Document filename:	Data Protection Impact Assessment		
Directorate / Programme	Product Development		
Document Reference	IAR0000767		
Information Asset Owner		Version External	
Author		Version issue date	**14/2/2022**

Data Protection Impact Assessment Direct Care APIs

Document Management

Revision History

Version	Date	Summary of Changes
1.2	09/9/2021	DPIA Me
1.3	14/2/2022	Context changes from national sharing based on COPI / Covid Direction to national data sharing agreement, new functions on web site showing sharing parties

Reviewers

This document must be reviewed by the following people:

Reviewer name	Title / Responsibility	Date	Version
	PTE Specialist	14/2/2022	1.3
	Senior Project Manager		1.3

Approved by

This document must be approved by the following people:

Name	Title / Responsibility	Date	Version

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.

Glossary of Terms

Term / Abbreviation	What it stands for
API	Application Programming Interface – the set of technical components enabling information to be exchanged (interoperability) between systems
Capability	The description for a set of business requirements being delivered by GP Connect APIs
Controller	Role identified in the Data Protection Act, for the persons/organisations carrying legal responsibility to ensure that the data in their control is governed in accordance with the act. A controller determines the purposes and means of processing personal data
Processor	The processor is responsible for processing personal data on behalf of a controller. If you are a processor, the GDPR places specific legal obligations on you; for example, you are required to maintain records of personal data and processing activities. You will have legal liability if you are responsible for a breach
DIP	Digital Interoperability Platform
FHIR	Fast Healthcare Interoperability Resources – open standard for healthcare data models and transfer resources https://www.hl7.org/fhir/overview.html - part of the API specification
GP Principal System suppliers	The GP Principal System suppliers are: EMIS, TPP, Vision and Microtest
MESH	Message Exchange for Social care and Health
IAO	Information Asset Owner
PDS	Personal Demographics Service is the national electronic database of NHS patient details such as name, address, date of birth and NHS Number (known as demographic information)
PRSB	Professional Records Standards Body
SCAL	Supplier Conformance Assessment List – an assurance document that is completed by a Consumer Supplier which documents how they meet the requirements detailed in the GP Connect Specifications
SDS	Spine Directory Service is an endpoint and identifier directory for Spine and Spine connected systems, containing information on accredited systems, services and NHS registered users
SSP	Spine Secure Proxy – the set of NHS 'Spine' functions which provide security & validation of Consumer - Provider API interactions
Provider	A Direct Care APIs Provider are usually but not limited to the Principal GP Clinical Systems, that provide the registered GP patient record data for the GP Connect APIs to consume
Consumer	A Direct Care APIs Consumer are the Systems that develop to access data via the GP Connect APIs
COPI	Control of Patient information (COPI) Notice.

Sender	The service sending a consultation summary (or other document) via Send Document as they have had an interaction with the patient that requires a message to be sent
Receiver	The recipient of Send Document

Contents

Purpose of this document

A Data Protection Impact Assessment (DPIA) is a useful tool to help NHS Digital demonstrate how we comply with data protection law.

DPIAs are also a legal requirement where the processing of personal data is *"likely to result in a high risk to the rights and freedoms of individuals".* If you are unsure whether a DPIA is necessary, you should complete a DPIA screening questionnaire to assess whether the processing you are carrying out is regarded as high risk.

By completing a DPIA you can systematically analyse your processing to demonstrate how you will comply with data protection law and in doing so identify and minimise data protection risks.

This document should be read in conjunction with the DPIA Guidance and DPIA Screening Questionnaire

Introduction to Direct Care APIs / previously known as GP Connect

This service is known as GP Connect to the wider NHS and Direct Care within NHS Digital.

Organisations who use or have developed a Direct Care APIs product should use this document to understand NHS Digital's and their responsibilities as a Controller or Processor. The document can also be used as a starting point for organisations and considering their own privacy and data risks and how they should be mitigated and managed locally.

The DPIA is a living document and will continue to be updated as the service launches, progresses new functionality and products through First of Type testing and then moves into live service. Use in new care settings will also be noted.

1. Consultation with Stakeholders

This impact assessment has been developed in consultation with the following stakeholders:

- NHS Digital GP Connect Programme team
- NHS Digital Information Governance (IG) team
- NHS Digital Clinical Safety team
- NHS Digital Information Security team
- NHS Digital Clinical leads

The IG model, assurance principles and technical architecture of GP Connect has been developed in consultation with the following stakeholders:

- NHS Digital Deputy Caldecott Guardian
- The Information Commissioner's Office (ICO)
- The Information Governance Alliance (IGA)
- The Joint GP IT Committee
- NHS Digital GP Connect Programme team
- NHS Digital IG team
- NHS Digital Clinical Safety team
- NHS Digital Information Security team
- NHS Digital Clinical leads

The GP Connect data specifications have been developed in consultation with:

