National Data Sharing Arrangement (NDSA) Direct Care APIs (GP Connect products)

Contents

- Background
- Definitions
- Obligations of the Parties in relation to Shared Personal Data
- Confidentiality Obligations
- Accession to this NDSA
- Termination of this NDSA
- Role of NHS England and Enforcement
- Variation of this NDSA
- Governing law
- Consideration
- Annex 1: Sharing of personal data
- Annex 2: NHS England Connection Agreement and End User Organisation Acceptable Use Policy (AUP)
- Annex 3: Joint Controller Arrangements

1. BACKGROUND

Go back to contents

A. Direct Care Application Programming Interfaces (API) (Direct Care APIs) is a service set up by NHS England that allows GP practices to share clinical information quickly, efficiently, and safely. APIs make patient data held on accredited practice clinical systems available securely to health and social care organisations to use for direct patient care. This service is known as 'GP Connect' to the wider NHS.

The Definition of 'direct care' used by NHS England is set out in The Information Governance Review as follows:

"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, person satisfaction including measurement of outcomes undertaken by one or more registered and

regulated health or social care professionals and their team with whom the individual has a legitimate relationship for their care."

The Information Governance Review further defines what should be considered as 'indirect care' or 'purposes beyond individual care', as follows:

"Activities that contribute to the overall provision of services to a population as a whole or a group of patients with a particular condition, but which fall outside the scope of direct care. It covers health services management, preventative medicine, and medical research. Examples of activities would be risk prediction and stratification, service evaluation, needs assessment, financial audit."

The use of GP Connect for indirect care or purposes beyond individual care purposes is prohibited.

B. Parties to this NDSA (apart from NHS England) are described as Providers and Consumers, depending on the capacity in which they are acting. A Party (other than NHS England) may act as both a Consumer and a Provider pursuant to this NDSA.

C. This NDSA sets out the purpose and the legal basis upon which the Shared Personal Data can be made available and accessed. Personal Data must only be shared and used in accordance with the Agreed Purposes set out in this NDSA.

D. In addition to the obligations contained within this NDSA, the Parties are bound by the conditions of the End User Organisation Acceptable Use Policy (AUP), and in some limited circumstances as set out in Annex 1, may be bound by the NHS England Connection Agreement, contained in Annex 2.

E. NHS England has certain Controller responsibilities and is responsible for the operation of GP Connect and is party to this NDSA for the purposes of managing the transfer of data across the service and to oversee compliance with this NDSA. See Annex 1 for details of the Processing carried out by NHS England.

F. The Parties acknowledge that GP Connect is an evolving service and additional Products may be added to the service and/or care settings may be expanded. In such circumstances, notification of such changes will be provided to the Parties via the Portal and GP Connect web page.

IT IS AGREED as follows:

---

2. DEFINITIONS

Go back to contents

Agreed Purposes: shall have the meaning as set out in Annex 1;

Consumer: means an organisation providing health and social care, which accesses Shared Personal Data made available by Providers for the Agreed Purposes;

Controller, Joint 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;

Data Protection Legislation: means (i) the UK General Data Protection Regulation (UK GDPR), (ii) the Data Protection Act 2018, and (iii) any other laws and regulations which may apply;

Data Sharing Relationship: means the relationship which arises where one Party accesses Shared Personal Data made available by another Party;

Direct Care: has the meaning set out in Recital A;

FOI: means the Freedom of Information Act 2000;

Environmental Information Regulations (EIR): means the Environmental Information Regulations 2004;

Party, Parties: means organisations who have accepted the NDSA (and NHS England);

Portal: means the National Data Sharing Portal for GP Connect, the portal through which organisations which use GP Connect may be onboarded;

Products: means the various GP Connect products that may be made available to the Parties, as listed at https://digital.nhs.uk/services/gp-connect/gp-connect-in-your-organisation/transparency-notice#the-gp-connect-products;

Provider: means a health and social care organisation that makes available Shared Personal Data via GP Connect;

Shared Personal Data: means Personal Data, including confidential patient information, contained within a patient's medical record, which a Provider makes available, and a Consumer accesses;

SPINE: is a collection of national applications, services and directories that support the NHS in the exchange of information across national and local NHS systems;

Technical and Organisational Obligations: means the obligations set out in Annex 1 in respect of the technical and organisational measures to be put in place in relation to the Shared Personal Data.

