Data Protection Impact Assessment (DPIA)

Project Title:	**GP Connect roll-out in Humber, Coast and Vale for Direct Booking and Record Access**	
Project Description:	GP Connect is a national technology solution, delivered through NHS Digital (NHSD) that allows health and care organisations and authorised clinical staff to share and view GP practice clinical information as well as the direct booking of GP appointments from NHS 111, to improve patient care.	
Project Manager Details:		
	Title:	Business Change Lead
	STP:	Humber, Coast and Vale
Implementation date:	March 2020	

Information Asset Owner (IAO): (All systems/assets must have an Information Asset Owner (IAO).		
	Title:	Associate Director of IT
	STP:	Humber CCGs
	Telephone:	

Information Asset Owner (IAO): (All systems/assets must have an Information Asset Owner (IAO).		
	Title:	Head of Digital
	STP:	NHS Scarborough & Ryedale CCG
	Telephone:	
	Email:	

Information Asset Administrator (IAA): (All systems / assets must have an Information Asset Administrator (IAA) who reports to the IAO as stated above. IAA's are normally System Managers / Project Leads)	Name:	
	Title:	Business Change Lead
	STP:	Humber, Coast and Vale

Information Governance Approval
North East Lincolnshire CCG
Hull CCG
North Lincolnshire CCG
East Riding of Yorkshire CCG
Vale of York CCG
Scarborough & Ryedale CCG

Data Protection impact assessment screening questions:

Answering 'yes' to any of these questions is an indication that a DPIA is a necessary exercise. You can expand on your answers as the project develops if you need to.

You can adapt these questions if necessary for unusual circumstances.

Questions	Yes/No
Will the project involve the collection of new information about individuals?	no
Will the project compel individuals to provide information about themselves?	no
Will information about individuals be disclosed to 3rd party organisations or people who have not previously had routine access to the information?	yes
Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?	no
Does the project involve you using new technology which might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition.	no
Will the project result in you making decisions or taking action against individuals in ways which can have a significant impact on them?	no
Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records or other information that people would consider to be particularly private.	yes
Will the project require you to contact individuals in ways which they may find intrusive?	no

Step One: Identify the need for a DPIA

Explain what the project aims to achieve, what the benefits will be to the organisation, to individuals and to other parties.

You may find it helpful to link to other relevant documents related to the project, for example a project proposal.

Also summarise why the need for a DPIA was identified (this can draw on your answers to the screening questions).

To support GP practices in meeting the new GP Contract requirement to enable NHS 111 to directly book appointments with GP practices by 31 March 2020, we are implementing GP Connect to all GP practices in Humber, Coast and Vale (HCV).

GP Connect allows GP practices and Integrated Urgent Care (NHS 111) to share and view GP practice clinical information and data between IT systems, quickly and efficiently. This will make sure patient medical information is available to clinicians when and where they need it, improving patient care.

The GP Connect programme is supporting the development of products which will enable different systems to communicate. In the first instance, HCV will be using GP Connect to:

1) Enable NHS 111 (Yorkshire Ambulance Service) to book direct appointments with GP Practices and GP Record Access for Urgent Care Clinicians in NHS111 in read-only format
2) Enable appointment booking and record sharing between GP practices within Primary Care Networks (PCNs).

More information and videos can be found at: https://digital.nhs.uk/services/gp-connect

Why are we doing this?

It will improve patient care. Clinicians with NHS 111 will have up-to-date clinical information about patients. Currently when finishing a call to NHS 111, patients need to contact their practice to make an appointment if required. Instead, using Appointment Management they can be booked immediately into an appointment by NHS 111.

Making appointments available to NHS 111 is a national contractual requirement in the 2019/2020 GP Contract. This system will help meet this contractual requirement.

https://www.england.nhs.uk/wp-content/uploads/2019/05/19-20-gms-contract-guidance-audit-requirements.pdf

It will also improve clinical experience. By being able to view a patient's record, clinicians in NHS 111 can make a better decision about patient need, resulting in more appropriate action and referrals.

Why the need for a DPIA was identified?

The need for a DPIA was identified because it involves a new electronic method of booking appointments and sharing patient information for direct care to update existing methods that are based on telephone and paper-based information sharing.

