**Personal Demographics Service (PDS) Access Request Brief**

This brief covers:

* Use of NHS Numbers.
* Legal basis for organisations accessing the PDS.
* PDS access methods.
* The authorities required for PDS access.
* Secure network connection requirements.
* Cloud storage considerations
* Access request process.
* Legal agreements
* Initial information needed by NHS Digital to consider a request.

**Use of NHS Numbers**

Longstanding Department of Health (DH) policy directs health and care organisations to use the NHS Number to identify, communicate with, and link records of patients. The most recent and explicit example is the Health and Social Care (Safety and Quality) Act 2015, which, *inter alia*, mandates the use of a single consistent identifier across health and social care settings; the single identifier is defined in subsequent regulations as the NHS Number. Additionally, the continued and increasing focus on integrated care, emerging generally and within the specific commitments of the National Information Board (NIB), are dependent on the availability and use of shared identifiers.

Whilst the use of the NHS Number across health and social care settings is therefore well-established in principle and in practice, NHS Digital has specific responsibilities to ensure that access to, and disclosure of, the data that it holds on individuals is consistent with its specific legal and other responsibilities, as well as complying with general requirements relating to data protection and the processing of personal data.

**Legal Basis for PDS Access**

Being a public body NHS Digital is governed by legislation. It can release data to other organisations - either public or private - only on the basis of the Health and Social Care Act 2012, and some other relevant legislation. This legal basis is determined by the purpose for which the data is required. If the purpose is operational, direct care**[[1]](#footnote-1)** - ie, the delivery of care to patients by care providers - then there is a clear legal basis.

For any purpose other than direct care, then the legal basis must be established by reference to the Health and Social Care Act 2012.

For public bodies requesting data, the purposes and the legal bases must clearly relate to the statutory functions of those bodies, and be stated in the access request.

NHS Digital also releases bulk data, generally pseudonimised, for research and analytics purposes, on the basis of the 2012 Act. However, such releases are managed by the [NHS Digital Data Access Request Service](https://digital.nhs.uk/services/data-access-request-service-dars/data-access-request-service-dars-process/data-access-request-service-dars-guidance-notes-on-security) (DARS) process, and not by the process described in this document.

Note that in the case of PDS access for the Child Protection-Information Sharing (CP-IS) purpose, the driver for sharing information is child protection and direct care; as such a data sharing agreement is not required. However, these are strictly only for the cohort of patients who are the subject of child protection measures, and not for any other cohort of patients. CP-IS is not covered in this document, and any existing or planned CP-IS deployments are not affected by this process.

**PDS Access Methods**

The PDS is the national electronic database of NHS patient demographic data, such as name, address, date of birth and NHS number. Therefore it supports quick and accurate identification of a patient, contact and communication with a patient, and linkage of data and records across care settings and information systems.

The primary purpose of the PDS is the direct care purpose, although data is also supplied for secondary uses through the DARS process.

The embedded presentation below gives an overview of the PDS and its interactions.



In summary the access methods for direct care only are:

* Full Spine Integration: This requires a secure network connection and [smartcards](https://digital.nhs.uk/Registration-Authorities-and-Smartcards), because such systems have advanced search capabilities and can update the PDS.
* Partial Spine Integration: This also requires a secure network connection, but smartcards are not required, because the interactions with the PDS are as for the SMSP interactions (see below).
* Spine Mini Service Provider (SMSP): This is a middleware application that presents a simpler interface to local systems than that provided by Spine integration, but with more limited access. It requires a secure network connection, but smartcards are not required, because only exact matches to trace requests are returned, and updates to the PDS are not possible.
* Summary Care Record Application (SCRa): This requires a secure network connection, and provides online, real time access and PDS update capabilities through a web portal, so smartcards are required.
* Demographics Batch Service (DBS): This requires a secure network connection. It is an offline service, and provides batch responses to batch trace requests, so smartcards are not required (24 hour response SLA).
* DBS Bureau (DBSB): This is operated by the PDS National Back Office (NBO), and has the same trace/response functionality as the online DBS option (one week response SLA). There is no direct connection to the PDS, and data transfer is by secure email (eg, NHSmail).

The reason that these access methods are for direct care purposes only is because they do not take account of Type 2 Opt-Outs, where patients have stated that they do not want their information to be used for secondary purposes. Such opt-outs are implemented through the DARS process.

In all cases, there is a standard data set for trace requests to the PDS, and a standard response data set. These data sets are not configurable. However, it is possible to specify selective data items when tracing patients, depending on the access method. Tracing guidance is available, dependent on the access method.

Detailed information about each access method is available separately.