---

3. OBLIGATIONS OF THE PARTIES IN RELATION TO SHARED PERSONAL DATA

Go back to contents

a. Subject to clause 3(n), each Party agrees that it shall process the Shared Personal Data as an independent Controller and each shall comply with the applicable Data Protection Legislation. For the avoidance of doubt, no Party acts as a Data Processor on behalf of any other Party.

b. Each Party acknowledges that:
   i. access to Shared Personal Data shall be facilitated by NHS England;
   ii. when acting as a Consumer, they are required to indicate via the Portal which Products they wish to use; and
   iii. when acting as a Provider they are confirming that any Party acting as Consumer may access the Shared Personal Data made available, subject to the terms of this NDSA.

c. Each Party shall ensure that it is able to demonstrate compliance with its obligations under this NDSA and shall Process the Shared Personal Data in accordance with the terms of this NDSA and for the Agreed Purpose only. The Parties shall not process the Personal Data in a way that is incompatible with this NDSA.

d. Each Party shall ensure that it has a relevant legal basis for its Processing of the Shared Personal and be responsible for its own compliance with Articles 12, 13 and 14 ('Transparency') of the UK GDPR. Each Provider and Consumer shall give full information to any Data Subject whose Personal Data may be shared regarding the nature of the Processing (which shall be recorded and accessible via the Portal or such other mechanism as notified to the Parties by NHS England). This includes advising that, on the termination of this NDSA, Shared Personal Data relating to them may be retained by the Consumer or transferred to one or more other organisations if shared for Direct Care purposes.

e. 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 Party 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 as well as the Technical and Organisational Obligations described in Annex 1.

f. Each Party must ensure that all employees who have access to the Shared Personal Data have undergone training in the Data Protection Legislation and confidentiality.

g. Each Provider and Consumer shall meet the applicable standards set out in the Data Security and Protection Toolkit (DSPT). Each Provider and Consumer must have a

current valid DSPT submission of 'Standards met'.

h. Each party shall make their record of Processing Activity (UK GDPR Article 30) available to any other Party with which it has a Data Sharing Relationship, or to NHS England, upon reasonable request.

i. Parties to any Data Sharing Relationship that arises shall provide reasonable assistance to each other regarding any communications from the Information Commissioner's Office, or other competent authority concerning compliance with Data Protection Legislation.

j. Each Party shall appoint an individual within their organisation who will be the point of contact for all matters relating to the NDSA. This individual shall have appropriate knowledge and understanding of Data Protection Legislation and of their organisation's data processing operations in relation to this NDSA.

k. Any requests for disclosure made under FOI, UK GDPR, EIR or similar acts received by a Consumer and which relate to the Shared Personal Data will be communicated to the Provider within a reasonable time period. The obligation to respond to such request rests with the consuming organisation.

l. Any requests by a Data Subject in relation to their information rights under the Data Protection Legislation (including access to medical records) will be communicated to the Provider within a reasonable time period. The obligation to respond to such request rests with the consuming organisation, unless the request is directed to another Party and/or relates to another Party's processing of the Shared Personal Data, in which case, the receiving party will:

    i. promptly, on receipt of the request, inform the other Party that it has received the request and forward such request to the other Party; and

    ii. provide any information and/or assistance as reasonably requested by the other Party to help it respond to the request in the timescales specific in the Data Protection Legislation.

m. In respect of any request received in accordance with clause 3(k) and 3(l), the Provider shall provide any information and/or assistance as reasonably requested by the consuming Party to help it respond to the request, such assistance to be at the cost of the receiving Party.

n. Notwithstanding the above, the Parties acknowledge that in certain limited circumstances, as detailed in the purposes section of Annex 3, a Provider and Consumer may act as Joint Controllers in respect of the Shared Personal Data. In such instances the Parties will comply with the obligations set out at Annex 3.

Additional obligations of Parties acting as Providers

o. Providers shall:

   i. take reasonable steps to ensure that Shared Personal Data is accurate and up-to-date at the point of sharing; and

   ii. have in place appropriate processes to make any changes to the Shared Personal Data as are necessary in connection with the exercise of data subject rights under the Data Protection Legislation.