Step Two: Describe the information flows

You should describe the collection, use and deletion of personal data here and it may also be useful to refer to a flow diagram or another way of explaining data flows. You should also say how many individuals are likely to be affected by the project.

GP Connect is a national technology solution, delivered through NHS Digital (NHSD) that allows health and care organisations and authorised clinical staff to share and view GP practice clinical information as well as the direct booking of GP appointments from NHS 111, to improve patient care.

The GP Connect programme is supporting the development of capabilities which will enable the different systems to communicate, so that clinicians in different care settings can access patient data for the purposes of direct care and organisations can have access to book appointments at GP practices.

- **Access Record:**
    - HTML view – a static view, similar to a screen shot, sometimes referred to as 'HTML view'
    - Access to a webpage view of a GP Patient record. This view includes a detailed summary view of the record, as well as additional information about allergies, encounters, medications, observations, problems and procedures
    - This supports hub working by enabling the detailed patient record to be shared regardless of GP system used
    - Other care settings can also access information where agreements are in place.
- **Appointments Management** (Phase 1 for HCV, to be rolled-out by 31 March 2020):
    - Gives the ability to view, book, cancel and amend appointments between different GP Systems.
    - The GP Practice can choose which slots and type of slots are available for booking by different organisations
- **Access Record:**
    - Structured data (medications and allergies data) – Access to structured Medications and Allergies information from the GP Patient Record that can be imported into a different clinical system.
    - Medications and allergies are being prioritised as the most valuable information for the majority of clinical interactions
    - Additional structured information will be added over time.
- **Writeback**:
    - Systems can automatically send a consultation summary back to the patient's registered practice in the form of a PDF document, detailing the consultation and actions taken

Data Items Shared

For appointment booking functionality: patient name and demographic details. The GP Connect solution will surface appointment slots that GP practices have configured to be available to the consuming organisation.

For Record Access: a view of the GP Practice clinical record in read-only format, including information about allergies, encounters, medications, observations, problems and procedures.

Who Will Be Able To View Data?

Data will be available to appropriate staff within each organisation controlled by each organisations access policy.

- NHS 111 Call handlers from or other administrative staff will not be able to view a patient's record but will be able to book appointments where appropriate
- GP Record Access is only enabled for the clinician role within the Integrated Urgent Care Service – NHS 111.
- At a GP Practice level necessary patient-level data will only be accessible to authorised clinicians and administrative staff with a justified purpose.

Technical Overview of the GP Connect service

GP Connect services can be accessed by an authorised NHS clinician (or administrator) via their clinical system, when it is required to support the direct care of that patient.
GP Connect enables 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. GP Connect also 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 GP Connect Service utilises two main Spine components to securely transfer messages between clinical systems:

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

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

Data Flow Diagrams

The topography diagram (figure 1) below shows the flow of messages when the SSP is utilised for transferring requests for patient record and appointments information. The flow 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 consumer system then uses 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,
- 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) will receive the request and return the appropriate information via the Spine Secure Proxy to the Consumer system.

Whilst NHS Digital is delivering the GP Connect 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 GP Connect are the Provider and Consumer Systems.

