaging Organisational channels. While the NIR facilitates data sharing for Direct Care, any rights requests are directed to the originating data controller usually the provider.

Patients retain the right to exercise their individual rights:

- Request access to their data
- Ask how their data has been used and be informed about how their personal data is being processed
- Raise concerns or complaints through their local NHS or Private Imaging Provider’s data protection officer
- Have inaccurate or incomplete personal data corrected
- Ask to have their personal data deleted (only in certain circumstances, and in most cases not applicable to NIR as the data is used for direct care purposes, however any right to erasure request should be assessed on a case-by-case basis)
- Request to restrict processing (in certain circumstances)

- Object to the processing (in certain circumstances)
- The right to data portability would not be applicable in this case
- Request not to be subject to automated decision-making and profiling

These rights are communicated through privacy notices and standard NHS information governance channels.

8. National Data Opt Out

The National Data Opt-Out does not apply because the NIR processes personal data **solely for direct care purposes**, such as enabling clinicians to access imaging for diagnosis and treatment. The opt-out only applies to secondary uses like research and planning, which are not part of this processing.

National Imaging Registry (NIR) Providers and Consumers will be responsible for managing any objections from patients who do not want their information shared via the system.

9. Transparency

To ensure individuals are informed about the ways in which their personal data is used within the National Imaging Registry (NIR) framework, all Providers and Consumers to this Arrangement acknowledges that, and where necessary actions, the following steps:

Local Privacy Notices

Each Provider and Consumer participating in the NIR is responsible for maintaining an up-to-date **privacy notice which references the NIR** on their website and patient communications. These notices explain:

- What types of personal data are collected (e.g. imaging and diagnostic data)
- Why the data is shared (direct care, continuity of treatment) and accessed by health and care staff with a legitimate relationship to the relevant patient for the purposes of direct care.
- Who it may be shared with (other health and care organisations)
- The legal basis for sharing
- These notices explicitly state that imaging and clinical information may be shared with other NHS providers to support direct care delivery.

10. Retention

Data remains under the control of the originating Provider who will retain them in line with their retention schedules.

Personal Data must not be retained by the Consumer except for instances where Shared Personal Data has been used to update the Consumer's patient medical record for the purposes of Direct Care.

No persistent data storage occurs within the NIR platform. Data is only retrieved temporarily for Direct Care and then discarded after viewing. Source systems (e.g. PACS) retain the data according to their local retention policies, which comply with NHS Records Management Code of Practice.

11. How the NIR works and user access

A summary of how the NIR works and the onboarding requirements are set out at Schedule 2 below. Schedule 3 below sets out the Acceptable use policy for users.

12. Obligations of Providers and Consumers in relation to Shared Personal Data

Each Provider and Consumer shall Process Personal Data through the NIR as an independent Controller and shall comply with the applicable Data Protection Legislation. For the avoidance of doubt, Providers and Consumers do not act as a Processor on behalf of any other Provider or Consumer.

Each Provider and Consumer shall Process the Personal Data only as set out in this Arrangement and in accordance with the Agreed Purposes only.

Each Provider and Consumer acknowledges that, and where necessary actions:

- (a) When acting as a Provider they are confirming that organisations acting as Consumers may access the Shared Personal Data upon request, subject to the terms of this Arrangement and as per the Controller Catalogue;
- (b) When acting as a Consumer, health and care professional with a legitimate relationship to a patient to access the record for delivering direct care, and (where relevant) to prioritise available resources most effectively at that time, to the extent such prioritisation is required for the provision of Direct Care to the patient whose Personal Data is being Processed;
- (c) They may be subject to audits from NHS England to ensure that they are meeting their obligations under this Arrangement;
- (d) Their privacy notice(s) and/or other relevant communication materials must explain what Personal Data is Processed through the NIR, when and who it may be shared with and why, and how Data Subjects may object to their information being shared through the NIR;
- (e) They must have appropriate role-based access controls in place to ensure health and care professionals access the Shared Personal Data appropriately;
- (f) It shall be responsible for its own compliance with Articles 12, 13 and 14 (“Transparency”) of the UK GDPR.
- (g) To maintain a secure outbound network configuration
- (h) Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the Processing, as well as the risk of varying likelihood and severity for the rights and freedoms of Data Subjects, each Provider and Consumer shall, with respect to its processing of Personal Data as Controller, implement and maintain appropriate technical and organisational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32 of the UK GDPR.
- (i) It must ensure that health and care professionals who have access to the Shared Personal Data have undergone training in the Data Protection Legislation and confidentiality, in line with each Controller's mandatory training programme;
- (j) It has a current NHS Data Security & Protection (DSPT) submission at ‘Standards Met’, or at ‘Approaching Standards’ with an NHS England validated improvement plan.
- (k) It shall provide reasonable assistance to another Provider or Consumer to this Arrangement or to NHS England regarding any communications from the ICO, or other regulatory or competent authority concerning compliance with Data Protection Legislation;

