Document filename:	**Data Protection Impact Assessment**		
Directorate / Programme	**GP Connect Programme**	Date published	**11/02/2019**
Document Reference	**GP Connect IAR0000767 DPIA**	Status	**Published**

Data Protection Impact Assessment – IAR0000767 GP Connect Service

Document Management

Revision History

Version	Date	Summary of Changes
1.0		Published

Approved by

This document must be approved by the following people:

Title / Responsibility	Date	Version
Information Asset Owner		

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
Data 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
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
IAO	Information Asset Owner
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
SSP	Spine Security Proxy – the set of NHS ‘Spine’ functions which provide security & validation of Consumer - Provider API interactions

Contents

1. Introduction

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.

GP Connect is one of the services that is part of the wider Digital Interoperability Platform. The GP Connect 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.

This Data Protection Impact Assessment (DPIA) has been undertaken during the development of the GP Connect service to enable NHS Digital to systematically identify and minimise the privacy and data protection risks of the introduction of this new service.

The GP Connect Programme initiated this work to understand the privacy and data protection risks in late 2016 and since this point this document has gone through several iterations to ensure it stayed relevant to the programme and it has responded to stakeholder feedback. The DPIA is a living document and will continue to be updated as the service launches, progresses through First of Type testing and then moves into live service.

2. DPIA Scope

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.

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.

NHS Digital acts as a Processor for the content of the messages that are passed using the GP Connect Service, this means that NHS Digital is responsible for the processing of messages as they traverse NHS Digital Infrastructure, and ensure they are passed securely, accurately and safely to and from provider and consumer systems. The content of the messages is not collected or stored by NHS Digital. NHS Digital is not a Controller of the content of the messages passed between clinicians using the GP Connect Service. NHS Digital processes the messages on behalf of the GPs, who are controllers of the GP patient record.

The scope of this DPIA is limited to assessing the risks associated with what NHS Digital is a Controller for as part of GP Connect Service. This includes the collection and storage of audit data which is collected as part of the message transaction via the Spine Security Proxy; and the assurance of the components that directly interact with the Spine to deliver the GP Connect Service. Details of what NHS Digital is responsible for is set out in Section 4 of this DPIA.

Outside the scope of this DPIA is the assessment and mitigation of information risks in the consumer and provider systems and the organisations that use them, or risks associated with the transfer of the message content between these systems.

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

3. Consultation with Stakeholders

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

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

The 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 (EMIS, TPP, Vision, Microtest)
- Professional Records Standards Body (PRSB)

For an explanation of the specification curation process please see Appendix A

4. Description of Data Processing

Summary

The GP Connect service offers a number of products which will enable different systems to communicate so that clinicians in different care settings can:

- view a patient's GP Practice record
- manage GP appointments
- import or download elements of a patient's record in a structured data format (currently limited to an export of a patient's medicines and allergies information)

This will save time for clinicians, and provide better, more convenient care for patients.

Detail of the GP Connect system

GP Connect services can be accessed by an authorised NHS Clinician (or administrator) via their clinical system from the patient's registered GP Practice, where it is required to support the direct care of that patient.
This is done by requesting the information - via their clinical system - from the patient's registered GP practice, where the information is held. The clinician (or administrator) may be in another practice, an acute hospital, 111 Call Centre or other care setting.

The topography diagram (figure 1) below shows this flow, it can be described as follows:

- A request for information is raised in the Consumer System (the clinical system used by the clinician or administrator)
- The request is then sent to NHS Digital infrastructure, known as the Spine Security Proxy (SSP), where the request is validated
- If the validation is successful, then the request for information will traverse the Spine and the Provider System (the clinical system for the patient's registered GP practice) will receive the request and return the appropriate information via the Spine Security Proxy

Whilst NHS Digital is delivering GP Connect, its role in the end-to-end flow of information is minimal, being limited to the use of the Spine Security Proxy for message validation. The main constituent parties involved in GP Connect are the Provider and Consumer Systems.