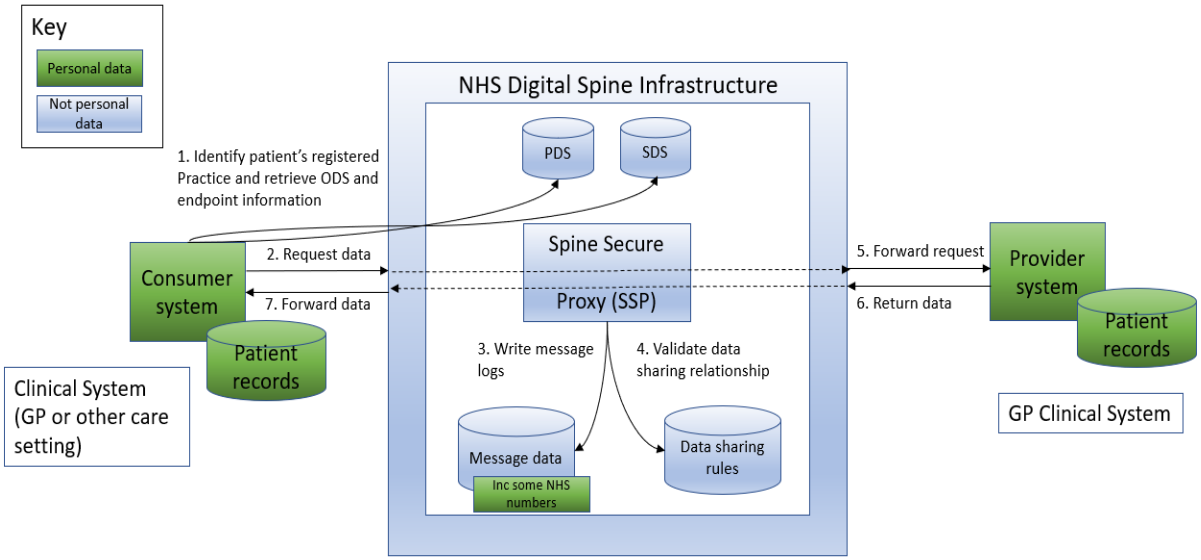

Figure 1 – Technical Architecture of the GP Connect Service using the SSP (HTML, Structured and Appointment Management capabilities)

The second topography diagram (figure 2) below shows the flow of messages when MESH is used to transfer messages back to a patient's registered GP practice. The flow can be described as follows:

- A clinician completes a consultation with a patient and writes a summary of the consultation to send to the patient's registered practice which results in a message being constructed, which includes a PDF describing the consultation,
- The MESH client at the federated practice sends the message to the MESH server where it awaits collection by the registered practice,
- The MESH client at the registered practice collects the message from the MESH server and makes it available to other registered practice system components for onward processing
- The message is processed at the registered practice, 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, and then a business acknowledgement will then be sent once the message has been processed by the receiving practice.

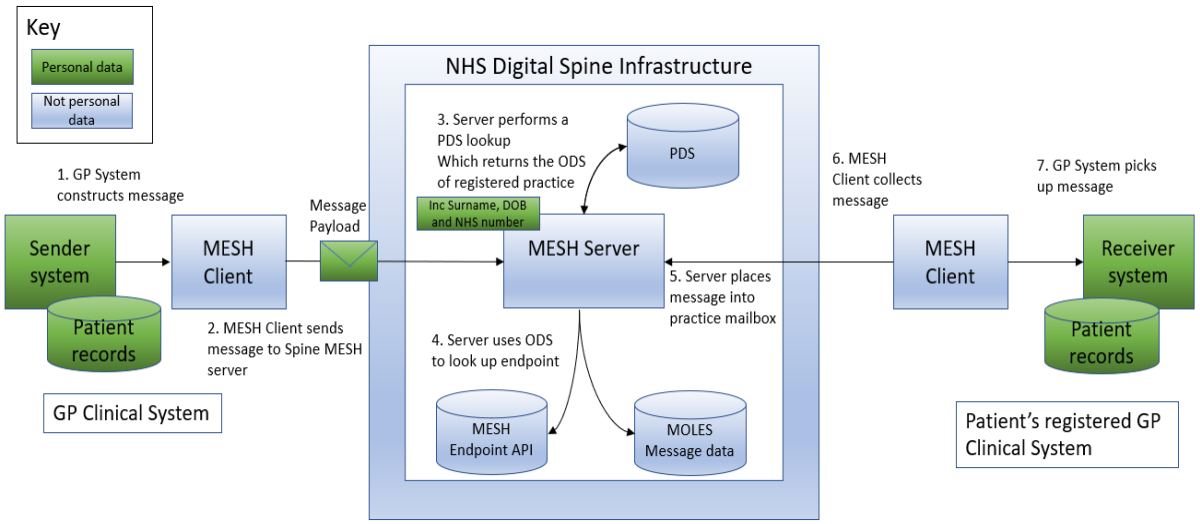

Figure 2 – Technical Architecture of the GP Connect Service using MESH (Messaging capability) note that MOLES is the audit data repository of MESH

Data Retention

No data is retained on the GP Connect technology architecture. Data will be retained by GP practices and NHS111 (YAS) in accordance with the Records Management Code of Practice for Health and Social Care 2016.

