

23/24-036

Data Protection Impact Assessment (DPIA)

A DPIA is designed to describe your processing and to help manage any potential harm to individuals in the use of their information. DPIAs are also important tools for demonstrating accountability, as they help you as a Controller to comply with the requirements of the Data Protection Legislation. Non-compliance with DPIA requirements can lead to fines imposed by the Information Commissioners Office (ICO); this includes not carrying out a DPIA at all, carrying out a DPIA in an incorrect way or failing to consult the ICO where required.

DPIA's are not new; the use of Privacy Impact Assessments has become common practice in the NHS and can provide evidence of compliance within the Data Security and Protection toolkit (DSPT); DPIAs build on that practice.

It is not always clear whether you should do a DPIA or not but there are a number of situations where a DPIA **should** be considered or where a DPIA is a **legal requirement**. If you can tick against the criteria below it is highly recommended that you undertake a DPIA and if you decide not to, ensure that you document the reasons for your decision.

You as Controller **MUST** carry out a DPIA where you plan to:

	Tick or leave blank
Use profiling or automated decision-making to make significant decisions about people or their access to a service, opportunity or benefit;	<input type="checkbox"/>
Process special-category data or criminal-offence data on a large scale ;	<input checked="" type="checkbox"/>
Monitor a publicly accessible place on a large scale;	<input type="checkbox"/>
Use innovative technology in combination with any of the criteria in the European guidelines;	<input checked="" type="checkbox"/>
Carry out profiling on a large scale;	<input type="checkbox"/>
Process biometric or genetic data in combination with any of the criteria in the European guidelines;	<input type="checkbox"/>
Combine, compare or match data from multiple sources;	<input type="checkbox"/>
Process personal data without providing a privacy notice directly to the individual in combination with any of the criteria in the European guidelines;	<input type="checkbox"/>
Process personal data in a way that involves tracking individuals' online or offline location or behaviour, in combination with any of the criteria in the European guidelines;	<input type="checkbox"/>
Process children's personal data for profiling or automated decision-making or for marketing purposes, or offer online services directly to them;	<input type="checkbox"/>
Process personal data that could result in a risk of physical harm in the event of a security breach.	<input checked="" type="checkbox"/>

You as Controller should **consider** carrying out a DPIA where you

	Tick or leave blank
Plan any major project involving the use of personal data;	<input checked="" type="checkbox"/>
Plan to do evaluation or scoring;	<input type="checkbox"/>
Want to use systematic monitoring;	<input type="checkbox"/>
Process sensitive data or data of a highly personal nature;	<input checked="" type="checkbox"/>
Processing data on a large scale;	<input checked="" type="checkbox"/>
Include data concerning vulnerable data subjects;	<input checked="" type="checkbox"/>
Plan to use innovative technological or organisational solutions;	<input checked="" type="checkbox"/>

A new DPIA should be carried out if you decide that there is a significant enough change to what you originally intended but it is good practice for DPIAs to be kept under review and revisited when necessary.

There is guidance to help you. Your Data Protection Officer (DPO) can be consulted before completing a DPIA in order to provide specialist advice and guidance or simply to talk things through with you.

Background Information	
Date of your DPIA:	15/07/2024
Title of the activity/processing:	Mortimer Surgery – Migration to EMIS Clinical System
Who is the person leading this work?	██████████
Who is the Lead Organisation?	Buckinghamshire, Oxfordshire and Berkshire West Integrated Care Board (BOB ICB)
Who has prepared this DPIA?	██████████ / ██████████
Who is your Data Protection Officer (DPO)?	██████████ for the BOB ICB ██████████ for GP Practices across BOB
<p>Describe what you are proposing to do: (Include as much background information as you can about why the new system/change in system/sharing of information/data processing is required).</p>	<p>Mortimer Surgery (K81027) will be adopting the EMIS Web clinical system supplied by EMIS Health.</p> <p>This existing principal clinical system in the Practice is Vision, and the supplier is In Practice Systems Limited (INPS), part of the Cegedim Group. Cegedim is withdrawing the Vision system from the market in England, and Mortimer Surgery has selected EMIS Web as the replacement. Vision will exit the market on 31 October 2024 and the practice needs to finalise the migration of all electronic patient records to the EMIS system by that exit date. (Vision will continue to be available in NHS Scotland and NHS Wales).</p> <p>Vision and EMIS Web are applications used to deliver GP services allowing clinical users such as GPs and nurses to view and add medical information to patient records. Other functionality is available, providing services such as appointment booking and diary management.</p> <p>EMIS web is a software solution for primary care organisations, containing and sharing personal and sensitive data. This data is encrypted in transit. The Data Controllers for EMIS Web are GP organisations; EMIS acts as a Data Processor.</p> <p>This DPIA outlines the plans to migrate all patient records from the Vision clinical system to the EMIS clinical system, ensuring data security and compliance with data protection regulations. The process will involve data mapping, testing of the new system with a focus on data security and functionality, controlled data transfer, and secure decommissioning of the old system.</p> <p>EMIS Web will utilise the migrated data to deliver healthcare services to patients such as appointment scheduling, prescription issuance, referrals, and communication with patients. All data will be handled according to relevant data protection regulations.</p> <p>Once the EMIS Web system goes live, EMIS will take over the processing of patient data on behalf of the GP Practice. The purpose of the processing is for the provision of healthcare to the patients. The system is used for the storing of data relating to the diagnosis and treatment of any medical condition and the</p>