**PDS Access Requests in the context of other authorisations**

There may be some confusion about the different types of NHS Digital authority and agreements. The PDS Access Request process is about the authority for a Non-NHS organisation to access the PDS. It is the organisation that is granted the authority at the end of the process. There are associated legal agreements, as explained later in this document.

Other types of authority are:

* Network Connection - HSCN:
* There will be a legal agreement between NHS Digital and the organisation for access to HSCN.
* There will also be an Information Governance Statement of Compliance (IGSoC) in respect of this connection.
* Data Security and Protection Toolkit (DSPT) Compliance:
  + This type of authority has superseded the previous Information Governance Toolkit (IGT).
  + DSPT is an online self-assessment tool that enables health and social care organisations to measure and publish their performance against the National Data Guardian's ten data security standards, introduced in the [National Data Guardian review of data security, consent and opt-outs](https://www.gov.uk/government/publications/review-of-data-security-consent-and-opt-outs).
  + Whilst this new version of the toolkit is the replacement assurance against data security and correct handling of information, previous versions of the IG Toolkit may still apply until initial reports using the DSPT are completed.
  + The details provided with any submission should be of the latest version of the DSPT, if completed.
  + For more information visit - <https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/data-security-and-protection-toolkit>.
  + Organisations are required to publish an assessment using the new toolkit by 31 Mar 2019. Acute, mental health and ambulance trusts together with community service providers are required to provide a baseline assessment by October 2018.
* End Point Registration and Security Certificates:
* These are needed for all of the PDS access methods except the DBS Bureau service. This is about the technical aspects of accessing the PDS.
* Smartcards:
* Some access methods require the use of smartcards - eg, Spine Integrated systems and the Summary Care Record Application (SCRa).
* This is about the authority for users in an organisation to access the Spine - PDS or Summary Care Record, depending on their role. Smartcard roles are assigned through the Registration Authority (RA) process.

**Secure Network Connections**

Some organisations may already have a secure connection in place.  For those that do not and require new connectivity, the market place for the Health and Social Care Network ([HSCN](https://digital.nhs.uk/health-social-care-network)) is available.

If information is needed about implementing a secure connection to the PDS, please add this to the email at Appendix A, or send a separate enquiry to [enquries@nhsdigital.nhs.uk](mailto:enquries@nhsdigital.nhs.uk), with “*PDS Access - Secure Network Connection Information Request*” in the subject line.

Alternatively, for local authorities, there may be local options to connect via the Public Services Network (PSN), or via a local healthcare partner organisation with a HSCN connection.

**Cloud Storage**

[Guidance](https://digital.nhs.uk/services/data-access-request-service-dars/data-access-request-service-dars-process/data-access-request-service-dars-guidance-notes-on-security#cloud-hosting) was produced by NHS Digital in January 2018 which enables health and care organisations to use cloud services and/or store patient data offshore. An [overview of the requirements](https://digital.nhs.uk/binaries/content/assets/legacy/pdf/3/q/guidance_on_nhs_and_social_care_use_of_public_cloud_services1.pdf) provides more detailed information.

Organisations that include the use of cloud services and/or store patient data offshore in their applications will need to provide evidence that they have undertaken the steps described in the guidance for their application to progress.

Where cloud storage applies, details listed in the sections “Specific DARS requirements” and “Evidence to support a DARS application” found in the guidance should be provided with the applications for PDS Access. As long as these prerequisites are met, then cloud storage can be approved.

**PDS Access Request Process**

The approach rests on establishing consistent criteria against which any given application and purpose (use case) can be assessed. Both the criteria and the procedures draw on the experience and lessons learned from prior submissions, with the following being key:

* Applications need to be clear and explicit about what business processes the requested access will support, and why PDS access is required;
* The legal basis for NHS Digital releasing the data must be stated, if known at the initial request stage. For public bodies the relevant statutory duties should be stated.
* The assessment of applications includes assessment of the risk associated with the proposed access and use, to consider whether it is within the tolerance range for NHS Digital, rather than seeking to reduce risk to near-zero;
* Any novel type of application or use case may require referral to the NHS Digital Information Governance (IG) Team, in the first instance.

As stated above, this process is concerned only with requests for tracing access to the PDS, that is for direct care purposes in organisations that already have a service relationship with an individual, and hold identifying information about them that they wish to validate and, if necessary, update.