Consultation Requirements

Explain what practical steps you will take to ensure that you identify and address privacy risks. Who should be consulted, internally and externally? How will you carry out the consultation? You should link this to the relevant stages of your project management process.

You can use consultation at any stage of the DPIA process.

The GP Connect solution is a national system delivered and technically assured by NHS Digital. The Humber, Coast and Vale Digital Team have established a project team that includes NHS Digital representation. We have worked with a representative from eMBED (IG service provision in HCV) and a DPO from one of the HCV CCGs (North East Lincolnshire) to review and assess any privacy risks and to develop an Information Governance approach for the roll-out of GP Connect. NHS Digital has also been involved in this process and has approved the IG approach proposed. The IG approach, including this DPIA and the GP Connect Information Sharing Statement, have been shared with the DPOs of the six HCV CCGs for feedback and approval.

Step Three: identify the privacy and related risks

Definition of personal data:

Data which relate to a living individual who can be identified –

(a) from those data, or
(b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller.

Definition of special categories of personal data:

Personal data consisting of information as to -

(a) the racial or ethnic origin of the data subject,
(b) their political opinions,
(c) their religious beliefs or other beliefs of a similar nature,
(d) whether they are a member of a trade union,
(e) their physical or mental health or condition,
(f) their sexual life and orientation,
(g) genetic data,
(h) Biometric data which can be used to identify an individual,
(i) the commission or alleged commission by them of any offence, or,
(j) any proceedings for any offence committed or alleged to have been committed by them, the disposal of such proceedings or the sentence of any court in such proceedings,

Identify the key privacy risks and the associated compliance and corporate risks. Larger scale DPIA's might record this information on the Trusts formal risk register.

The 7 Data Protection Principles:

Principle 1: Lawfulness, Fairness and Transparency

Personal Data shall be processed lawfully, fairly and in a transparent manner in relation to the Data Subject. This means, the organisation must tell the Data Subject what Processing will occur (transparency), the Processing must match the description given to the Data Subject (fairness), and it must be for one of the purposes specified in the applicable Data Protection regulation (lawfulness).

Privacy issue	Comments
Have you identified the purpose of the project?	Yes

Is there a lawful reason you can carry out this project?	Yes - Direct care purposes For the processing of personal data: Article 6.1 (e) of GDPR: processing is necessary for the performance of a task carried out in the public interest or in exercise of official authority vested in the controller. For the processing of 'Special Category Data': Article 9.2 (h) of the 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 system and services.
How will you tell individuals about the use of their personal data?	Each participating organisation, including GP practices and Yorkshire Ambulance Service (NHS111 provider) are required to have a Privacy Notice published on their website which outlines how they use and share patient information with other health and care organisations to deliver direct care. The HCV Digital Team will conduct a check of all websites to ensure that these Privacy Notices are in place and will liaise with any organisations where these are not in place to ensure that the requirement is met.
If you are relying on consent to process personal data, how will this be collected and what will you do if it is withheld or withdrawn?	N/A
Will your actions interfere with the right to privacy under Article 8 of the Human Rights Act? If yes, is it necessary and proportionate?	No

Principle 2: Purpose Limitation

Personal Data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. This means the organisation must specify exactly what the Personal Data collected will be used for and limit the Processing of that Personal Data to only what is necessary to meet the specified purpose.

Privacy issue	Comments
Does your project plan cover all of the purposes for processing personal data?	Yes

Which personal data could you not use, without compromising the needs of the project?	All information accessible through GP Connect is necessary for the provision of direct care.

Principle 3: Data Minimisation

Personal Data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. This means the organisation must not store any Personal Data beyond what is strictly required.

Privacy issue	Comments
Is the quality of the information good enough for the purposes it is used?	Yes
Which personal data could you not use, without compromising the needs of the project?	Only information that is strictly relevant to the delivery of direct care will be shared.

Principle 4: Accuracy

Personal Data shall be accurate and, where necessary, kept up to date. This means the organisation must have in place processes for identifying and addressing out-of-date, incorrect and redundant Personal Data.