- INTEROPen (Interoperability SME network)
- NHS Digital Clinical leads
- NHS Digital Clinical Safety team
- NHS Digital Data Standards team
- NHS Digital Clinical Terminologists
- The Principal Clinical System Suppliers
- Professional Records Standards Body (PRSB)

The Direct Care APIs programme has not actively engaged at a patient level, this decision was taken for the following reasons:

- Although patients will benefit from the interoperability provided they are not the users of Direct Care APIs functionality
- The Direct Care APIs deal with access to the GP Patient Record for the purposes of direct care. It is the responsibility of the identified Controller to inform those Data Subjects (patients) the ways in which their data is accessed and shared.
- Other programmes within NHS Digital have dealt more widely with the subject of patients support of Data Sharing, The Direct Care APIs apply the outcome of their engagement where necessary (e.g. data will not be shared if a patient has a ‘dissent to share’ flag on their record)

2. Summary of the Direct Care APIs Service

GP Connect is for direct patient care

Direct Care APIs products can help people share, view or act on information that they are legally entitled to access, but cannot do so easily because they are using different IT systems. Direct Care APIs can only be used for direct patient care, not for planning or research. Direct patient care is defined as 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 making sure care and treatment is safe and high quality through local audits, managing when things go wrong, and working to improve satisfaction by measuring patient outcomes.*

Direct Care APIs products

Access Record

Access Record allows authorised clinicians to access GP patient records held on their practice system. Access Record has two methods of retrieving data from the patient record;

- Access Record: HTML enables a read-only view of a patient's record regardless of the practice clinical system. The record can be viewed within another care setting including another GP practice, an urgent care call centre, or an acute care organisation via an accredited system or application
- Access Record: Structured provides access to a patient's record in a machine-readable, structured, and coded format. Structured data allows the consuming system to import and process patient data provided that it's only used for direct care, and the system meets the specified GP Connect consumer requirements, including information governance and clinical safety standards.

Update Record

Update Record provides a simple and standardised way of updating a patient record. It sends a consultation summary that may have taken place away from the patient's registered practice. Each message sent using Update Record makes use of the GP Connect Messaging components ITK3, and MESH to deliver the message.

Appointment Management

Appointment Management is used to book appointments on behalf of a patient into their registered practice or another care setting. This is useful for services such as NHS111 and is being used to manage appointments for the COVID-19 vaccination programme.

3. Details of the Direct Care APIs Service

Direct Care APIs services can be accessed by an authorised NHS clinician (or administrator) via their clinical system, when they are required to support direct patient care.

Access Record APIs enable a clinician to access patient information in real time by requesting the information - via their clinical system - from the patient's registered GP practice, where the information is held. Appointment Management API allows a clinician and authorised staff to manage appointments by enabling appointment information to be requested from another clinical system. The requesting clinician (or administrator) may be in another practice, an acute hospital, 111 call centre, or other care setting.

The Service utilizes two main Spine components to securely transfer messages between clinical systems;

- The Spine Secure Proxy (SSP) – this is used to transfer patient record (Access Record: HTML and Structured) and Appointment Management products,
- The Message Exchange for Social Care and Health (MESH) – this is used for the Messaging products.

The GP Connect Service also relies on two main Spine components to provide prerequisite information to the Consumer systems so they can send messages to the right organisations:

- PDS (Personal Demographic Service) – all Consumer systems must use PDS to obtain a patient's NHS number, date of birth and registered practice,
- SDS (Spine Directory Service) – all Consumer systems must use SDS to obtain details about the target GP provider organisation.

4. Data Flow Diagram: Access Record and Appointment Management

Figure 1 shows the interactions between components when the SSP is utilised for transferring requests for patient record and appointments information. The consuming system may design their transaction to use these components as follows:

- A request for information is raised in the Consumer system (the clinical system used by the clinician or administrator),
- The consumer system would use two NHS Digital Spine components, PDS and SDS, to identify the patient's registered practice and build an endpoint that will direct the message to the patient's registered practice (NB - appointment requests can be made to other practices or hubs),
- The request is then sent to the SSP where the request is validated and audited,
- If the validation is successful, then the request for information will traverse NHS Digital Infrastructure and the Provider System (the clinical system for the patient's registered GP practice, or the clinical system where the patient is being booked for appointment management) will receive the request and return the appropriate information via the Spine Secure Proxy to the Consumer system.
- Data Sharing Rules are all set to share but the component is still in use to validate the capability and is how a limitation may be set for first of type.