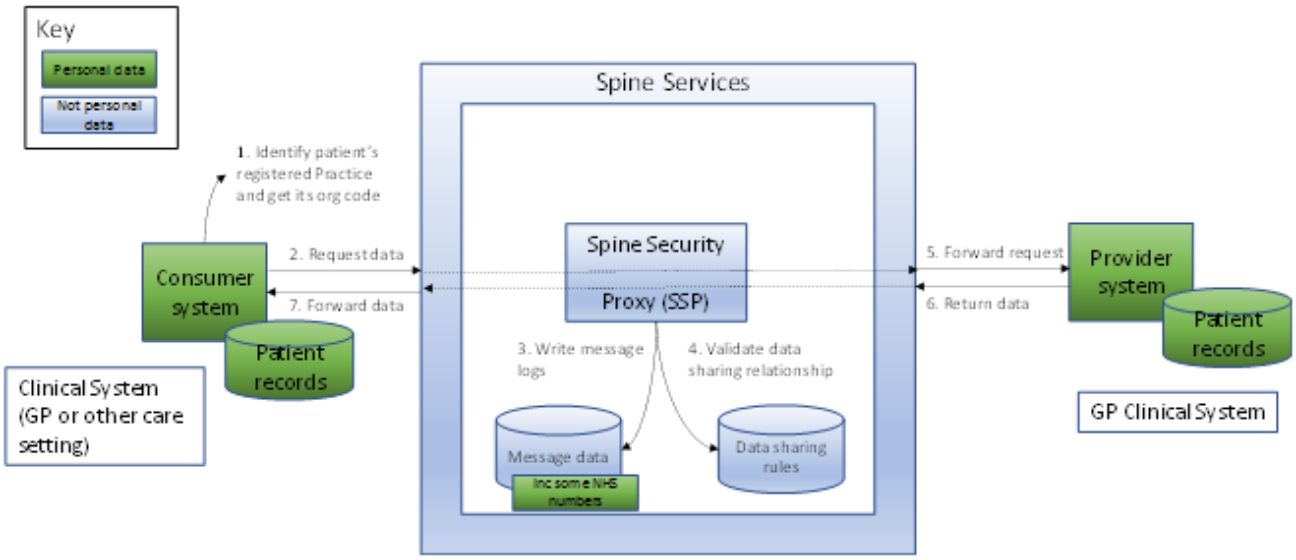

Figure 1 – Technical Architecture of the GP Connect Service

GP Connect Components

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 three Capabilities to be provided via these APIs are:
    - An HTML (webpage) view of a patient's record
    - Appointments Management – booking, amending, cancelling and viewing appointments
    - An export of a patient's medicines and allergies information (with further aspects of the patient's GP record to follow)

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

- 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 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 customer portal which contains the technical guidance, documentation and tools required for easy development using GP Connect APIs
    - conformance and assurance processes, including engagement with Commissioning organisations to enable end-user organisations to commission new or use existing GP Connect Capabilities

- **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
Consuming Organisation (also an End User Organisation)	The organisation deploying the GP Connect-enabled Consumer System to access GP Connect services
Consumer System	The technically conformant and commissioned (deploying) IT system that is consuming data via the GP Connect API
Commissioning Authority	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
Commissioning Organisation	The NHS organisation commissioning development of a GP Connect-enabled Consumer System
Providing Organisation (also an End User Organisation)	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
Provider System	The Principal Clinical System providing the data in response to a legitimate (SSP-validated) request for patient data

	For GP Connect the Principal Clinical Systems are: EMIS Web, TPP SystmOne, InPS Vision, and Microtest Evolution.
API Interactions	These implement the capabilities being delivered by GP Connect.
Spine Security Proxy (SSP)	The Spine components controlling access and validating the API interactions
Data Sharing Configuration File Rule Builder Tool	A tool that maintains the data-sharing validation file used by SSP, as described above
Developer Portal (currently hosted on the Developer Network)	Externally-facing resource available to end users and suppliers that supports multiple customers pathways including: • Consumer system suppliers to develop and test in an unsupported, independent environment • Consuming organisations to commission new or utilise existing GP Connect Capabilities via a self-serve process The portal will also support the assurance and accreditation processes carried out by NHS Digital Solutions Assurance team
Supplier Conformance Assurance List (SCAL)	Provides the assurance process and tools by which consumer suppliers evidence the GP Connect technical conformance of their systems
End User Organisation Onboarding Portal	The provision of an End User Organisation Onboarding Portal so Commissioning bodies can to commission new or utilise existing GP Connect Capabilities via a self-serve process