Privacy issue	Comments
If you are procuring new software does it allow you to amend and / or delete data when necessary?	Yes.
How are you ensuring that personal data obtained from individuals or other organisations is accurate?	Each health and care provider is responsible for the quality and accuracy of data in their own clinical systems.

Principle 5: Storage Limitation

Personal Data shall be kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Data is processed. This means the organisation must, wherever possible, store Personal Data in a way that limits or prevents identification of the Data Subject.

Privacy issue	Comments
What retention periods are suitable for the personal data you will be processing? How long will you keep the data for?	Data is not retained within the GP Connect solution. Within each participating NHS organisation, data will be retained in accordance with the Records Management Code of Practice for Health and Social Care 2016.

Are you procuring software that will allow you to delete information in line with your retention periods?	No – the GP Connect solution does not retain data.

Principle 6: Integrity & Confidentiality

Personal Data shall be processed in a manner that ensures appropriate security of the Personal Data, including protection against unauthorised or unlawful processing, and against accidental loss, destruction or damage. The organisation must use appropriate technical and organisational measures to ensure the integrity and confidentiality of Personal Data is maintained at all times.

Privacy issue	Comments
Do any new systems provide protection against the security risks you have identified?	Yes. GP Connect is a national solution delivered and assured by NHS Digital.
What training and instructions are necessary to ensure that staff know how to operate a new system securely?	Full training materials have been created by NHS Digital for national use. These will be shared with all participating organisations and training will be delivered by NHS Digital and the HCV Digital Team.
What training on data protection and / or information sharing has been undertaken by relevant staff?	All staff will undertake standard NHS Digital Information Security training or equivalent. All staff MUST be appropriately trained as per the Data Security & Protection Toolkit.
What process is in place to answer 'Subject Access Requests' (requests for personal data)?	The organisation the request is made to will respond in line with their procedures. Where it impacts on other data controllers, reasonable efforts will be made prior to disclosure. Where necessary data subjects will be signposted to the appropriate organisation.
Will the project require you to transfer data outside of the EEA? If yes how does it demonstrate an adequate level of protection?	No
If you will be making transfers outside of the EEA, how will you ensure that the data is transferred securely?	N/A

Principle 7: Accountability

The Data Controller shall be responsible for and be able to demonstrate compliance with the data protection principles. This means the organisation must demonstrate that the six Data Protection Principles (outlined above) are met for all Personal Data for which it is responsible.

Privacy issue	Comments

Are Data Protection contracts / Information Sharing Agreements in place with all 3rd parties who will be acting as Data Processors?	No. NHS Digital requires GP Practices to have been informed about what information will be shared using GP Connect and to provide an outline of the method for sharing information. We have produced an **GP Information Sharing Statement** for each GP Connect Use Case which will be sent to all GP Practices and Yorkshire Ambulance Service. This Statement outlines the purpose for sharing, the data being shared and the method for sharing and will be approved by NHS Digital and the Data Protection Officers for the six Humber, Coast and Vale CCGs before it is sent to participating organisations. When GP Practices configure their Practice's clinical system to enable the data sharing through GP Connect, this will be taken as agreement to the terms of the **GP Connect Information Sharing Statement**.

Step Four: Identify privacy solutions

Describe the actions you could take to reduce the risks, and any future steps which would be necessary (e.g. the production of new guidance or future security testing for systems).

Risk	Solution	**Result:** is the risk eliminated, reduced, or accepted?	**Evaluation:** is the final impact on individuals after implementing each solution a justified, compliant and proportionate response to the aims of the project?
Fair Processing Requirements – lack of transparency and therefore non-compliance to GDPR/DPA 18	Ensure that all practices in HCV and YAS have an appropriate PN in place that outlines how patient information is shared with other health and care provides for Direct Care Purposes	Reduced	The impact is a justified, compliant and proportionate response to the aims of the project.
Data sharing with new organisations and adherence to the Sharing Statement without an ISA	Communications to participating organisations will stipulate that by configuring and switching on GP Connect they are adhering to the Information Sharing Statement. A Positive Action must be taken to start using GP Connect	Reduced	The impact is a justified, compliant and proportionate response to the aims of the project.