The process for handling requests for access to PDS data for operational direct care purposes is based on a principle of categorising the request through a set of pre-defined criteria, whereby the request is assessed and granted. The criteria used include:

* Organisation type - eg, NHS or type of non-NHS organisation.
* Type of service provided - eg, direct care or not.
* Processing objectives and purpose (use case). For non-standard cases it will be helpful to have a context diagram as a supporting document, also indicating the underlying technical architecture.
* Where patients are interacting directly with a system that connects to the PDS, then there must be clear and robust identity validation processes in place.
* Legal basis for the organisation accessing PDS data, based on the purpose.
* Governance/IG arrangements, such as:
* Data Sharing Framework Contract (DSFC), which may already be in place, and any existing Data Sharing Agreements (DSAs), between the requesting organisation and NHS Digital, noting that each purpose will have a separate DSA.
* DSPT compliance.
* DPA Registration - to ensure that the requested data items are covered in the registration, including the use of the NHS Number.
* Privacy Notice (PN) - especially to ensure compliance with the [Information Commissioner’s Office (ICO) guidance](https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control/). Additional criteria have been mandated, indicating the PN standards that must be covered in the PN to allow PDS access authority to be given - see Appendix B. An organisation’s PN will be reviewed for compliance with the Appendix B criteria. A model PN is available.
* Types of end users of data, and the associated local security and RBAC policies.

Requests are processed using the DARS Online system. This requires requesting organisation contacts and legal agreement signatories to log on with credentials provided by NHS Digital.

This may result in the need to refer a request to the [Independent Group Advising on the Release of Data](http://content.digital.nhs.uk/IGARD) (IGARD) for advice and (if required) a recommendation to disseminate**[[2]](#footnote-2)**.

**Legal Agreements**

The legal relationship is between NHS Digital and an organisation requesting the PDS data. It is not with a service and/or system supplier facilitating access to the PDS. Where there is a service and/or system supplier, then information is required about the supplier involved, and the nature of the service and/or system provided. Where a system/service provider is operating as an aggregator**[[3]](#footnote-3)**, then separate agreements may be required for each organisation served. The system/service provider may facilitate this on behalf of its client organisations.

The requesting organisation’s signatory for both DSFCs and DSAs will normally the organisation’s Senior Information Risk Owner (SIRO), or a person with equivalent responsibilities.

**Information needed for an initial request**

An organisation requesting access to the PDS for the first time, or a system/service provider aggregator on behalf of an end user organisation, should send an email to the NHS Digital Contact Centre - [enquries@nhsdigital.nhs.uk](mailto:enquries@nhsdigital.nhs.uk). The email content should be of the form given in Appendix A.

This enquiry will be logged by the Contact Centre and allocated a unique (NIC) reference, which should be used in the subject line of all subsequent email exchanges.

If there is already a NIC reference for the subject case, then this email need not be sent.

**Appendix A - Initial PDS Access Request Email**

**To:** enquiries@nhsdigital.nhs.uk

**Subject:** PDS Access Request - FULL ORGANISATION NAME

*DELETE THE ELEMENTS THAT ARE NOT APPLICABLE*

< *ORGANISATION NAME* > requests access to the PDS for the purpose of < *brief summary of the purpose* >, using the < *access method* > access method.

< *provide a context diagram, if this is a non-standard or novel case* >

Please send further information about the < *access method* > access method.

This organisation currently has access to the PDS for the purpose of < *brief summary of the purpose*>, using the < *access method* > access method.

The existing Data Sharing Framework Contract reference is < *reference* > and the expiry date is < *date* >.

The service and/or system supplier involved in the requested access is < *SUPPLIER NAME*>.

The organisation contact details are:

* Organisation.
* Contact Name.
* Email.
* Telephone.

The contact details for the aggregator acting on behalf of the client organisation are:

* Aggregator.
* Contact Name.
* Email.
* Telephone.

Previous email exchanges about this case are attached as .msg files

**Appendix B - IGARD Privacy Notice (PN) Guidance**

This guidance supplements the [ICO guidance](https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control/).

The criteria against which PNs are reviewed have been endorsed by IGARD. The check list that the criteria are measured against has three standards: good practice, advice and mandatory. The criteria are categorised as either red or amber; red criteria are those that must be addressed satisfactorily. However, if a red criterion is in the notice, but needs improvement, then it is marked as advice - ie, IGARD might accept the fact that the PN will be updated, within a reasonable time frame, usually one month.

The criteria and guidance are embedded here …



1. The Caldicott Review in 2013 defined direct care as:

   A clinical, social or public health activity concerned with the prevention, investigation and treatment of illnesses and the alleviation of suffering of individuals. It includes supporting individuals’ ability to function and improve the 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, person satisfaction including measurement of outcomes undertaken by one or more registered and regulated health and social care professionals and their team with whom the individual has a legitimate relationship for their care. [↑](#footnote-ref-1)
2. The word “disseminate” is used in the Health and Social Care Act 2012, to mean the release of data for whatever purpose. [↑](#footnote-ref-2)
3. In this context a service aggregator is a third party provider that provides an information management service to multiple organisations, using its own application software or that of a third party application provider. [↑](#footnote-ref-3)