Additional obligations of Parties acting as Consumers

p. Consumers shall promptly notify the Provider upon becoming aware of any Personal Data Breach relating to Shared Personal Data and shall:

   i. do all such things as reasonably necessary to mitigate the effects of the Personal Data Breach;

   ii. implement any measures necessary to restore the security of any compromised Shared Personal Data;

   iii. 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);

   iv. not do anything which may damage the reputation of the Provider or its relationship with the Data Subject, save as required by Law; and

   v. provide such information and assistance to the relevant Provider as may be required by them.

q. If a Consumer becomes aware that any of the Shared Personal Data is inaccurate or incomplete, they shall inform the Provider in a timely manner.

r. Consumers shall not retain Shared Personal Data for longer than is necessary to in connection with the Agreed Purposes, unless as part of the provision of Direct Care, the Shared Personal Data is added to the Consumer's record.

---

4. CONFIDENTIALITY OBLIGATIONS

Go back to contents

a. The Parties recognise that information to which access is granted under this NDSA 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' may refer to:
    i. Personal Data or Special Category Personal Data (as defined in the UK GDPR);
    ii. Confidential Patient Data (as defined by the NHS Act 2006)

c. Except as described under Agreed Purposes, Confidential Information is owned by the Provider and the Consumer has no other right to use it.

d. Subject to clause 4b, the Consumer agrees:
    i. not to disclose Confidential Information to any third party or to use it to the detriment of the Provider;
    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.

e. The Consumer may disclose the Provider's Confidential Information:
    i. to comply with the Law;
    ii. to any appropriate Regulatory or Supervisory Body;
    iii. to their staff, who will be under a duty of Confidentiality;
    iv. to NHS Bodies for the purposes of carrying out their statutory duties; and
    v. as permitted or required for any NHS Counter-Fraud or Security Management processes.

---

5. ACCESSION TO THIS NDSA

Go back to contents

Each Party agrees to be bound by the terms of this NDSA in the following circumstances:

a. Where upon commencement of this NDSA and this NDSA having been made available to that Party, a Party continues to use GP Connect, such Party shall be subject to the terms of this Arrangement, which shall be deemed as having been accepted by and binding on that Party; and

b. Where a new Party commences, or an existing Party makes changes to its use of GP Connect, that Party must confirm its acceptance of this NDSA via the Portal, prior to accessing any Shared Personal Data.

6. TERMINATION OF THIS NDSA

Go back to contents

a. A party may terminate this NDSA by ending its use of all Products available via GP Connect.

b. NHS England may issue written notice to terminate a Party's access to GP Connect in the event the Party commits a material breach of the Data Protection Legislation or the terms of this NDSA.

c. Notwithstanding clause 6a – 6b above, any obligation imposed on a Party under this NDSA in relation to the Shared Personal Data will survive any termination or expiration of this NDSA.

7. ROLE OF NHS ENGLAND AND ENFORCEMENT

Go back to contents

a. The Parties acknowledge and understand that NHS England has been directed under Section 254 of the Health and Social Care Act 2012 by the Department of Health and Social Care to establish and operate the Direct Care API Service.

b. NHS England is a Controller in respect of Personal Data it Processes in respect of the delivery of GP Connect, as further described in Annex 1.

c. NHS England is therefore a Party to this NDSA for the purposes of managing the transfer of Personal Data via the GP Connect and the operation of this NDSA, including the onboarding of each Party, and ensuring that the Parties comply with the terms of this NDSA.

d. Each Party hereby grants NHS England the right to enforce any of its rights under this NDSA against any other Party, which may include NHS England revoking a Party's access to any or all GP Connect Products. For the avoidance of doubt this right is granted in addition to the rights a Party has to enforce its rights under this NDSA itself against other Party, and the grant of such right to NHS England does not affect such Party’s rights or ability to pursue any action independently of NHS England

(recognising that only NHS England has the technical means to revoke a Party's access to GP Connect).

e. A person who is not Party to this NDSA shall have no rights under the Contracts (Rights of Third Parties) Act 1999 to enforce any term of this NDSA.

f. Any material breach of the Data Protection Legislation or the terms of this NDSA by a Party may result in termination of such Party's involvement in the NDSA and access to GP Connect.