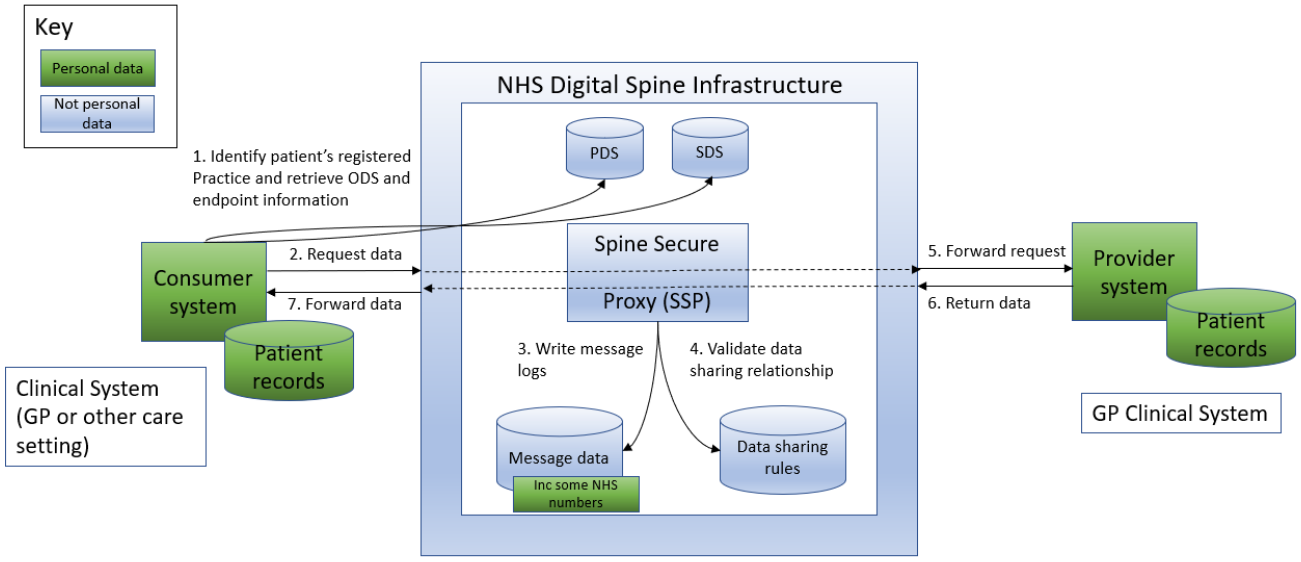

Figure 1 – Technical Architecture of the Service using the SSP (HTML, Structured and Appointment Management capabilities)

5. Data Flow Diagram: Send Document

Figure 2 shows the flow of messages when MESH is used to transfer messages back to a patient's registered GP practice or to an alternative care provider where Send Document has been configured. The flow can be described as follows:

- After a consultation with a patient takes place, the sender system writes a summary of the consultation to send to the patient's registered practice or an alternative care provider. This results in a message being constructed containing a PDF of the consultation, it may contain additional binary documents (for example, images)
- Using the MESH client or API, the sender sends the message to the MESH server for collection on behalf of receiver.
- The MESH client or API is used to collect the message from the MESH server and makes it available to other system components in the receiving system for onward processing.
- The message is processed in the receiving system, usually this will result in a task being created in the practice workflow.
- Once received the receiving system will send back an infrastructure acknowledgement to say the message has been received, followed by a business acknowledgement once the message has been processed and accepted by the receiving system
- Three message payloads are available for sending patient data:
  1. **Consultation Summary Report** – designed to send a patient consultation summary back to the patient's registered GP practice
  2. **Online Consultation Report** – designed to send a patient populated online consultation (survey) to the patient's registered GP practice, or to alternative care provider
  3. **Generic Report** – designed to send FHIR structed documents from any* sender to any receiving system(* sender/receiver systems must be approved for usage)

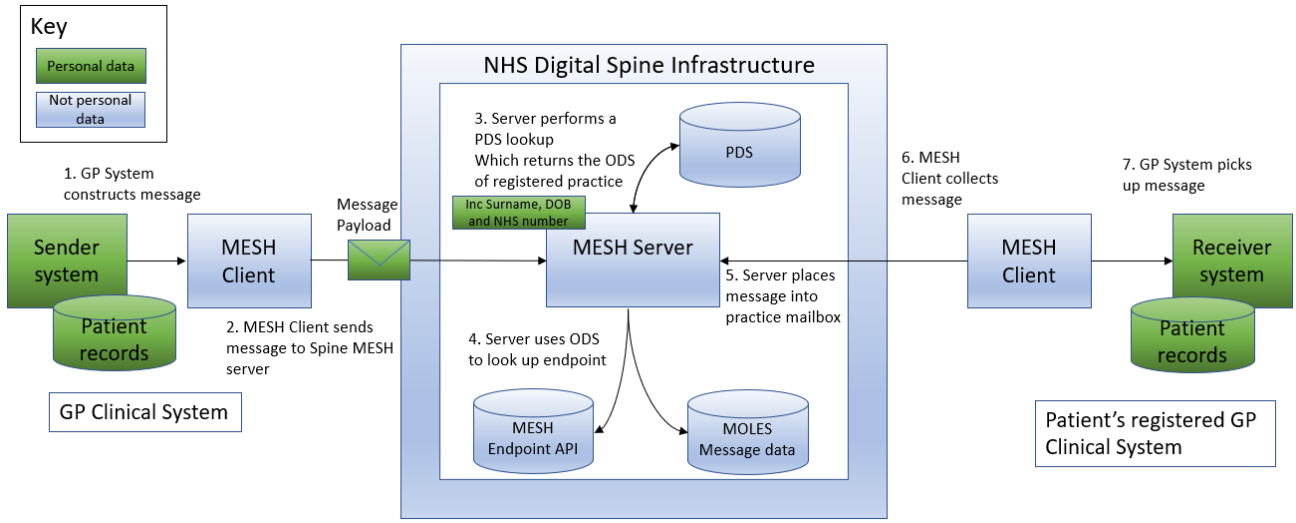

Figure 2 – Technical Architecture of the GP Connect Service using MESH (Messaging capability) note that MOLES is the audit data repository of MESH