	<p>recording of medical information such as testing and vaccinations.</p> <p>This offers significant advantages for both the customer and patients. By enabling access to a comprehensive view of a patient’s medical history, EMIS Web facilitates more effective, informed treatment decisions and delivery of healthcare services.</p> <p>A Data extraction with test data will take place to perform configuration work in advance of the Live Merge, test the process, and establish timings for the Live Merge. Data from the extract will be provided electronically to EMIS Web which will be encrypted prior to transmission.</p> <p>While the EMIS Web platform is a well-established solution within the NHS, its adoption by Mortimer Surgery has been necessary due to the requirement to migrate data from the soon to be decommissioned Vision clinical system. This migration from the Vision system to EMIS Web introduces potential risks to patient data privacy, which this DPIA aims to assess and mitigate.</p>
<p>Are there multiple organisations involved? (If yes – you can use this space to name them, and who their key contact for this work is).</p>	<p>BOB ICB – [REDACTED] - [REDACTED]@nhs.net & [REDACTED] [REDACTED] - [REDACTED]@nhs.net ; [REDACTED]@nhs.net Mortimer Surgery (K81027) – [REDACTED]@nhs.net EMIS - [REDACTED]@emishealth.com; [REDACTED]@emishealth.com Cegedim Vision - [REDACTED]@visionhealth.co.uk & [REDACTED]@cegedimrx.co.uk</p>
<p>Can you think of any other Key Stakeholders that should be consulted or involved in this DPIA? (If so then include the details here).</p>	<p>SCW CSU for additional service provision:</p> <ul style="list-style-type: none"> - IT Services - IG/DPO Services
<p>Detail anything similar that has been undertaken before?</p>	<p>Since the Vision Clinical System is being decommissioned, this migration will be necessary for all practices in England currently utilising Vision as their principal clinical system.</p> <p>The NHS undergoes frequent clinical system migrations, driven by both modernisation efforts and unforeseen circumstances such as a supplier exiting the market, as in this case with the Vision solution. Frequently, mergers or acquisitions within the GP environment may necessitate migrating clinical systems to a single platform.</p> <p>While this situation (Vision’s withdrawal) might be less common, the concept of migrating patient data from one EPR system to another is a well-established process within the NHS. EMIS Web GP, the replacement principal clinical system for Mortimer Surgery, is a software solution for primary care organisations, containing and sharing personal and sensitive data. It is specifically designed for GP Practices in the NHS and is widely used both in the BOB ICB associated practices, and nationally in</p>

the NHS. Many of the BOB ICB practices will have migrated from other systems to EMIS Web, with the data encrypted in transit.

1. Categories, Legal Basis, Responsibility, Processing, Confidentiality, Purpose, Collection and Use

1.1.

