Gosford Hill Medical Centre
167 Oxford Road
Kidlington
OXON

DATA PROTECTION IMPACT ASSESSMENT (DPIA)

DPIA Screening Questions

Will the processing involve 'personal data'[2] (i.e. any information relating to an identified or identifiable individual, the data subject)?	Y
Will the processing involve 'personal data' as well as 'special category of data'? (E.g. information about an individual's: race, ethnic origin, health, sexual orientation etc.) ICO website: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/	Y
Will the processing involve personal data and special category data on a large scale? (Should consider the number of individuals concerned, the volume of data, the variety of data, duration of processing, the geographical extent etc.) ICO website: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/when-do-we-need-to-do-a-dpia/	N
Will the project involve the use of cutting edge new technologies? (E.g. includes the innovative application of existing technologies to process data in new ways or for new purposes, using technology in novel and unexpected ways, using technologies that are not tried and tested elsewhere, application of artificial intelligence or machine learning, etc.) . ICO website: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/when-do-we-need-to-do-a-dpia/	Y
Is there the risk that the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy (e.g. health records), unauthorised reversal of pseudonymisation[1], or any other significant economic or social disadvantage?	Y
Is there the risk that data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data?	N
Will there be processing of biometric or genetic data, or data concerning sex life that identifies individuals?	Y
Are the data to be processed revealing racial or ethnic origin, political opinions, religion or philosophical beliefs, or trade union membership?	N
Will there be processing of data concerning criminal convictions and offences or related security	N

[1] '**pseudonymisation**' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

2 '**personal data'** means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

measures?	
Will personal data of vulnerable natural persons, in particular of children, be processed?	Y
Will the processing involve the use of systematic and extensive profiling or automated decision-making to make decisions about people in particular analysing or predicting aspects concerning**:** performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, and location and movements.	N
Will the processing involve combining, comparing or matching of personal data from multiple sources? `	N
Will the project include a systematic and extensive evaluation of personal aspects relating to natural personal which is based on automated processing, including profiling and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person (e.g. a recruitment aptitude test which uses pre-programmed algorithms and criteria)?	N
Will it systematically monitor a publicly accessible area on a large scale (e.g. CCTV)?	N

If 'Y' to any questions – proceed to complete DPIA template below

DATA PROTECTION IMPACT ASSESSMENT (DPIA) template V.2.1

Project title	Referral Navigation
Date DPIA started	14/6/19
DPIA prepared by (project lead with email address)	Paul Kettle, paul.kettle1@nhs.net

1. DESCRIPTION OF PROCESSING

1.1 Summarise the project or change, including the benefits (*helpful to refer to/link to other documents such as project proposal/initiation document*)

This is a pilot (project) of an electronic referral system.

We expect 20 GP practices will pilot the system. The criteria for referral will not change as a result of this pilot but existing referral criteria will consistently be more closely followed and GPs prompted to seek advice and guidance where referral is not recommended.

Because it should take less time and be easier than current referral administration we expect GPs will complete the process in clinic while the patient is with them, giving patients opportunity to comment on the choice of clinic site/provider and potentially the date.

The key data change relates to how the system (Rego) will interface with EMIS and eRS.

The nature and amount of referral data moving from GP to provider (e.g. OUHFT) will not change. The data will leave the GP via eRS and be received by the provider by eRS just as at present. The difference is that eRS will be populated by Rego, which in turn will be partly populated by EMIS.

NB This data will not be received at the OCCG.

1.1.1 Is there another way to achieve the same outcome without using any PID?
No, the data being used is essential and will not change during or as a result of this pilot. This data will not be received at the OCCG.

1.2. Describe exactly the data to be used, the data flows, and the retention period for the data. If this is a trial or pilot project, include the criteria, process and data that will be used for evaluating its outcome