---

8. VARIATION OF THIS NDSA

Go back to contents

a. All Parties acknowledge that its use of GP Connect is subject to the terms of this NDSA. This NDSA may be updated only by NHS England.

b. Any change to the terms of this NDSA, will be notified to the Parties, for example via a notice on the Portal or via other communications channels such as NHS England's 'GP and Practice Manager Bulletins' and continued use of GP Connect by a Party shall constitute that Party's acceptance of the terms of such revised NDSA.

---

9. GOVERNING LAW

Go back to contents

This NDSA and any dispute or claim (including non-contractual disputes or claims) arising out of or in connection with it or its subject matter or formation shall be governed by and construed in accordance with the law of England and Wales.

---

10. CONSIDERATION

Go back to contents

The Parties acknowledge that the mutual promises and covenants contained herein are sufficient and adequate to support this NDSA.

ANNEX 1: SHARING OF PERSONAL DATA

Go back to contents

Description

Details

Identity of Controller for each Category of Personal Data

NHS England

NHS England is responsible for the APIs which enables interoperability between Health and Social Care IT systems. For NHS England to support the service, audit data about the message transactions is collected and used for operational support purposes. NHS England is a Controller for the message audit data collected on Spine. Details of the audit are listed in the transparency material, which can be located at https://digital.nhs.uk/services/gp-connect/gp-connect-in-your-organisation/transparency-notice.

NHS England is also responsible for the security of the content of the messages as they traverse NHS England infrastructure, ensuring that they are passed securely to and from Provider and Consumer IT systems. The content of the messages is not collected or stored by NHS England.

Providers

Providers are Controllers of the patient Personal Data which they share via GP Connect.

Consumers

The Consumers become Controllers of any Shared Personal Data which they receive via GP Connect which is incorporated into their own record systems.

In certain limited circumstances, the Parties may act as joint controllers. Annex 3 details the specific processing the Parties may be acting as joint controllers.

Agreed Technical and Organisational Obligations

All Parties must:

- Agree that they are subject to audits from NHS England to ensure that they meet the obligations of this NDSA and the AUP, which are available on the portal. This may also include adherence to the Connection Agreement in the event an NHS consuming organisation develops its own software.
- Ensure that transparency notices detailing this arrangement are made available to any potentially affected Data Subjects as per the obligations contain in clause 3(d).
- Engage in appropriate communications strategies to promote awareness of this data sharing within their patient cohorts.

Providers must:

- Ensure that patients (or their representatives) are aware of the ability to dissent from this data sharing mechanism, and that information on how to do this is clear and unambiguous.
- Ensure that they are able to provide Data Subjects with an audit trail of access to their records upon request.

Consumers must:

- Determine what Personal Data they require access to from the Shared Personal Data made available by the Provider, and the manner and format in which a record will be viewed.
- Have appropriate role-based controls in place to ensure staff members (or classes of staff members) can access data appropriately.
- Ensure the Personal Data retained is limited only to that necessary for the Agreed Purposes.

Agreed Purposes

The Shared Personal Data shall be Processed by the Parties only:

- for the purposes of Direct Care as specified within this Arrangement, including for the purpose of medical diagnosis, treatment and social care and there is a legitimate relationship between the Patient and the Care Provider i.e., the patient must be receiving Direct Care from a registered health or social care professional, or other health or social care worker who is working under the authority of a registered health or social care professional;
- in the context of the particular Product(s) selected by the Parties; and
- for the purposes of the Direct Care use case as agreed with NHS England during the onboarding process;
- together, the **'Agreed Purposes'**.

Legal basis for processing

The purpose of the Processing of the Shared Personal Data is the delivery of Direct Care in the exercise of the duties of the relevant Controllers, supported by:

Article 6(1)(e) of the UK GDPR ("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");

and

Article 9(2)(h) of the UK GDPR ("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")

The legal basis for NHS England's collection and Processing of Personal Data is Article 6(1)(c) ("processing is necessary to comply with a legal obligation").