Whilst NHS Digital is delivering the Direct Care APIs service, its role in the end-to-end flow of information is minimal, being limited to the use of the SSP and MESH for message validation and transfer. The main constituent parties involved in the service are the Provider (Receiver) and Consumer (Sender) Systems.

6. Purpose of the processing

NHS Digital has been commissioned to develop and operate a series of services which will support new models of care and allow health and care professionals to get the information they need to deliver the best possible care for patients. Together these services are known as the Digital Interoperability Platform, it will bring together care information related to the patient at the point of care. The services will support wider sharing of records along care pathways and across organisational boundaries.

Direct Care APIs provide part of the wider Digital Interoperability Platform. The Direct Care APIs service allows GP practices and clinical staff to share GP Practice clinical information and data between IT systems, quickly and efficiently via Application Programming Interfaces (APIs). These APIs make data from clinical systems available in a standard format that can be used across different systems and be made available to clinicians who need access to the data for direct patient care. From a privacy/data protection perspective, the service provides more secure information transfer using the APIs, removing the need to use less secure methods of information transfer, such as email or fax. They also provide an alternative real time access to patient data, free of charge without local sharing restrictions.

7. Description of the Processing

Nature and scope of the processing:

GP Connect has components, within the *Digital Interoperability Platform,* which enable interoperability between GP Clinical Systems and other consumer care setting systems. The components comprise of:

- A set of **standardised, non-proprietary APIs** used by all provider systems. The capabilities provided via these APIs are:
    - An HTML (webpage) view of a patient's record
    - Appointments Management – booking, amending, cancelling and viewing appointments.
    - An coded, structured export of a patient's record
    - Access to unstructured attachments to the patient record
    - The ability to send a message back to the patient's registered practice or alternative care provider.

- **Central (NHS Digital) Spine-based 'middleware' (the Spine Secure Proxy, SSP)** – this component provides security and message validation functionality for NHS Digital, enabling more open, generic interfaces and appropriate controls to be put in place.

- **Central (NHS Digital) Spine-based 'middleware' (The Message Exchange for Social Care and Health (MESH)** – this is the main messaging service used across health and social care. It's used to transfer electronic messages directly from one clinical system to another, so different organisations can communicate securely.

- A **Data Sharing Configuration File Rule Builder Tool** which enables the maintenance of the data-sharing validation file used by SSP to validate that a data-sharing agreement is in place between requesting (consuming) and providing organisations; SSP will only pass messages where a data-sharing agreement exists between these participating organisations. The data sharing tool has been set to allow data to flow between all organisations, since national data sharing was invoked with COPI and new capabilities will need to be added to the Tool. This is how a controlled rollout can be staged for new capabilities.

The GP Connect Service also has the following non-technical components:

- A **Commercial Framework** which allows suppliers to use the standard interfaces.

- An **Onboarding process**, which provides:
    - A Developer Portal which contains the technical guidance, documentation and tools required for easy development using GP Connect APIs
    - An End User Organisation Portal which contains the guidance and the Declaration needed for Commissioning or End User organisations to commission GP Connect Capabilities to be implemented in their area or organisation
    - Conformance and assurance processes, including engagement with Commissioning organisations to enable end-user organisations to commission GP Connect Capabilities to be implemented in their area or organisation
    - A National Data Sharing Agreement is part of the commercial framework and lays out the responsibilities of end user organisations and NHS Digitals role in supporting the service.

- **Ongoing API platform management -** Information Governance components will need to be aligned as required to any evolving solutions designed to meet broader strategic objectives for interoperability

GP Connect Actors

The following table describes the Actors (human, organisational and system) involved in the deployment and use of the GP Connect service, and their role:

What/Who	Role
Healthcare Organisation	May be a commissioning organisation, a Consuming (deploying) organisation or data Providing Organisation
End User Organisation (EUO)	An organisation which has an enabled provider or consumer GP Connect system. An End User Organisation can be: • An organisation deploying the GP Connect-enabled Consumer system to access GP Connect services; • Or the patient's current, registered GP practice, or other appointment-hosting practice that holds the patient's record and which is responsible for patient information shared via the GP Connect Services
Consumer System	The technically conformant and commissioned (deploying) system that is consuming data via the GP Connect API
Commissioning Organisation	The organisation with overall responsibility for the deployment by: • Either commissioning the development of a GP Connect-enabled Consumer System • Or leading the deployment of GP Connect capabilities within a group of deploying organisations
Provider System	The Principal Clinical System providing the data in response to a SSP validated request for patient data, currently this is the patient's registered practice system
API Interactions	These implement the capabilities being delivered by GP Connect
Personal Demographics Service (PDS)	All GP Connect Consumer systems must use PDS to obtain a patient's NHS number, date of birth and registered practice
Spine Directory Service (SDS)	All GP Connect Consumer systems must use SDS to obtain details about the target GP provider organisation
Spine Secure Proxy (SSP)	The Spine component controlling access and validating the API interactions for information requests to the Provider Systems
The Message Exchange for Social Care and Health (MESH)	The Spine component which is used to transfer electronic messages directly from one clinical system to another
Data Sharing Configuration File Rule Builder Tool	A tool that builds the data-sharing validation file used by SSP to check if a request for information from one organisation to another is underpinned by a valid Data Sharing Agreement, as described above
Developer Portal (currently hosted on the Developer Network)	Externally facing resource available to suppliers that supports: • Principal system suppliers to develop and test in an unsupported, independent environment.

	• Consumer system suppliers to develop and test in an unsupported, independent environment • The assurance and accreditation processes carried out by NHS Digital Solutions Assurance team
Supplier Conformance Assessment List (SCAL)	Collates consumer suppliers' evidence of the technical conformance of their systems to the GP Connect specification
End User Organisation Onboarding Portal	The provision of an End User Organisation Onboarding Portal where Commissioning organisations can commission GP Connect Capabilities via a self-serve process
End User Organisation Declaration ('Declaration')	The Declaration is hosted on the Portal and is an online form which requires a Commissioning organisation or an End User Organisation to confirm their compliance to NHS Digital requirements. Once submitted the Declaration and End User Organisation Terms forms part of the agreement between NHS Digital and the EUO(s).
Sender	The sender of the messaging capability via MESH
Receiver	The recipient of the messaging capability via MESH.

NHS Digital Responsibilities

For the GP Connect Service, NHS Digital is responsible for:

- The development and upkeep of the API specifications which are clinically safe and set out clearly to explain how the suppliers should develop their products.
- The review of test evidence from the consumer suppliers to assess the technical conformance of a Consumer system's use of the APIs, including the review of test evidence of information security controls.
- Assuring that Provider Systems are meeting the necessary information governance and information security requirements. The DSPT is completed which provides a common confidentially and security tool for all GPS and NHS care providers
- The development and maintenance of self-service assurance (currently the Supplier Conformance Assessment List – shortened to the SCAL) and onboarding materials for consumer suppliers.
- Assuring the SCAL for completeness; this includes the necessary framework requirements, e.g. Usage and Settings Statement, Clinical Safety requirements, Information Governance requirements
- Obtaining confirmation from lead End User Organisation or Commissioning Organisation that there are appropriate IG arrangements in place.
- The programme will continue to support how data sharing arrangements can be made visible to end users, a portal and data sharing agreement is being prepared to transition from COPI
- Mitigation and management of the information security risks incurred by Spine processing - these are found in IAR000144 Spine Core DPIA
- The safe and responsible use and storage of SSP audit data
- The safe and responsible use and storage of MESH audit data
- The validation of legitimate requests to the SSP for the use of GP Connect services
- Ensuring the secure, accurate and safe transfer of messages containing patient data while it traverses Spine (NOTE: the patient data contained within GP Connect messages is not collected or stored by NHS Digital)
- Dealing with incidents when / should users are reported to be using the service inappropriately

Notification to relevant Stakeholders (such as, NHSX, NHS England, Department of Health and Social Care, the Provider Organisation and the Consumer Organisation) if there is a data breach

that occurs during the processing of data over Spine. This is fulfilled by the Spine Core System Level Security Policy (SLSP)

Context of the processing:

NHS Digital 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 GP Connect Service. The signed Direction (Establishment of systems: digital interoperability platform 2019) can be found on the NHS Digital website.

To comply with the Direction, NHS Digital is a Controller for the delivery of the GP Connect Service, which means NHS Digital is responsible for establishing and maintaining a service which enables interoperability between GP IT systems. For NHS Digital to support the GP Connect service, audit data about the message transactions is collected, which is used for operational support by service management. NHS Digital is a Controller for the message audit data collected on Spine.

To fulfil the role of Controller, NHS Digital is also responsible for ensuring that the messages traverse NHS Digital's Infrastructure securely, accurately and safely to and from provider and consumer systems for the purposes of Direct Patient Care. The content of the messages is not collected or stored by NHS Digital. NHS Digital processes the messages on behalf of the GP practices, who are Controllers of the GP patient record.