1.2.1 List each data item, the source of that data and how the data will be received at the CCG:

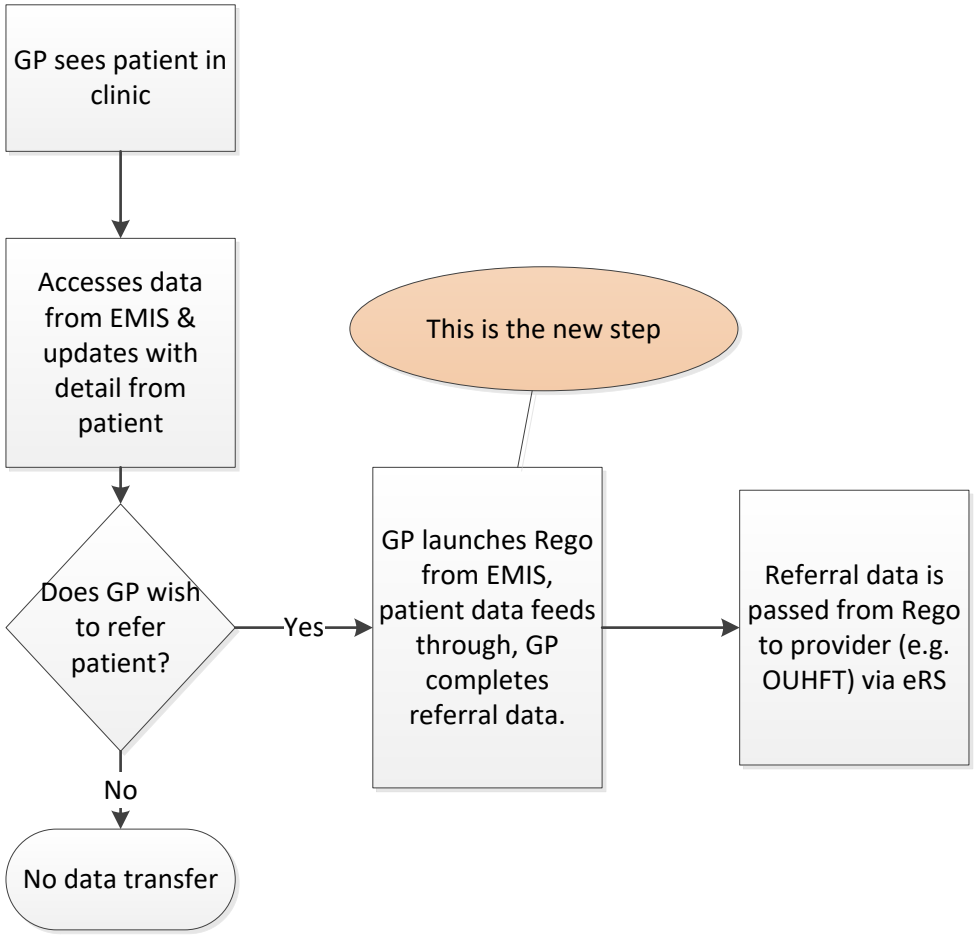
Data	Source	Method received	Retention period	Will it be shared further?
NB Data will not be received at the OCCG.	N/A	N/A	N/A	N/A

For each patient, personal data relevant to the referral	EMIS and recorded by GP during clinic			

1.2.2 If the Source for any data is NHS Digital (eg SUS) do you have NHSD permission to use the data for the proposed purpose?

N/A

1.2.3 Draw / describe the flow of data.



NB

Vantage Health is not part of the G-Cloud 11 framework. The servers used by Rego system are ISO 27001 and ITIL ISO 20000 accredited, they are hosted in the UK with Carelink. (*More*

information about Carelink can be found in their brochure (https://pikselgroup.com/carelink/wp-content/uploads/sites/6/2017/12/Piksel-Carelink-Brochure-Final.pdf) and on their website https://carelink.co.uk/services/).
Vantage Health is on the HSCN and follow the HSCN cloud compliance.

2. COMPLIANCE & PROPORTIONALITY MEASURES

2.1 What is the lawful basis for processing the personal data under GDPR/DPA 2018? (refer to IG Lead or NHS Digital guidance, particularly sections 5 and 6)

2.2 Is the project only using anonymised data?
No, but the patient data will not come to the CCG, please see data flow.

2.3 Is the project only using pseudonymised data inc NHS no?
No, but the patient data will not come to the CCG, please see data flow.

2.4 If the project is processing ***Personal*** Data – what is the legal basis:
The patient data, essential for treatment in secondary care, will be made available to clinicians as required for treatment only.

2.5 If the project is processing ***Special Category*** Data (e.g. health)- what is the legal basis:
N/A

2.6 Does any of the data include that from children or other vulnerable groups?
Yes but the patient data will not come to the CCG, please see data flow and 2.4 above.

2.7 What is the purpose of processing and what lawful ground is relied on under Common Law Duty of Confidentiality? (refer to IG lead)
Please see 2.4 above.