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
- Assessment of technical conformance of Consumer System use of the APIs, including the testing of information security controls
- Assuring that Provider Systems are meeting the necessary information governance and information security requirements
- The development and maintenance of self-service assurance (currently the Supplier Conformance Assurance 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
- Ensuring there are Data Sharing Agreements between Consuming and Providing Organisations
- Mitigation and management of the information security risks incurred by Spine processing (SSP). These are found in IAR000144 Spine Core DPIA
- The safe and responsible use and storage of SSP 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)
- Notification to relevant Stakeholders (such as, 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 the SSP. This is fulfilled by the Spine Core System Level Security Policy (SLSP)

NHS Digital helps support the mitigation of information sharing risks by ensuring that prior to the deployment of GP Connect, the following are in place:

- Data sharing agreements between the Providing and Consuming (deploying) organisations
- A completed Supplier Conformance Assurance List (SCAL) which covers: compliance requirements and controls of the consumer system, commissioning and deploying organisations, and the IG and Clinical Safety assurance activities of those parties

As part of the SCAL submission, a list of participating Providing and Consuming Organisations is provided. A Data-Sharing Group is created to represent this relationship within the Spine Security Proxy (SSP) (via the Data Sharing Configuration File Rule Builder Tool), which will reject interactions where the Providing and / or Consuming Organisation are not members of the same Data-Sharing Group.

5. Data Protection Impact Assessment Questions

5.1. Stakeholder Groups Consulted

See response detailed in Section 3

5.2. Is there a clear legal basis for the processing (collection, analysis or disclosure) of personal data?

Direction will be given by 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 processing which may be considered special category data the legal basis for the processing is Article 9(2)(h) – the processing is necessary for the management of health or social care systems and services.

There is no disclosure process other than ad-hoc as part of Subject Access Request process.

5.3. Are individuals clear about ways in which personal data about them is being used?

This DPIA covers the audit data which NHS Digital is a Controller of. This section does not cover the data that traverses Spine in the content of the message as NHS Digital is not a Controller of that data.

The data collected in the SSP audit dataset is purely about the message transaction (e.g. Time, Date, Type) but it does collect some **organisation data** therefore affects the End User Organisations. The SSP audit dataset also contains a small amount of **patient data**. This is limited to the NHS number, which is contained within the URL of some of the GP Connect messages that traverse the Spine.

Individuals are informed about how their data is used in the following ways:

- **Organisation data:** users of the GP Connect have to sign up to an End User Organisation Policy prior to GP Connect being deployed. Information about the data collected will be provided via the End User Organisation Onboarding Portal.
- **Patient data:** There is transparency information on the NHS Digital Website about the GP Connect audit dataset. (NOTE: A patient's registered GP Practice is responsible for making transparency information available about a patient's GP record.)

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

Data Categories [*Information relating to the individual's*]	**Yes**	**N/A**	**Justifications** *[there must be justification for collecting the data items. Consider which items you could remove, without compromising the needs of the project]*
Personal Data			
General Identifier e.g. NHS No	**X**		**Patient Data** – the NHS Number is used in the message URLS to inform the provider system whose information is required by the consumer system. The URL is stored in the Audit Log.
Online Identifier e.g. IP Address/Event Logs	**X**		**GP Connect User** – IP Address of device used by the user when interacting with Spine.

5.5. Will personal data be shared and/or merged with other datasets?

No

5.6. How long will personal data be retained?

GP Connect follows the same retention period as that of Spine 2 where Audit Data is required to be retained for a 2-year period.