What data/information will be used? <small>Tick all that apply.</small>	Tick or leave blank	Complete
Personal Data	<input checked="" type="checkbox"/>	1.2
Special Categories of Personal Data	<input checked="" type="checkbox"/>	1.2 AND 1.3
Personal Confidential Data	<input checked="" type="checkbox"/>	1.2 AND 1.3 AND 1.6
Sensitive Data (usually criminal or law enforcement data)	<input type="checkbox"/>	1.2 but speak to your IG advisor first
Pseudonymised Data	<input checked="" type="checkbox"/>	1.2 and consider at what point the data is to be pseudonymised
Anonymised Data	<input checked="" type="checkbox"/>	Consider at what point the data is to be anonymised <input type="checkbox"/>
Commercially Confidential Information	<input type="checkbox"/>	Consider if a DPIA is appropriate
Other	<input checked="" type="checkbox"/>	Consider if a DPIA is appropriate

1.2.

Processing has to be lawful so identify which of the following you believe justifies what you are proposing to do and include an explanation as to why in the relevant box. You must select at least one from a – f.

Article 6 (1) of the GDPR includes the following:	
a) THE DATA SUBJECT HAS GIVEN CONSENT	Tick or leave blank <input type="checkbox"/>
Why are you relying on consent from the data subject? Click here to enter text.	
What is the process for obtaining and recording consent from the Data Subject? (How, where, when, by whom). Click here to enter text.	
Describe how your consent form is compliant with the Data Protection requirements? (There is a checklist that can be used to assess this). Click here to enter text.	
b) IT IS NECESSARY FOR THE PERFORMANCE OF A CONTRACT TO WHICH THE DATA SUBJECT IS PARTY	Tick or leave blank <input type="checkbox"/>
(The contract needs to be between the Controller and the individual and not concern data being processed due to someone else having a contract with the Controller. Processing can happen before the contract is entered into e.g. processing a pre-health assessment for a private or cosmetic procedure that is a paid for service with the delivery of that care done under contract between the Patient and the Practitioner).	
What contract is being referred to? Click here to enter text.	
c) IT IS NECESSARY UNDER A LEGAL OBLIGATION TO WHICH THE CONTROLLER IS SUBJECT	Tick or leave blank <input type="checkbox"/>
(A legal obligation mandates processing of data as a task in itself where there are likely to be legal measures available if not adhered to e.g. an Employer has a legal obligation to disclose salary information to HMRC).	

Identify the legislation or legal obligation you believe requires you to undertake this processing. Click here to enter text.	
d) IT IS NECESSARY TO PROTECT THE VITAL INTERESTS OF THE DATA SUBJECT OR ANOTHER NATURAL PERSON (This will apply only when you need to process data to protect someone's life. It must be necessary and does not only relate to the individual whose data is being processed. It can also apply to protect another person's life. Emergency Care is likely to fall into this category but planned care would not. You may need to process a Parent's data to protect the life of a child. The individual concerned is unlikely to be able to provide consent physically or legally; if you are able to gain consent then this legal basis will not apply).	Tick or leave blank <input type="checkbox"/>
How will you protect the vital interests of the data subject or another natural person by undertaking this activity? TBC	
e) IT IS NECESSARY FOR THE PERFORMANCE OF A TASK CARRIED OUT IN THE PUBLIC INTEREST OR UNDER OFFICIAL AUTHORITY VESTED IN THE CONTROLLER (This is different to 6 c). If you are processing data using this basis for its lawfulness then you should be able to identify a specific task, function or power that is set out in law. The processing must be necessary, if not then this basis does not apply)	Tick or leave blank <input checked="" type="checkbox"/>
What statutory power or duty does the Controller derive their official authority from? The ICB is established by order of NHS England under powers in the Health & Social Care Act 2022 sec 13 (2b i) with a general function for primary medical services in England	
f) IT IS NECESSARY FOR THE LEGITIMATE INTERESTS OF THE CONTROLLER OR THIRD PARTY (Public authorities can only rely on legitimate interests if they are processing for a legitimate reason other than performing their tasks as a public authority. See the guidance for more information about the legitimate interest test).	Tick or leave blank <input type="checkbox"/>
What are the legitimate interests you have? Click here to enter text.	