3.RISK ASSESSMENT AND MITIGATION MEASURES

3.1 List the relevant stakeholders who have been consulted about data protection and privacy risks (name, role)

Paul Antony [Information Governance Manager, NHS South, Central and West Commissioning Support Unit]

3.2. Describe any data protection and privacy risks identified

Describe the source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood of harm** Remote, possible or probable	**Severity of harm** Minimal, significant or severe	**Overall risk** Low, medium or high

GPs are the data owners of the patient referral data which will flow from EMIS to eRS via Rego. The introduction of Rego, which is provided by Vantage Health, may introduce risk to GP data owners in the event that Vantage Health becomes insolvent.	Remote	Minimal	Low

3.3. Describe the risk management measures agreed (what, why, who, when)**, including how they will be implemented**

3.3.1 Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in 3.2

Risk	**Options to reduce or eliminate risk**	**Effect on risk** Eliminated reduced or accepted	**Residual risk** Low, medium or high	**Measure approved** Yes/no
Data Owners	The contract that was signed by the provider (Vantage Health) and Oxfordshire CCG has been reviewed by Paul Antony, who considers it provides reassurance for GPs. However, GPs participating in the pilot will be asked to sign: • an electronic DPA acknowledgement form (Appendix 1 attached below) acknowledging Data Protection Act roles and responsibilities. • An information sharing agreement (see example in Appendix 2 below)	Accepted	Low	
Data Owners	Vantage Health confirm • They are ICO compliment • They are DSP toolkit compliant • They are not part of GPsoc	Reduced	Low	
Data Owners	Once completed, the DPIA will be shared with GP practices	Accepted	Low	

4. SIGN OFF AND RECORD OUTCOMES

4.1 Comments / Recommendations - signed by the DPO

Signed (DPO) **Date**

4.2 where requested – comments/recommendations of DPIA Panel

Signed (DPIA Panel) **Date**

4.3 Approved and signed by the SIRO (where DPO advice is overruled, note the reason)

Signed (SIRO) **Date**

APPENDIX 1

Vantage Diagnostics Limited
Integrated Care Communication Service
Data Processing Agreement (to be accepted as 'terms of use')

We have been commissioned by Oxford CCG to provide You with an Integrated Care Communication Service (ICCS). We take seriously Our commitment to safeguarding Your data as required under the Data Protection Act 1998 and General Data Protection Regulation 2018.
As part of the ICCS service We will process items of data which are considered to be Personal Data. Your role is as the Data Controller and Ours is that of the Data Processor; in effect We process Your referral data. A full description of these roles can be found at https://ico.org.uk/media/for-organisations/documents/1546/data-controllers-and-data-processors-dp-guidance.pdf.
This agreement sets out Our commitment to manage Your referral data in line with the requirements of the aforementioned Data Protection Legislation.
Please read the agreement below and click the "Accept" button at the end to confirm that You accept and agree to these terms and that You agree to comply with them.
If You do not agree to these terms, You must not use the ICCS system.
If you have any queries regarding this agreement, please contact Oxford CCG.
We recommend that You print a copy of these terms for future reference.

Definitions & Interpretation

Data Protection Legislation means the Data Protection Act 1998, General Data Protection Regulation 2018 and any other Law relating to the protection of personal data and the privacy of individuals, including where applicable guidance and codes of practice issued by the Information Commissioner, and the terms **Data Controller**, **Data Processor** and **Personal Data** shall have the same meaning as set out in the Data Protection Legislation;
ICCS means the Electronic Referral Service commissioned by OCCG;
Law means any applicable statute or proclamation or any delegated or subordinate legislation or regulation; any applicable European Union directive, regulation, decision or law; any enforceable community right within the meaning of section 2(1) European Communities Act 1972; any applicable judgment of a relevant court of law which is a binding precedent in England and Wales; requirements set by any regulatory body; and any applicable code of practice, in each case as applicable in England and Wales;
OCCG means Oxford CCG, the Commissioning Board;
Personal Data Breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed;
Staff means all persons employed or engaged by Us to perform our obligations in relation to ICCS including any subcontractors and person employed or engaged by such subcontractors;
We means Vantage Diagnostics Limited (Company number 05819429) whose registered office is at 14 David Mews, London, W1U 6EQ and **Our** and **Us** and shall be construed accordingly;
You means any sole practitioner, partnership, body corporate or other legal entity which uses the DERS or which employs or engages individuals using the DERS and Your shall be construed accordingly.

Data Controller and Processor

You acknowledge that, in relation to the Personal Data processed within ICCS:

- You are a Data Controller in respect of the Personal Data for which You (alone or jointly with other Data Controllers) determine the purposes and means of the processing;
- We are a Data Processor in respect of such personal data; and
- You, as a Data Controller, and We, as a Data Processor, are each subject to the respective obligations upon Data Controllers and Data Processors under the Data Protection Legislation.