The scope of this DPIA is limited to assessing the risks associated with NHS Digital's role as Controller as part of GP Connect Service. This means that it covers how the messages are transferred securely over NHS Digital infrastructure, including:

- The safe and accurate transfer of messages over NHS Digital Infrastructure to Provider and Consumer systems.
- the collection and storage of audit data which is collected as part of the message transaction.
- the assurance of the components that directly interact with the NHS Digital Infrastructure to deliver the GP Connect Service.

Details of NHS Digital's responsibilities are set out below.

Outside the scope of this DPIA is the assessment and mitigation of information risks in the Consumer and Provider systems and the End User Organisations who use those systems to access the GP Connect service.

It is the legal responsibility of each Data Controller and Processer, whom are a component of, or a user of the GP Connect Service, to assess and manage their own data protection risks.

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

Direction was given by the Secretary of State for the Department of Health and Social Care to establish and operate the Digital Interoperability Platform (which includes GP Connect) using the powers given under section 254 of the Health and Social Care Act 2012.

The legal basis for NHS Digital's processing under GDPR is Article 6(1)(c) – the 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 GDPR 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'.

There is no disclosure process other than ad-hoc as part of Subject Access Request process. The common law duty of confidentiality is met by implied consent

A patient can opt out via the local record share, there is no override in GP connect

Additional controls include

- Parts of the record marked as sensitive or confidential are excluded from sharing
- RCGP exclusion set is respected, and no data shared
- 'S' Flag rules are respected, and no data shared

9. Demonstrate the fairness of the processing

The Direct Care APIs are passed over NHS Digital Infrastructure to allow seamless information sharing where it is necessary for a patient's direct care. The processing is only for the purposes of direct care and is in line with the sharing that a patient would reasonably expect to be shared between clinicians for the purposes of caring for that patient. The Direct Care APIs respects a patient's 'Dissent to Share' decision as flagged in their record and also respects anything marked as sensitive or private within the record, so this information is not shared.

Audit data is captured when any message is transferred using either the SSP or MESH, this collection is limited to what is needed for service management to be able to support the service.

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

Transparency information about the data collected by NHS Digital is published on the NHS Digital website on the GPDR register.

End User Organisations are notified of their duty as Controllers to be fair and transparent about their processing of their patients' data. They are required to ensure they are GDPR and DPA compliant to complete a Declaration for GP Connect, which is a prerequisite to deployment. As part of this compliance to IG regulations they have to ensure that they have updated their Privacy information about how patient data is being used.

NHS Digital has a new portal which aims to explain the sharing of data through this service by End User Organisations.

11. Is it necessary to collect and process all data items?

Data Categories [*Information relating to the individual's*]	**Yes**	**Justify** *[there must be justification for processing the data items. Consider which items you could remove, without compromising the purpose for processing]*
Personal Data		
General Identifier e.g. NHS No	X	**Patient Data** – the NHS Number is used in some of the message URLS transferred over the SSP to inform the provider system whose information is required by the consumer system. The URL is stored in the SSP Audit Log.

Data Categories [*Information relating to the individual's*]	**Yes**	**Justify** *[there must be justification for processing the data items. Consider which items you could remove, without compromising the purpose for processing]*
General Identifier e.g. Registration details	X	**Practitioner information** – the details of the practitioner involved in the consultations or appointments is used in some of the message URLS transferred over the SSP to inform the provider system whose information is required by the consumer system. The URL is stored in the SSP Audit Log.
Online Identifier e.g. IP Address/Event Logs	X	**Direct Care APIs User** – IP Address of device used by the user when interacting with Spine, this is stored as part of the audit log of which organisations have passed messages using GP Connect.
Special Category Data		
Physical / Mental Health or Condition	X	**Patient Data** – GP Connect passes messages containing patients' health data safely and securely over NHS Digital Infrastructure between authorised health and care professionals for the purposes of Direct Care. The content of the messages is not collected or stored by NHS Digital.

12. Describe if personal datasets are to be matched, combined or linked with other datasets? (internally or for external customers)

The Direct Care service includes use of a set of APIs. All suppliers, as an obligation for patient safety, check against PDS records for individual patients as part of the transaction set.

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

N/A

14. How long will the personal data be retained?

GP Connect audit-data follows the same retention period as that of Spine 2 where audit data is required to be retained for a 2-year period. Audit data within the consumer and provider systems has a longer retention period as the audit data collected by those systems is more granular and therefore can be used to audit how a patient's information has been accessed and shared using GP Connect which is required under GDPR.