- (l) It shall maintain a record of its Processing activities in accordance with Data Protection Legislation and shall provide evidence to the other Provider or Consumer upon reasonable request;
- (m) Any actions requested by a Data Subject in relation to information rights (including access to their records), will be dealt with by the receiving organisation in accordance with their processes for handling subject access requests.
- (n) It shall promptly notify the other Provider or Consumer upon it becoming aware of any Personal Data Breach relating to Personal Data (including but not limited to unauthorised data accessed) provided by the other Provider or Consumer for the Agreed Purposes and shall:
 - i. do all such things as reasonably necessary to assist the other Provider and Consumer in mitigating the effects of the Personal Data Breach;
 - ii. implement any measures necessary to restore the security of any compromised Personal Data;
 - iii. work with the other Provider or Consumer to make any required notifications to the Information Commissioner's Office and affected Data Subjects in accordance with the Data Protection Legislation (including the timeframes set out therein); and
 - iv. not do anything which may damage the reputation of the other Provider or Consumer or that Provider or Consumer's relationship with the relevant Data Subjects, save as required by Law.
- (o) It can demonstrate compliance with its obligations under this Arrangement;

12.1. Additional obligations on the part of the Providers

In addition to the obligations listed above, Providers shall:

- (a) Ensure that, where relevant, any IT system suppliers (acting as the Providers data processors) have successfully completed NHS England's live service onboarding process for NIR and accepted the conditions upon which they may connect to the NIR; and there is a legally binding contract with suitable data protection, data security, and information governance clauses in place between the Provider and their Data Processor.
- (b) Ensure that, if the Provider has developed and is operating its own IT system, the Provider has successfully completed NHS England's live service onboarding process for NIR and accepted the conditions upon which they may connect to the NIR;
- (c) Take reasonable steps to ensure that Shared Personal Data is accurate and up to date at the point of sharing;
- (d) Populate the data using the metadata schema provided by NHS England;
- (e) Provide metadata to allow Consumers to retrieve the record;
- (f) Ensure accuracy of the data, i.e., that it refers to the correct patient and that the Patient Record contains the correct information;
- (g) Validate the patient's NHS number on the Personal Demographics Service (PDS) and maintain the data to reflect any changes to a patient's PDS data;
- (h) Maintain the data to reflect any changes to the Patient Record that is referred to;
- (i) Audit data publication (including any subsequent amendments or deletions);
- (j) Ensure the Personal Data made accessible is limited only to the types as agreed by NHS England (as detailed in the Controller Catalogue) and which is necessary for the Agreed Purposes;

12.2. Additional obligations on the part of Consumers

- (a) In addition to the obligations listed above, Consumers shall use information obtained from the NIR only for the Agreed Purpose and not for any other purpose(s);
- (b) Ensure there are local policies and processes in place to ensure access to information is only by health and care professional who have a legitimate relationship with patients in the delivery of direct care.
- (c) Inform the Provider in a timely manner if they become aware that Shared Personal Data is inaccurate or incomplete;
- (d) Ensure that they have a legal basis for processing if they onward share patient identifiable information from the NIR. Any information passed on must be relevant and proportionate to the Agreed Purpose;
- (e) Not retain the Shared Personal Data for longer than is necessary for the Agreed Purpose unless, as part of Direct Care, the Shared Personal Data is added to the Consumer's own care records.