Article 9 (2) conditions are as follows:	
a) THE DATA SUBJECT HAS GIVEN EXPLICIT CONSENT (Requirements for consent are the same as those detailed above in section 1.2, a))	Tick or leave blank <input type="checkbox"/>
b) FOR THE PURPOSES OF EMPLOYMENT, SOCIAL SECURITY OR SOCIAL PROTECTION (Schedule 1, part 1 of the Data Protection Act 2018 gives more detail on when this can apply to processing and further guidance is available).	Tick or leave blank <input type="checkbox"/>
c) IT IS NECESSARY TO PROTECT THE VITAL INTERESTS OF THE DATA SUBJECT OR ANOTHER NATURAL PERSON WHERE THEY ARE PHYSICALLY OR LEGALLY INCAPABLE OF GIVING CONSENT (Requirements for this are the same as those detailed above in section 1.2, d))	Tick or leave blank <input type="checkbox"/>
d) It is necessary for the operations of a not-for-profit organisation such as political, philosophical, trade union and religious body in relation to its members	NA
e) The data has been made public by the data subject	NA
f) For legal claims or courts operating in their judicial category	NA
g) SUBSTANTIAL PUBLIC INTEREST (Schedule 1, part 2 of the Data Protection Act 2018 gives more detail on when this can apply to processing and further guidance is available).	Tick or leave blank <input type="checkbox"/>

<p>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 ON THE BASIS OF UNION OR MEMBER STATE LAW OR PURSUANT TO CONTRACT WITH A HEALTH PROFESSIONAL AND SUBJECT TO CONDITIONS AND SAFEGUARDS</p> <p>(Schedule 1, part 1 of the Data Protection Act 2018 gives more detail on when this can apply to processing and further guidance is available).</p>	<p>Tick or leave blank</p> <p style="text-align: center;">✓</p>
<p>i) 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 QUALITY AND SAFETY OF HEALTH CARE AND OF MEDICINAL PRODUCTS OR MEDICAL DEVICES, ON THE BASIS OF UNION OR MEMBER STATE LAW WHICH PROVIDES FOR SUITABLE AND SPECIFIC MEASURES TO SAFEGUARD THE RIGHTS AND FREEDOMS OF THE DATA SUBJECT, IN PARTICULAR PROFESSIONAL SECRECY</p> <p>(Schedule 1, part 1 of the Data Protection Act 2018 gives more detail on when this can apply to processing and further guidance is available).</p>	<p>Tick or leave blank</p> <p style="text-align: center;"><input type="checkbox"/></p>
<p>j) PROCESSING IS NECESSARY FOR ARCHIVING PURPOSES IN THE PUBLIC INTEREST, SCIENTIFIC OR HISTORICAL RESEARCH PURPOSES OR STATISTICAL PURPOSES IN ACCORDANCE WITH <u>ARTICLE 89(1)</u> BASED ON UNION OR MEMBER STATE LAW WHICH SHALL BE PROPORTIONATE TO THE AIM PURSUED, RESPECT THE ESSENCE OF THE RIGHT TO DATA PROTECTION AND PROVIDE FOR SUITABLE AND SPECIFIC MEASURES TO SAFEGUARD THE FUNDAMENTAL RIGHTS AND THE INTERESTS OF THE DATA SUBJECT.</p> <p>(Schedule 1, part 1 of the Data Protection Act 2018 gives more detail on when this can apply to processing and further guidance is available).</p>	<p>Tick or leave blank</p> <p style="text-align: center;"><input type="checkbox"/></p>

1.3.

If using special categories of personal data, a condition for processing under Article 9 of the GDPR must be satisfied in addition to a condition under Article 6. You must select at least 1 from a) to c) or g) to i). NOTE: d), e) and f) are not applicable

1.4.

Confirm who the Controller and Processor is/are. Confirm if the Controller/s are solely or jointly responsible for any data processed?

(Identify any other parties who will be included in the agreements and who will have involvement/share responsibility for the data/information involved in this project/activity. Use this space to detail this but you may need to ask your DPO to assist you. Copy and paste the last empty row in the table to add organisations where required (the text has been left unlocked for this purpose on that row only).

Name of Organisation	Role
Egton – (EMIS Web)	Processor
Cegedim – (Vision)	Processor
BOB ICB	Other
Mortimer Surgery (K81027)	Sole Controller

1.5.

Describe exactly what is being processed, why you want to process it and who will do any of the processing?

The data being processed is the electronic patient records for Mortimer Surgery (K81027). The data will be transferred from the Vision Clinical System to another clinical system, EMIS Web GP. This migration is essential given that Vision is exiting the market.

The initial data extraction and processing is necessary for the following purposes:

- Extracting relevant patient data from Vision in a format compatible with EMIS Web.