Our Obligations

In relation to the Personal Data for which You (alone or jointly with other Data Controllers) determine the purposes and means of the processing, We agree to:

- Process such Personal Data:
  - only on documented instructions from You or another person who is a Data Controller in relation to that Personal Data;
  - only for the general purposes of managing dental referrals through ICCS;

    - for the duration of the ICCS being commissioned by OCCG

  except and to the extent We are otherwise required or permitted to process the Personal Data by Law;
- Comply with Our obligations as a Data Processor under the Data Protection Legislation;
- Implement appropriate technical and organisational measures in such a manner that the processing of Personal Data will:
    - meet the requirements of the Data Protection Legislation;
    - ensure the protection of the rights of data subjects;
    - ensure the security of processing; and
    - assist You, insofar as possible, in relation to any obligation under the Data Protection Legislation including in relation to rights of data subjects and security of processing;
- Only engage another Data Processor:
    - with Your prior written authorisation; and
    - having imposed Our obligations set out in these terms and under the Data Protection Legislation upon that other Data Processor;
- Ensure that our Staff who process such Personal Data are under an obligation of confidence and are obliged to comply with Our obligations set out in these terms and under the Data Protection Legislation;
- At Your request, delete and/or return such Personal Data to You upon ICCS being de-commissioned (except and to the extent We are otherwise required or permitted to process the Personal Data by Law);
- Make available to You all information necessary to demonstrate compliance with the obligations laid down in the Data Protection Legislation and allow for and contribute to audits, including inspections, conducted by You or another auditor mandated by You;
- Notify You immediately should We, in Our opinion, consider that an instruction issued by You infringes the Data Protection Legislation;
- Notify You without undue delay should We become aware of a Personal Data Breach.

APPENDIX 2

Information Sharing Agreement

System & Process

Name of System	Rego
Description of process	Referral is initiated by a clinician, the referral is then validated against local pathways and is sent via eRS
Purpose of the information sharing	Provide better patient care
Who is the information about? CLIENT staff, CLIENT patients, other? If "other" please provide details	Other referral information
Approximately how many people will have their information shared using this system? Eg, all Trust staff/all Trust patients/all patients in department/all patient with certain condition, etc (please provide an estimate of numbers)	All patients who have been referred
Is information being sent to CLIENT, sent from CLIENT, or both?	Both
If an existing system will be utilised, provide the name of CLIENT system information will be shared from or to	NA
Will information be sent abroad directly by CLIENT or by the 3rd party? If yes, please provide details of the country and reason	No

Trust & Third Party Contact Information

Who will the information be shared with? (Provide name of company/organisation)	Vantage Diagnostics
The ICO registration number of the 3rd party	Z9532520
Contact person and address for the 3rd party	Adiel Benayahu, 116-118 Finchley Road, London, NW3 5HT
The person responsible for this information sharing at CLIENT - please provide name, job title, department, and site	Click here to enter text.
The name and job title of the person completing this form	Adiel Benayahu, CTO

Preliminary Questions

What information will be shared? Please select **all** relevant fields.	☐ No Personal Information ✓ Name ✓ Address ✓ Postcode ✓ Date of Birth ✓ GP ☐ Consultant Name ☐ Next of Kin ✓ NHS Number ☐ Unit Number ✓ Treatment Types and Dates	✓ Gender ✓ Diagnosis ☐ Racial/Ethnic Origin ☐ Religion ☐ Occupation ☐ Political Opinion ✓ Medical History ☐ Sexual Orientation/Sex Life Information ☐ Genetic or Biometric data (ie gene sequence, fingerprints, facial recognition, retinal scanning) ☐ Other Please State
Will any information be processed about …	✓ Under 18's ☐ Under 16's	
Please select one of the following options that describes the personal information being sent;		
Identifiable ✓	The information being shared is in an identifiable format (This doesn't have to include a person's name - it's anything that can identify them as an individual including their postcode, unit number, NHS number, etc)	
Pseudonymised ☐	The information being shared has had the personal identifiable data replaced with a unique artificial identifier Where is the key to Decode the Pseudonymisation held and who has access to it? Click here to enter text. How is the Pseudonymisation code created? (ie, automatically by a system such as the Data Warehouse, or manually by a member of staff)? Click here to enter text.	
Anonymised ☐	The information being shared has been fully anonymised and can't be traced back to the patient. **As this system does not send personal identifiable data no further information about this system needs to be included in the sharing agreement.**	