13. Supplier Requirements (included for information and assurance purposes)

- Conduct onboarding and periodic assurance checks on suppliers. The NIR Product Team is responsible for regularly checking compliance, and this is also part of the digital onboarding service process.
- Onboarding to NIR includes technical conformance steps, which will require the supplier to provide assurance and/or evidence of meeting these requirements. The technical and compliance is based on:
 - 1) Security & Compliance Strategy (mTLS, WAF, defense-in-depth, least-privilege IAM).
 - 2) NIR Security and Compliance Strategy
 - 3) Trust Model (certificate hierarchy, SAML/XUA, OAuth/IUA).
 - 4) NIR Trust Model-v24-20250912_16
- Confirmation within onboarding process that suppliers can support the use of NHS number and home community ID within the workflow.
- Suppliers are expected to provide assurance that they can adequately meet the NIR SLA (<https://digital.nhs.uk/developer/api-catalogue/national-imaging-registry-api>)
- To further reduce the likelihood of poor image quality, incomplete imaging, and data corruption, suppliers require data quality checks during onboarding: correct data mapping (IDs), accession numbers, study descriptors), completeness of returned studies, and verification of no corruption across XCA/MHDS flows; defined operational processes for ongoing data quality monitoring and correction.
- Explicit supplier side data quality tests (metadata mapping, completeness checks, regression testing after configuration changes) are the responsibility of the supplier. There is a recommended metadata schema which will be available for suppliers.
- Check that the supplier introduces structured end-user training and workflow validation to ensure clinicians understand when and how to use NIR within pathways (e.g. tumor boards, cross-network referrals), including safe fallback when NIR results are incomplete or unavailable.
- Formal technical onboarding and conformance testing for each supplier is required: protocol support (XCA, MHDS, WADO-RS/WS), trust-model alignment, endpoint configuration, and regression testing when suppliers change versions; define fallback paths where suppliers are not fully XCA and MHDS-ready.
- Suppliers are responsible for providing formal evidence of the digital onboarding requirements (<https://digital.nhs.uk/developer/guides-and-documentation/digital-onboarding>)

- The architecture anticipates mixed maturity, but supplier conformance testing and go-live gates (test scripts, pass/fail criteria) must be run as part of deployment. These need to be codified as explicit onboarding checks owned by the NIR Team.
- Connected suppliers must conform compatibility and test against the approved NIR API version before integration.

14. Confidentiality obligations

a. The Provider or Consumer recognises that information shared under this Arrangement is by its nature subject to a duty of confidentiality and has been provided in circumstances where it is expected that a duty of confidence applies.

b. For the purposes of this Arrangement 'Confidential Information' refers to:

- i. Personal Data including Special Category Personal Data (as defined in the UK GDPR);
- ii. Confidential Patient Information (as defined by the NHS Act 2006);

c. Subject to clause 14d, the Consumer agrees:

- i. not to disclose Confidential Information to any third party or to use it to the detriment of the Provider or the patient;
- ii. to maintain the confidentiality of the Confidential Information; and
- iii. to not access, or attempt to access, Confidential Information except under the Agreed Purposes.

d. The Consumer may disclose Confidential Information:

- i. to comply with the Law;
- ii. to their staff, who will be under a duty of confidentiality;
- iii. to Imaging Healthcare Organisations for the purposes of carrying out their duties; and
- iv. as permitted or required for any NHS Counter-Fraud or Security Management processes.

The Provider and Consumer organisations shall take reasonable steps to ensure:

- The reliability of any employee, agent or contractor who may have access to the confidential information;
- In each case that access is strictly limited to those individuals who need to know/access the relevant confidential information, as strictly necessary for the purposes of this Arrangement, and to comply with Data Protection Laws;
- All such individuals are subject to confidentiality undertakings and/or professional or statutory obligations or confidentiality.