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

NHS Digital is not responsible for how the personal data is obtained as the data that is processed by the GP Connect service is limited to data that has already been collected by clinicians as they use and update a patient's GP record

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

Individual Right	Yes/No	Justifications
Right to be informed (Articles 13 and 14)	Yes	Transparency information is published on the NHS Digital website so the public can see how their data is being used Information about the collection of organisation data is laid out in this DPIA which is available on the End User Organisation Portal and is also available on request from the GP Connect mailbox
Right of Access (Article 15) – "I want to see my data and what you do with it"	Yes	Subject Access Requests can be made here
Right of Rectification (Article 16) – "I want to add or change inaccurate data"	Yes	Will comply with corporate policy
Right to Erasure (Article 17) – "I want my data deleted"	No	This right does not apply under GDPR Article 17 3 (c)
Right to Restrict Processing (Article 18) – "Stop processing my data in that way"	Yes	Will comply with corporate policy
Right to Data Portability (Article 20) – "Give me a copy of my data"	No	This right does not exist since user consent is not the legal basis for this processing
Right to Object (Article 21) – "Stop doing that with my data"	No	This right does not exist because NHS Digital is legally bound to record this data as part of operating the Spine system
Right not to be subject to automated decision-making (Article 22) – "You can't use my data for 'computer-says-no' decisions"	No	This right does not apply as no automated decision-making is performed

17. What technical and organisational controls for "information security" have been put in place?

GP Connect is covered by the following System Level Security Policy:

SLSP	Unified Register ID
Spine Core	SLSP0000028

NHS Digital helps support the mitigation of information sharing risks by ensuring that the following are in place:

- NHS Digital audit data access is subject two factor authentication and role-based access controls. Only certain assured users can have access to the full audit logs.
- A completed Supplier Conformance Assessment List (SCAL) which covers service and capability specific compliance requirements and controls of the consumer system.
- The End User Organisations of the Direct Care APIs Service have to meet be compliant with the Direct Care APIs' requirements which cover IG, Clinical Safety, and acceptance of the Terms of Use of NHS Digital Services.
- As part of the Onboarding process, a list of participating End User Organisations is provided. Data sharing verification may be implemented to restricted access to GP Connect services to only those with valid data sharing rules within the SSP (via the Data Sharing Configuration File Rule Builder Tool) or bypassed where national data sharing rules apply
- The programme will transfer the declaration process to an online portal when the current National Data Sharing supported by COPI transitions to a new arrangement.
-

When MESH is used, a sending organisation will have to provide both the Mailbox ID and Workflow ID of the target organisation to be able to retrieve the matching MESH mailbox. MESH messages include a mandatory Workflow ID field that identifies the type of data being sent. Workflow IDs are pre-defined and grouped into Workflow Groups which are then defined against MESH mailboxes to identify the types of messages it can send and receive.

18. In which country/territory will personal data be stored or processed?

NHS Digital commits to storage and processing in England.

19. Does the National Data Opt Out apply to the processing?

The national data opt-out is defined based on purpose and applies to any disclosure of data for purposes beyond individual care. Therefore, as GP Connect processes data for the purposes of direct care, the national data opt-out doesn't apply.

Though the opt-out is not applicable, GP Connect doesn't transfer a patient's record (via either HTML or Structured capabilities) if there is 'dissent to share' flag or an 'S' flag on a patient's record.

Appointments can still be booked for patients with the 'dissent to share' flag as only limited demographic information is transferred during the booking process

20. Identify and assess risks

Consider the potential impact of your processing and the potential harm or damage that it might cause to individuals whether physical, emotional, moral, material or non-material e.g. inability to exercise rights; discrimination; loss of confidentiality; re-identification of pseudonymised data, etc.

You can also use this section to detail any risks you have in complying with data protection law and any resulting corporate risks e.g. impact of regulatory action; reputational damage; loss of public trust, etc.

Describe source of the risk and nature of potential impact on individuals	**Likelihood of harm** (Remote; reasonable possibility or more likely than not)	**Severity of impact** (Minimal impact; some impact; or serious harm	**Overall risk rating** (Low; medium; or high)
Provider and Consumer Organisation risk - Patients unaware that their data may be shared using GP Connect for their direct care	Reasonable possibility	Some impact	Medium
Provider and Consumer Organisation risk - Patient identifiable and confidential information used for purposes other than direct care	Remote	Some impact	Low

Provider and Consumer Organisation risk - Patient identifiable and confidential information used for unassured use cases/clinical settings within direct care	Remote	Some impact	Low
Provider and Consumer Organisation risk - Patient record accessed by Consumer Systems without the necessary security framework	Remote	Some impact	Low
Provider and Consumer Organisation risk - Patient record accessed by end users without appropriate authorisation	Remote	Some impact	Low
Provider and Consumer Organisation risk - Patient record-sharing dissent overridden	Remote	Some impact	Low
NHS Digital risk - Loss of availability of the GP Connect service	Remote	Some impact	Low
NHS Digital risk - Whole system failure	Remote	Some impact	Low

NHS Digital risk - Patients confused about how to find out about their data use in Direct Care APIss and coming to us not GPs	Reasonable possibility	Minimal impact	Low

20.1. Measures to mitigate (treat) risks

Against each risk you have identified, record the options/controls you have put in place to mitigate the risk and what impact this has had on the risk. Make an assessment as to the residual risk.

Also indicate who has approved the measure and confirm that responsibility and timescales for completion have been integrated back into the project plan.