- Potentially transforming the data structure or format to fit EMIS Web requirements.
- Uploading the extracted and transformed data into EMIS Web.
- Verifying the completeness and accuracy of the transferred data in EMIS Web.

Following the completion of data collection and verification the data will be migrated to EMIS Web GP, and Vision will cease being the principal clinical system for Mortimer Surgery and the Practice will transition to live use of EMIS Web for processing of patient data.

Once EMIS Web GP is live, the data is collected directly from the data subject during consultations and interactions, such as the booking of appointments. This data will be used for the purposes of provision of healthcare, although the exact use of the data is determined by the Data Controller.

The system processes a range of datasets as EMIS Web stores the full patient record, including:

- Full name
- Date of birth
- Address and postcode
- Email address
- Telephone number
- NHS number
- Full health record, including prescriptions, diagnosis, test results, vaccination information, clinical studies, appointment details, consultation records, nationality.

All patient records, including deceased records, will be transferred from Vision and into EMIS, regardless of registration status in Vision. The only exception to this is where a patient is marked as deleted in Vision. Home, work, mobile telephone numbers and email addresses are transferred where recorded.

1.6.

Tick here if you owe a duty of confidentiality to any information. ✓

If so, specify what types of information. (e.g. clinical records, occupational health details, payroll information)

Patients Clinical Health Records

Patient information may include demographics like name, date of birth, contact details (email and phone number), and medical history (NHS number, health conditions, medications, etc.), and any other information which may be provided when relevant to care, e.g. family life, occupation status, and religious or other beliefs.

BOB ICB is committed to protecting the confidentiality of patient information throughout the migration process from, and in any future use of EMIS Web. The ICB adheres to the principles of the UK GDPR including the right of individuals to privacy and the requirement for data to be processed in a lawful, fair and transparent manner. The commitment also aligns with BOB ICB's obligations under the NHS Data Security and Protection Toolkit. The ICB's confidentiality policies define the circumstances and methods by which users can access patient records.

If patient data is shared with other healthcare providers during or after migration, this will be done securely and in accordance with patient consent or legal authorisation. Data sharing agreements will be established with all third-party recipients, outlining specific data security obligations.

To safeguard patient confidentiality during migration, the following measures will be implemented:

- **Secure Data Transfer:** Patient data will be transferred between systems using secure protocols with encryption.

- **Access Controls:** Access to patient data during migration will be strictly limited to authorised personnel with appropriate access permissions within both Vision and EMIS Web.

Additionally, all staff involved in the migration will have received training on patient data confidentiality and security protocols.

By implementing these safeguards, we aim to minimise the risk of unauthorised access or disclosure of patient data.

1.7.

How are you satisfying the common law duty of confidentiality?

Consent - Implied

If you have selected an option which asks for further information please enter it here

Implied consent is assumed in direct care when patients share information with the expectation that it will be used for their healthcare.

Both Cegedim (Vision) and EMIS are NHS Approved Clinical Systems Suppliers on the NHSE Digital Framework and patient data will be transferred in accordance with approved processes to ensure that the data remains secure at all stages of the transfer and is only accessed by authorised practice or supplier personnel.

1.8.

Are you applying any anonymisation/pseudonymisation technique or encryption to any of the data to preserve the confidentiality of any information?

Yes

If you are then describe what you are doing.

It may be necessary to utilise anonymised or pseudonymised data for research purposes for example to study disease patterns and effective treatments or develop new healthcare approaches. This data includes information on diagnoses, procedures, medications, and demographics but with identities such as names and addresses removed.

NHSE may use anonymised data for instance to understand population health needs and allocate resources and funding appropriately. This could involve analysing data on hospital admissions, or diseases prevalent in different areas.

Commissioners may also use anonymised data for performance monitoring, for example waiting times for GP appointments, and patient satisfaction.

The data is collected directly from the data subject during the course of consultations and interactions, such as the booking of appointments. This data will be used for the purposes of provision of healthcare, although the exact use of the data is determined by the Data Controller.

Data is encrypted in transit. Data held is protected by domain access control, anti-virus, and anti-malware products. Data is synchronously copied across both data centres and all data files are backed up and encrypted at rest to AES-256 standard and the appliances are FIPS 140-2 validated. All sensitive data is held in secure data centres. Encrypted backups are stored off site in a secure location.