15. Termination of this Arrangement

a. A Provider or Consumer may withdraw from this Arrangement by terminating its access to the NIR.

b. The Provider or Consumer agree that NHS England may issue written notice to terminate a Provider or Consumer's access to the NIR if the Party commits a material breach of the Data Protection Legislation or the terms of this Arrangement. For the avoidance of doubt, NHS England has the right to terminate access with immediate effect.

c. Any data protection or confidentiality obligation imposed on a Provider or Consumer under this Arrangement will survive any termination or expiration of this Arrangement.

16. Role of NHS England and enforcement

a. The Provider and Consumer acknowledge and understand that NHS England has been directed under the Digital Operability Platform Directions 2019 to establish and operate the NIR.

b. Each Provider and Consumer to this Arrangement grants NHS England the right to enforce any of its rights under this Arrangement against any other Provider and Consumer, which may include NHS England revoking a Provider or Consumer's access to the NIR. For the avoidance of doubt, this right is granted in addition to the rights a Provider or Consumer has to enforce its own rights under this Arrangement against another Provider or Consumer, and the grant of such right to NHS England does not affect such Provider and Consumer's rights or ability to pursue any action independently of NHS England (recognising that only NHS England has the technical means to revoke a Provider or Consumer's access to the NIR).

17. Variation of this Arrangement

a. The Providers and Consumers acknowledge that this Arrangement may be updated only by NHS England with additional users and types of imaging records may be added to Annexes 1 and 2 in accordance with the Change Control Process.

b. NIR changes are managed through a formal process aligned with NHS England's API change framework. A multi-disciplinary Change Advisory Board (clinical, information governance, technical, supplier) evaluates the impact on safety, interoperability, and governance. Significant changes require approval by programme governance and NHS England. Minor updates follow a streamlined process but are still logged.

c. Any change to the terms of this Arrangement will be notified to the Providers and Consumers, which may be by email and/or by written notification on NHS England's website. Continued use of the NIR by a Provider or Consumer shall constitute that Provider or Consumer's acceptance of the terms of such revised Data Sharing Arrangement.

18. Notices

All notices and communications given under this Arrangement by the Providers and Consumers must be in writing, sent by post or sent by email.

19. Review of Arrangement

[Specify if, and when, and whom by (specify job role) the Arrangement will be reviewed.]

[Specify, if applicable, how long any review period will be.]

20. Third party rights

Except where expressly stated otherwise in relation to NHS England, this Arrangement does not give rise to any rights under the Contracts (Rights of Third Parties) Act 1999 to enforce any term of this Arrangement.

21. Governing law

This Arrangement and any dispute or claim arising out of or in connection with this Arrangement, or its subject matter or formation shall be governed by and construed in accordance with the law of England and Wales.

Subject to section 9 NHS Act 2006 this Arrangement and any dispute or claim arising out of or in connection with it shall be subject to the exclusive jurisdiction of the courts of England and Wales.

22. Commencement of Arrangement

The agreement will come into force on the date it is signed by all parties

23. End of Arrangement

[Specify how a party ends their participation in this arrangement]

24. End date

[Specify the date the Arrangement ends.]

25. Information Governance Contacts

[List here the Information Governance contacts for each organisation, including their postal address and email address.]

Name	Organisation	Position	Address	Email

26. Signatories

[Each organisation signs here, detailing the name and position of the signatory i.e. DPO/SIRO/CG/Head of Service. A list of onboarded NIR Providers and Consumers will be made available by NHSE on the NIR webpages]