Risk	**Options to mitigate (treat) the risk**	**Effect on risk** (Tolerate / Terminate / Treat Transfer)	**Residual risk** (Low / Medium / High)	**Measure approved** (Name and Date)	**Actions integrated back into project plan** (Date and responsibility for completion)
Provider and Consumer Organisation risk - Patients unaware that their data may be shared using GP Connect for their Direct Care	The End User Organisations and Commissioning Organisations are required to ensure they are GDPR and DPIA compliant. As part of this compliance to IG regulations they have to ensure that they have updated their Privacy information about how patient data is being used. NHS Digital has published Transparency information about the GP Connect Service on its website and a	Treat	Low	Michelle McDermott 07/11/2019	

	portal provides information on which organisations are using the service.				
Provider and Consumer Organisation risk - Patient identifiable and confidential information used for purposes other than Direct Care	All Direct Care APIs documentation and guidance states that this information sharing is for the purposes of direct care only. The Commissioning Organisation has to agree to this on behalf of all in scope End User Organisations. A consumer supplier has to state it's intended use when completing assurance. the system has to be for Direct Care only. NHS Digital retains ability to audit and check compliance to agreements and revoke access if consumers are not using the data for direct care.	Treat	Low	Michelle McDermott 07/11/2019	
Provider and Consumer Organisation risk - Patient identifiable and confidential information used for unassured use cases/clinical settings within Direct Care	All Direct Care APIs documentation and guidance states that this information sharing is for the purposes of direct care only. The Commissioning Organisation has to agree to this on behalf of all in scope End User Organisations as part of completing the Declaration. A Consumer supplier has to state it's intended use when completing assurance of its GP Connect system, the system has to be for Direct Care only. NHS Digital retains ability to audit and check compliance to agreements and revoke access if consumers are not using the data for direct care.	Treat	Low	Michelle McDermott 07/11/2019	

Provider and Consumer Organisation risk - Patient record accessed by Consumer Systems without the necessary security framework	Consuming organisations and systems must be HSCN and Data Security and Protection Toolkit compliant and meet national requirements for Technical (Endpoint) Security. The SCAL and provider assurance requires suppliers to evidence their Information Security Management System (ISMS) and compliance with the standard BS ISO/IEC 27001:2005 BS7799-2:2005. NHS Digital retains ability to audit and check compliance to agreements and revoke access if consumers compliant.	Treat	Low	Michelle McDermott 07/11/2019	
Provider and Consumer Organisation risk - Patient record accessed by end users without appropriate authorisation	The responsibility is picked up during consumer assurance via the SCAL End User Organisations should ensure that appropriate role-based access is in place to access the information transferred via the Direct Care product developed.	Treat	Low	Michelle McDermott 07/11/2019	
Provider and Consumer Organisation risk - Patient record-sharing dissent overridden	Patient clinical data is not provided in this scenario with a message sent to the Consumer system that the patient has dissented to share. These controls are part of the Provider System supplier IG requirements and SCAL submission. Direct does not accommodate the overriding of locally held Patient Dissent.	Treat	Low	Michelle McDermott 07/11/2019	

NHS Digital risk - Loss of availability of the GP Connect service	In the scenario where an End User Organisation suffers a loss of GP Connect service the organisation should revert the business process that was in place prior to the implementation of GP Connect. The loss of service should be flagged to the relevant service desk immediately. The National Service Desk at NHS Digital will coordinate and triage if the cause of the loss of availability is unknown or covers more than one supplier.	Tolerate	Low	Dan O'Neill 01/11/2019	
NHS Digital risk - Whole system failure – SSP and MESH	In the scenario where NHS Digital Infrastructure fails and causes a whole system failure the End User Organisations should revert the business process that was in place prior to the implementation of GP Connect. The loss of service should be flagged to the relevant service desk immediately. The National Service Desk at NHS Digital will coordinate and triage the work to identify the cause of the loss of availability.	Tolerate	Low	Dan O'Neill 01/11/2019	
NHS Digital risk - Human error in setting up DSAs on Spine	All staff who amend the data sharing relationships on Spine are required to undergo training prior to using the tool.	Treat	Low	Michelle McDermott 07/11/2019	

NHS Digital risk - Patients confused about how to find out about their data use in GPC and coming to us not GPs	NHS Digital has published Transparency information about the GP Connect Service on its website. It has also published information about the service and its purpose on its website.	Treat	Low	Michelle McDermott 07/11/2019	
NHS Digital risk – Services (GPs) confused about how to find out about their data use in GPC	Transparency information about the GP Connect Service on its website. In addition, the portal will be developed to support data sharing.	Treat	Medium	Michelle McDermott 21/5/2021	

21. Further Actions

- The completed DPIA should be submitted to the PTE Helpline Service (ighelplineservice@nhsdigital.nhs.uk) 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)

22. 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 PRIVACY, TRANSPARENCY AND ETHICS AND OFFICE OF THE DPO USE ONLY

23. 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**