For the NHS Number and message content processing which may be considered special category data the legal basis for the processing is Article 9(2) (h) – "processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services" and Data Protection Act 2018, Schedule 1, Part 1, Paragraph 2, Sub paragraph (2) (f) – "the management of health care systems or services or social care systems or services".

Common Law Duty of Confidentiality

Common Law Duty of Confidence is met with 'implied consent' and by ensuring:

- Explicit oral or written recorded consent is not required.
- Data is shared for the purpose of Direct Care, and under these circumstances it is reasonable to use implied consent, and the appropriate conditions to support this are in place:
- The patient is being provided with Direct Care.
- Patients (or their representatives) should always be advised that their Personal Data is being shared via transparency notices.
- The patient (or their representative) has been informed of the data sharing and has not objected.

All potential recipient organisations (Consumers and Providers) of the Shared Personal Data are subject to this NDSA and their own professional codes of confidentiality and are aware that any information received via GP Connect is provided in confidence, which must be respected.

Provided that the above conditions are met, it is reasonable to infer that the patient agrees to the data sharing.

Patients (or their representatives) have a right to object to this data sharing, upon such a request an assessment should be made by a clinician as to whether the processing is in the best interests of the patient or in the wider public interest.

Duration of the Processing

Processing will continue until a Party withdraws from the NDSA or the NDSA is otherwise terminated, in accordance with clause 6.

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

Nature of the Processing

GP Connect provides several Products which facilitate the sharing of Personal Data relating to patients between Providers and Consumers. The nature of the Processing for each Product is [further described at https://digital.nhs.uk/services/gp-connect/gp-connect-in-your-organisation]

Type of Personal Data processed

Personal Data and Special Categories of Personal Data contained within a patient's clinical record, including:

Patient Data

- NHS number;
- Demographic details, including (but not limited to) age, race, ethnicity, gender, marital status;
- Medical Conditions and histories;
- Medication;
- Appointments;

Staff Data

- Names and roles of treating clinicians

Categories of Data Subject

- Patients and service users of health and social care services.
- Clinicians and other professionals involved in a patient or service user's care.

ANNEX 2: NHS ENGLAND CONNECTION AGREEMENT AND END USER ORGANISATION ACCEPTABLE USE POLICY (AUP)

Go back to contents

The NHS England Connection Agreement and End User Organisation Acceptable Use Policy, as may be updated from time to time, can be located here:

View the NHS England Connection Agreement

Download the End User Organisation Acceptable Use Policy

ANNEX 3: JOINT CONTROLLER ARRANGEMENTS (ONLY TO BE USED IN LIMITED CIRCUMSTANCES AS SET OUT IN THE PURPOSE OF THE PROCESSING SECTION IN THIS ANNEX)

Go back to contents

1. The Parties have determined that they are Joint Controllers of personal data covered in certain limited circumstances under this Agreement.

2. This Annex sets out the terms and arrangements applicable to the sharing between them of the data in respect of which they are Joint Controllers. These terms and arrangements only apply to the processing as set out in the purpose of the processing section in this Annex.

3. The legal basis, subject matter, duration, type and categories of Personal Data being shared remains as set out in the table at Annex 1: Sharing of Personal Data.

Joint Controller's Responsibility:

Purpose of the processing:	To enable an update from a healthcare provider directly to the patient's healthcare record to provide an update of the care or treatment delivered.

	Responsible Party	
Responsibility	**Provider (Sender)**	**Consumer (Receiver)**
Determine the means of processing	Yes	Yes
Determine the purpose of processing	Yes	Yes
Responsible for reporting a personal data breach to Information Commissioner and, where applicable, data subjects under Article 33 of the UK GDPR	No	Yes
Response to the data subject in exercising their rights under UK GDPR, acting as a single point of contact for data subjects	No	Yes
Providing information to the data subject: Articles 13 and 14 UK GDPR	Yes	Yes
Publishing the Controller's responsibilities to ensure transparency	Yes	Yes

	Responsible Party	
Responsibility	**Provider (Sender)**	**Consumer (Receiver)**
Risk assessment of processing and implementing and maintaining appropriate technical and organisational measures to ensure a level of security appropriate to that risk	Yes	Yes