Name	Organisation	Position	Signature	Date

Schedule 1 - Data sharing

Description	Details
Personal Data	see Annex 2 for the current list of information available on the NIR.
Categories of Data Subject	<p>Patients and service users of health and adult social care services.</p> <p>Clinicians and other professionals involved in a patient or service user's care and wellbeing.</p>
UK GDPR/DPA 2018 lawful bases for processing	<p>Personal Data is processed by Providers and Consumers under the following lawful bases:</p> <ul style="list-style-type: none"> • Article 6(1)(e) - Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; • Article 6(1)(g) – Reasons of substantial Public Interest (with a basis in law) and with Conditions 11 and 18 under Schedule 1 of the Data Protection Act 2018 and/or; • Article 9(2)(h) – Health or social care (with a basis in law) - 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. <p>Imaging Healthcare Organisations share and receive Personal Data subject to an appropriate lawful basis having been established and documented in their privacy notice(s).</p> <p>Schedule 1 of the Data Protection Act 2018</p>
Common Law Duty of Confidentiality	The Common Law Duty of Confidence is met because the processing of personal confidential information is for the purpose of Direct Care. Information may be further shared where the disclosure is necessary to safeguard the individual or others, or for another purpose where it is necessary to do so in the public interest.
Duration of the Processing	<p>Processing will continue until a Provider or Consumer withdraws from the Arrangement or the Arrangement is otherwise terminated by NHS England.</p> <p>Personal Data must not be retained except for instances where Shared Personal Data has been used to update the Consumer's patient medical record for the purposes of Direct Care.</p>
Information Asset Owner	<p>Clinical Data Sharing Lead, Platforms/Clinical Pillar</p> <p>Transformation Directorate</p> <p>NHS England</p>

Annex 1: NIR Providers and Consumers

Stakeholder	Role	Responsibilities
NHS England	<p>NIR provider and operator.</p> <p>NHS England has developed and provides the technical platform for NIR (the product). The users consume the capabilities of NIR, such as discovery of the data, retrieving the report/image rather than receiving a service that is delivered by the NHS England for them.</p> <p>The system architects are TSAS Solution Architect.</p>	<p>Maintain the secure registry infrastructure.</p> <p>Ensure compliance with NHS Data Security and Protection standards.</p> <p>Provide onboarding, audit, and monitoring capability.</p> <p>Retain metadata only and avoid persistent storage of clinical data.</p> <p>Provide national guidance and public-facing communications about the NIR and the wider interoperability programme.</p>
NHS England	<p>National Record Locator (NRL) provider and operator.</p> <p>NHS Imaging organisations and Private Imaging organisations register newly generated imaging records via the NIR into the National Record Locator (NRL), so they are discoverable by others</p>	<p>Maintain the secure registry infrastructure.</p>
NHS Imaging organisations and Private Imaging organisations	<p>They are both Data Controllers as well as Data Processors.</p> <p>They are both the Consumers and providers integrated into the NIR.</p>	<p>Where they are Data Processors, they process on the instruction of the Data Controller that contracted them.</p> <p>Where they are Data Controllers they determine the means of the processing.</p> <p>Where they are the consumer, they determine the means of consumption.</p> <p>Where they are the provider of the data, they own the data and they determine whether it is accessible to NIR.</p>

Connected Care Records

Most regions now make their Connected Care Record available via the NIR. The types of organisations and information vary regionally.

All Connected Care Records require approval from NHS England.

Annex 2: Information available on the NIR

NHS England provides the technical platform for NIR. The users consume the capabilities of NIR, such as discovery of the data, retrieving the report/image rather than receiving a service that is delivered by the NHS England for them.

Data item	Justification
Name	To identify patient
Date of birth	To confirm patient identification and support clinical context
Age	To guide clinical decisions
Sex	For clinical relevance in imaging interpretation
Physical description	To guide clinical decisions
General identifier e.g. NHS number	Core identifier for patient matching across NHS systems
Online identifier e.g. IP Address/Event Logs	Event logs are retained for audit and security monitoring. IP addresses may be logged but are not used for patient care.

Information permitted to be shared on the NIR (where available for the patient) includes:

- Diagnostic imaging studies (X-ray, CT, MRI, Ultrasound, PET, etc.)
- Associated diagnostic imaging reports
- Multidisciplinary Team (MDT) outcome reports (where linked to imaging)
- Imaging-related care plans (e.g., radiotherapy treatment plans, imaging follow-up protocols)

The information provided to the NIR is limited to:

- Patient NHS number
- ODS code for the Provider
- Name of the care setting
- Type of imaging or report held
- Technical reference allowing retrieval via supplier system integration

The NIR does not store clinical images or full reports. The NIR does not store metadata either. Actual imaging and documents are retained by and retrieved from the source organisations.