5.7. How will standards of data quality be achieved and maintained?

GP Connect audit-data is written to log-files that are indexed into read-only, tamper-proof Splunk data-stores. The accuracy of these processes for every new log-point is verified by NHS Digital Solutions Assurance.

5.8. Are individuals made aware of their rights (under certain circumstances)?

Individual Right	**Yes/No**	**Justifications**
Right to be informed (Articles 13 and 14)	Yes	Transparency information is published on website so the public can see how their data is being used

		Information about the collection of organisation data will be laid out in the End User Organisation Policy Portal
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

5.9. If individuals exercise their rights how are these rights upheld?

See comments in Section 5.8

5.10. Have technical and organisational controls for "information security" been considered?

Yes – see following System Level Security Policy

SLSP	Unified Register ID
Spine Core	SLSP0000028

Organisational/service design controls:

Risk	Mitigation
Patients unaware that their data may be shared using GP Connect for their direct care	The Providing Organisations will be required to confirm these activities (notification to patients of information sharing potential) to NHS Digital Solutions Assurance as part of the deployment
Patient identifiable and confidential information used for purposes other than direct care	All GP Connect documentation and guidance states that this information sharing is for the purposes of direct care only. The Commissioning Authority will need, as part of the NHS Digital Supplier Conformance Assurance List (SCAL), to define Usage and

	Settings information to detailed use case and Capability level
Patient identifiable and confidential information used for unassured use cases/clinical settings within direct care	The Commissioning Authority will need, as part of the NHS Digital Supplier Conformance Assurance List (SCAL), to define Usage and Settings information to detailed use case and Capability level
Patient record accessed by Consumer Systems without the necessary security framework	Consuming organisations and systems must be N3/HSCN and Data Security and Protection Toolkit compliant, and meet national requirements for Technical (Endpoint) Security The GP Connect 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
Patient record accessed by end users without appropriate authorisation	Rules defined within the Data Sharing Configuration File Rule Builder Tool allow only those interactions between organisations where a DSA is in place.
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 GP Connect does not accommodate the overriding of locally-held Patient Dissent.

5.11. Will personal data be transferred outside the EEA?

No – service usage is limited to England.

6. Further Actions

This DPIA will be revisited during the lifecycle of the project / programme to ensure:

- Details of the processing are kept up to date
- Outcomes and measures identified are still relevant
- Actions recommended to mitigate risks are implemented
- Mitigating actions are successful

7. Appendix A - Curating the GP Connect Capability Specifications

The programme has worked with the GP Principal System suppliers, other NHS programmes, clinicians and SME groups to define (i) the standard dataset structures (FHIR Profiles) used as part of the GP Connect capabilities to carry the required information, and (ii) the business rules determining population of the profiles.

This work has involved several steps:

- The programme conducted analysis on the use cases gathered for the GP Connect capabilities. A logical model was created from this analysis that contained detailed records of the data items that the business required

- The team then analysed what information currently exists within the GP Principal Clinical Systems and how this is exported to support other NHS Digital projects. The projects considered have been: GP2GP, Summary Care Record (SCR) and Electronic Prescription Service (EPS). The programme also considered future needs of ongoing NHS Digital projects, such as; GP Data Implementation, Care Connect and the National Data Architecture team to ensure synergy between the NHS Digital projects

- This analysis was used to create draft profiles that were then discussed in detail with all four of the GP Principal Clinical System Suppliers to ensure their feasibility. Once this was done the profiles were taken through a curation process by a multi-disciplinary team that involved representatives from many organisations. These included: primary and secondary care clinicians, pharmacists, terminologists, data standards, clinical informaticians that had been involved in creating the base FHIR profiles, clinical safety representatives and representatives from primary and secondary care clinical systems suppliers and PRSB

All this analysis was then fed into the profiles that have been published by data standards as part of the GP Connect specification on the NHS Health Developer Network and are part of the Care Connect profiles, which are also published on the Network.