Legal Reasons for Sharing

From the following list, please tick all that apply regarding the reasons **personal** information will be shared:		**Tick if applicable**	**Please provide detail to support each ticked reasons**
Personal information includes ; Name DoB Postcode	1. The data subjects have all consented to the sharing and I have written evidence of this	✓	Before a referral is submitted, the patients mush consent. Otherwise a referral cannot be sent. The Trust has a contract with NHS England. NHS England have commissioned Vantage to manage all dental referrals utilising Rego.
	2. Sharing the data is necessary for the performance of a contract the Trust has with the data subject(s)	✓	
	3. Sharing is necessary to complete a legal obligation	☐	
	4. Sharing is necessary to protect the vital interests of the data subjects or another person	☐	
	5. Sharing is necessary for the performance of a task carried out in the public interest or to exercise official authority vested in the Trust	☐	

From the following list, please tick all that apply regarding the reasons **Special Category** information will be shared:		**Tick if applicable**	**Please provide detail to support each ticked reasons**
Special Category Information includes; Racial/ethnic origin Political opinion, Religion, Health information, Sexual orientation/sex life information, Genetic or biometric data (gene sequence, fingerprints, facial recognition, retinal scanning, etc)	1.Explicit consent of the data subject has been written down, unless reliance on consent is prohibited by EU or Member State law	☐	NA
	2. Processing is necessary for carrying out obligations under employment, social security or social protection law, or a collective agreement	☐	
	3. Processing is necessary to protect the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent	☐	
	4. Processing carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without consent	☐	
	5. Processing relates to personal data manifestly made public by the data subject	☐	
	6. Processing is necessary for the establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity	☐	
	7. Processing is necessary for reasons of substantial public interest on the basis of Union or Member State law which is proportionate to the aim pursued and which contains appropriate safeguards	☐	
	8. Processing is necessary for the purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the	☐	

From the following list, please tick all that apply regarding the reasons **Special Category** information will be shared:		**Tick if applicable**	**Please provide detail to support each ticked reasons**
	basis of Union or Member State law or a contract with a health professional		
	9. Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices	☐	
	10. Processing is necessary for archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 89(1)	☐	

Sharing Activity

When does the information sharing commence?	
How long will the data sharing go on for?	
How often is the data shared?	Daily
How Long will the Third Party store Personal & Special Category data for?	Retention of information will be for as long as the contract requires. Typically 8 years.
How will the Third Party dispose of data when its no longer required?	Data will be permanently erased from the servers
Will the Third Party Share this data with other parties?	No
If yes, how will this be shared, secured and retained?	Click here to enter text.

Third Party Support & Service

If the information is being sent to how will they store the data to securely?	Information is securely stored on N3 hosted servers
Will the 3rd party provide IT support for the system/process?	Yes
Will the IT support be provided remotely or on site or both?	Both
What support do the third party provide on site?	Training
Is the IT support directly part of the 3rd party company or do they outsource this to another provider? If they outsource, who do they outsource this to and where are they based?	☐ Outsourced Support If they outsource, who do they outsource this to and where are they based?
Will the 3rd party be given VPN access? If yes, what information will they be able to access and when?	☐ VPN If yes, what information will they be able to access and when?

Sending Personal Information

	To	From	Detail	What information is being sent?
Email	☐	☐	Please provide email address; Click here to enter text.	Click here to enter text.
Fax	☐	☐	Fax Type Choose an item. Location Click here to enter text.	Click here to enter text.
System Messages (between two distinct systems)	✓	✓	How is messaging between the systems secured? Click here to enter text.	Server: Our servers are hosted on an N3 environment. Our hosting provider (carelink) is accredited to the highest level. The hosting facility incorporates the highest level of physical security. Access: N3 + username and password. Transmission: HTTPS (transmission is encrypted using SSL 256bit, nhs.net (if sending via email is required)
Post	☐	☐	☐ **Paper** Delivery Type Choose an item.	Click here to enter text.
			☐ **CD** Security Choose an item. Delivery Type Choose an item.	Click here to enter text.
			☐ **USB** Security Choose an item. Delivery Type Choose an item.	Click here to enter text.
			☐ **Courier**	Click here to enter text.

Report & Breach Notification

If the third party experience a breach which includes CLIENT data they must contact CLIENT straight away via infogovCLIENT@CLIENT.nhs.uk.**Identifiable information should not be included in the email - please await further contact once the initial email has been sent**	
If CLIENT experience a breach of data and need to contact the 3rd party, please provide details of who they should contact	infogov@referral.management

Third Party Approval

Signature	
Print Name	
Role	
Company/Organisation	
Date	

CLIENT Approval

Signature	*Dr M Wallace*
Print Name	Dr Mark Wallace
Role	GP Partner
Date	27.12.2019