Access model:

- Consumers have view-only access. Once a Consumer closes the retrieved image or report, the Shared Personal Data is no longer accessible and must be requested again through the same NIR process.

Annex 3: Definitions

Agreed Purpose means the sharing of Personal Data by a Provider to a Consumer for the purposes of enabling the Consumer to view appropriate imaging records where it is deemed by the Consumer to be necessary for the provision of Direct Care and within the scope of the NIR Technical Specification.

Arrangement means this document and all its Annexes and Schedules.

Change Control Process means the process set out in the NIR Technical Specification and which includes:

- i. consultation with the relevant health and social care professionals to ensure access to the proposed imaging record is necessary for the Agreed Purpose; and
- ii. agreement and approval by the Interoperability Working Group (“IWG”) or any group, board, or committee (within NHS England) with equivalent responsibility, that the imaging record falls within scope of the Digital Interoperability Platform Directions 2019 and the NIR Technical Specification.

Consumer means an organisation delivering health or [adult social] care of one of the types set out at Annex 1, who accesses Shared Personal Data through the NIR, and which has been approved and assured for access by NHS England as having demonstrated that such access is lawful and necessary for the Agreed Purpose.

Controller, Processor, Data Subject, Personal Data, Personal Data Breach, Processing, Special Categories of Personal Data shall have the meanings as set out in Data Protection Legislation, and their cognate terms shall be construed accordingly.

Controller Catalogue means the database which identifies which organisations are approved as Providers, the types of imaging records to which the Provider’s pointers relate, and which consuming organisations are approved to view information contained within the pointers.

Direct Care means “A clinical, social, or public health activity concerned with the prevention, investigation and treatment of illness and the alleviation of suffering of individuals. It includes supporting individuals’ ability to function and improve their participation in life and society. It includes the assurance of safe and high-quality care and treatment through local audit, the management of untoward or adverse incidents, patient 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.”

Data Protection Legislation means (i) the UK GDPR, (ii) the Data Protection Act 2018, (iii) the Law Enforcement Directive (LED) and (iv) any other laws and regulations which may apply to the Processing of Personal Data as amended from time to time, (v) all applicable Law concerning privacy, confidentiality or the processing of personal data including but not limited to the Human Rights Act 1998, the Health and Social Care (Safety and Quality) Act 2015, the common law duty of confidentiality, and the Privacy and Electronic Communications (EC Directive) Regulations.

Imaging Record means the types of records as set out in Annex 2 (as may be updated in accordance with the Change Control Process).

Law means any law, subordinate legislation within the meaning of Section 21(1) of the Interpretation Act 1978, byelaw, enforceable right within the meaning of, regulation, order, regulatory policy, mandatory guidance or code of practice, judgment of a relevant court of law, or directives or requirements in force in England and Wales with which the Parties are bound to comply.

NIR Technical Specification means the current NIR Technical Specification.

Provider means an organisation delivering health or [adult social] care of one of the types set out in Annex 1, who publishes a pointer on the NIR and which has been approved by NHS England as having Personal Data relevant to the Agreed Purpose and that the sharing of such data is lawful and necessary for the Agreed Purpose.

Pointer means the metadata published by a Provider on the NIR that identifies the existence and location of an imaging record within a specified type.

Shared Personal Data means the imaging record which has been made accessible by the Provider in line with the Agreed Purpose.

Supplier is a Data Processor under contract by individual Data Controllers (the Imaging Healthcare Organisations).

Supplier Systems are Imaging Systems that are provided by Suppliers who are contracted by individual Data Controllers (Imaging Healthcare Organisations).

Type means the type of imaging record or document available to a Consumer via the NIR pointer (for example, CT scan, MRI scan, diagnostic report).

UK GDPR means Regulation (EU) 2016/679 (General Data Protection Regulation) as transposed into the national law of the United Kingdom by operation of section 3 of the European Union (Withdrawal) Act 2018, as modified by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (SI 2019/419), and as may be further modified from time to time.

User means either a Provider or a Consumer depending on the capacity in which they are acting. A User can be both a Provider and a Consumer if they both publish pointers and access Shared Personal Data through pointers published by other Users.