Step Five: Sign off and record the DPIA outcomes

Who has approved the privacy risks involved in the project? What solutions need to be implemented?

Risk	Approved Solution	Approved By
The risks are as detailed in step 4	Someone to be delegated with the responsibility of obtaining assurance that GP Practices, YAS and NHS 111 have completed privacy notices to reflect this use of information	Laura Whitton IG Lead
Who is to check GP Practices, YAS and NHS 111 have completed a Data Security and Protection Toolkits	Someone to be delegated with the responsibility of checking organisations complete their Data Security and Protection Toolkits	Laura Whitton IG Lead
Data sharing with new organisations and adherence to the Sharing Statement without an ISA	Someone to be delegated with the responsibility of checking adherence to this Information sharing statement	Laura Whitton IG Lead

Step Six: Integrate the DPIA outcomes back into the project plan

Who is responsible for integrating the DPIA outcomes back into the project plan and updating any project management paperwork? Who is responsible for implementing the solutions that have been approved? Who is the contact for any privacy concerns that may arise in the future?

Action to be taken	Date for completion of actions	Responsibility for action
		Tara Athanasiou

Contact point for future privacy concerns
The initial point of contact for any privacy concerns is: hnf-tr.yhcrhcv.carerecord@nhs.net. This will be escalated as necessary to the Information Governance lead of the respective CCG.

For further information or guidance, see the ICO's website at http://www.ico.gov.uk

Information Governance Risk Assessment of DPIA
Project : HCV

CCG: North East Lincolnshire

	Risk	Main Risk Sources	Main Threats	Main Potential Impacts	Main Controls Reducing the Severity and Likelihood	Severity	Action
1	How is the public to be informed of this access to their GP record and ensure practices sign up to the information sharing statement	The processing organisation not processing information fairly and lawfully	The processing organisation not processing information fairly and lawfully	• The public not understanding how their information is used	Gp Practices and NHS11/YAS to add a statement to their privacy notice in relation to access to and use of this information	minor	Checked by Project Lead
2	The legal basis is recorded incorrectly, it should be Public Task, and Medical Related.	Processing information unlawfully	Legal challenge over information processing	Legal challenge over information processing	Requires correction on the DPIA	minor	Completed
3	responsible for checking continued completion of Data Security and Protection Toolkit	The processing organisation not processing information securely, fairly and lawfully	The processing organisation not processing information, securely, fairly and lawfully	Breaches of information being processed	NHS England check these are completed annually	minor	N/A

IG review completed by: Dr Mark Culling **Review date:** 13.02.20
Date complete and risk assessed: 13.02.20 **Consultation with ICO required?** **No**

Section 4: Review and Approval

Assessment completed by

Name:	Dr Mark Culling
Title:	Senior Information Governance Specialist
Date:	13.02.20

Data Protection Officer Approval

Name:	Paul Ellis
Title:	Data Protection Officer (NEL CCG)
DPO advice: DPO should advise on compliance, risks identified and whether processing can proceed. If accepting any residual high risk, consult the ICO before going ahead	There is a clear lawful basis for the sharing of information for the purpose of direct care (public task 6 1 e / provision health and social care 92 h). Clear arrangements are in place to ensure access to information is controlled. I would recommend that the CCG approve the approach set out for the use of GP Connect, on the understanding that this doesn't extend to GP Practices who will be responsible signing up independently, approving the IG governance (Information Sharing Agreement / Data Protection Impact Assessment) and that by configuring their systems to use GP Connect they are agreeing to adhere to the standards outlined.
Approved	☒
Date:	14/02/2020

The DPO should also review ongoing compliance with DPIA

SIRO/Caldicott Guardian Approval

Name:	Jan Haxby
Title:	
DPO advice accepted or overruled: If overruled, you must explain your reasons	DPO advice accepted and happy to proceed. Can we assure ourselves on the last point raised by Paul that GP practices are able to adhere to the standards required – can this be built into future audit planning?.
Approved:	☒
Date:	28.02.2020

This DPIA will be kept under review by:	Business Change Lead