Schedule 2

A summary of how the NIR works and the onboarding requirements are set out at here in Schedule 2

1. The NIR enables clinicians to discover and retrieve diagnostic images and reports created in other organisations through their existing supplier systems.

a. Providers make data available to the NIR via their local imaging or clinical system (e.g., PACS, RIS, or EPR). The data confirms that an image or report is available and its type(s).

b. Supplier systems present the NIR metadata within the user's normal workflow. Clinicians access the NIR through their existing PACS, RIS, or EPR without needing to log into a separate system. A link within the supplier system connects to the NIR, enabling discovery of available external imaging and reports.

c. When a Consumer requests access, the supplier system connects with the NIR to identify the relevant information. The imaging or report is then retrieved from the Provider's system and delivered into the Consumer's local PACS, RIS, or EPR.

d. Consumers therefore discover and retrieve external imaging and reports through the NIR entirely within their existing supplier systems, ensuring seamless integration into local workflows.

NHSE maintains audit logs related to system access and is the controller for audit log data

2. NHSE will manage the assurance for onboarding to NIR

During the digital onboarding service (DOS) process the following requirements will be checked / implemented by the NHSE DOS Onboarding Teams and the organisations that are to be onboarded:

NHSE will as part of compliance and assurance:

DSA

- Confirm that this DSA is signed before enabling live system access. The DSA defines the role and responsibilities of the Data Controller and explicitly states the requirement to maintain secure outbound network configuration (e.g., no reliance on WPAD (Web Proxy Auto-Discovery)).
- Maintain a bank of signed DSAs.

DSPT

- Checking for DSPT compliance (an organisation can not be onboarded if they do not comply, and organisations will be suspended should they no longer be compliant following onboarding);

Local governance processes

- Confirmation that there are local access governance processes to organisations that are to be onboarded, including the joiner-mover-leaver (JML) processes and access reviews, audit samples to confirm timely deactivation of leaver accounts, and Multi-Factor Authentication (MFA) compliance
- Platform-level availability and monitoring are covered by NIR, but **consumer-side resilience** (local runbooks, NIR vs local PACS failover rules, on-call arrangements,

alert routing into local ITSM tools) depend on deployment work. These should be written into onboarding plans and proven in dress rehearsal testing.

- Organisations must confirm during onboarding that suppliers' systems correctly register/report all relevant studies. Supplier-side configuration checks are verified at onboarding.
- Ensure observability and alerts are wired into local operations before switching to live traffic.
- Platform defines **how** failures are reported, but organisations still need:
 - 1) local client behaviour definitions (retries, user messages),
 - 2) service-desk and clinical escalation SOPs, and
 - 3) acceptance tests proving behaviour under failure. These are deployment-specific safety controls and should be added to onboarding plans.
- Ensure that audit logging, reporting dashboards, and governance routines (monthly service reviews, error trend review, network-level KPIs) are implemented; confirm that consuming organisations know how to access and act on audit data.

3. NHSE as part of DOS will check for published information

- Ensure privacy notices at all provider and consumer organisations include NIR participation; align with NHS England's national privacy notice; provide example text and communications materials to local IG teams.

Schedule 3- Acceptable Use

This Acceptable Use Policy (AUP) applies to all users accessing the NIR.

Who is this Acceptable Use Policy for?

Users should ensure this AUP is made available to staff and that staff understand their responsibilities when accessing the NIR.

Your obligations as a User?

- Access to the NIR is limited to health and care professionals with a legitimate relationship to the patient
- Access is strictly for Direct Care purposes
- Information accessed and used should be limited and necessary for the care being provided
- Access to the NIR should be via appropriate role-based access controls as agreed by your organisation
- Staff are required to have been trained and keep up to date with data protection, confidentiality, and appropriate system use
- Staff are required in accessing NIR to comply with local IG and confidentiality policies

Users must not:

- Access records without a legitimate care relationship
- Access records for personal interest or curiosity
- Use the NIR for non-direct care purposes (including research or planning unless separately authorised)

Users must promptly report and manage any incidents involving Personal Data accessed via their local incident reporting process and cooperate with other organisations where required.