If you don't know then please find this information out as there are potential privacy implications with the processing.

1.9.

Tick here if you are intending to use any information for a purpose that isn't considered as direct patient care. ✓

If so describe that purpose.

EMIS Web includes reporting functionality that could be used for both direct patient care as well as the production of management information, such as appointment book data, service planning, statistic trends, number of patients registered, etc.

1.10.

Approximately how many people will be the subject of the processing?

Unknown - specific patient cohort

1.11.

How are you collecting the data? (e.g. verbal, electronic, paper (if you need to add more selections then copy the last 'choose an item' and paste, the text has been left unlocked for you to do this.)

Electronic form

By e-mail

By telephone

Face to face - in person

If you have selected 'other method not listed' describe what that method is.

Collecting the data from patients for the EMIS Web GP Clinical system will be collected electronically or by email, telephone, and captured during face-to-face meetings with patients.

All data migrating from the Vision to the new EMIS system will be transferred electronically between the clinical systems by secure file transfer. Full details of the data collected for both EMIS and Vision is set out at Section 2.2 of this DPIA and covers:

- Patient demographic information.
- All historical clinical information on the patient record including clinical diagnoses, lifestyle and social care information and medication.
- Appointments data.

1.12.

How will you edit the data?

Once the data has been transferred into EMIS Web, it will be amended by clinicians in the same way as with Vision prior to the transition; by authorised users with the appropriate RBAC.

1.13.

How will you quality check the data?

For the migration, Vision have provided a Guidance document giving an overview of the migration process utilised by them in the migration of data. The guidance sets out roles and responsibilities involved to understand all requirements are met and the data received is what is expected to be transferred, and in the format required.

That guidance is here:



CHS Vision Data
Merges Splits Migrati

EMIS have issued a guide for the practice outlining the process of transferring data from Vision to EMIS Web and outlines potential issues that may be encountered during the migration:



Once the migration is complete and usage of the EMIS Web clinical system starts, ongoing data quality measures will be implemented. The patient submits their data and it is the data controller’s responsibility to ensure the data matches the patient record.

The system also uses data validation to ensure entries fit the required format. Entries not conforming will be flagged for correction.

EMIS also have additional quality measures in place that will be used to monitor quality:

- PR5463 MD Software Risk Management
- PR1936 Management Review
- PR1846 Internal and External Auditing Process. – Adherence to processes described in this document is internally audited.
- IF5517 Complaints Process Group Support Customer Service Team
- Service Review Meetings – Continuous review of service
- IF5426 Group Support Customer Satisfaction Policy - To ensure products provide value and are still meeting customer needs.

1.14.

Review your business continuity or contingency plans to include this activity. Have you identified any risks?

No

If yes include in the risk section of this template.

1.15.

What training is planned to support this activity?

There is no training required for the migration as Vision and EMIS will be undertaking the data conversion and transfer. However, the Cegedim support staff will be available for advice or guidance when required.

The ICB has purchased user training sessions to be delivered by EMIS both pre-and post-migration to familiarise staff with the knowledge and skills to effectively utilise the new system's features and functionalities.

Once the EMIS Web system goes live, EMIS will continue to offer business as usual user support to GP Practices.

The SCW training team have expertise in both Vision and EMIS systems and will also be providing pre- and post-migration training to the Practice on EMIS Web functionality to ensure staff proficiency.

2. Linkage, Data flows, Sharing and Data Opt Out, Sharing Agreements, Reports, NHS Digital

2.1.

Are you proposing to combine any data sets?

No

If yes then provide the details here.

[Click here to enter text.](#)

2.2.

What are the Data Flows? (Detail and/or attach a diagram if you have one).

The data flows for the migration from Vision to EMIS is set out in the Vision guidance document at 1.14 above.

The Data Flows for the live EMIS Web system is as follows:

Patient > Data Entry to EMIS Web System > Secure Data Storage > Data Retrieval > Clinical Decision > Data Sharing (optional) with other Healthcare Providers > Reporting > Data Archiving

The activities processed in EMIS are:

Care Record

To record and store clinical, administrative and consultation information about patients. This information includes clinical terms, free text observations, lab reports, and attachments such as letters or scanned documents.

Registration

Record information about new and existing patients.

Appointment Book

Use of the Appointment Book to view appointments for planned sessions.

Population reporting

Create, run, save and re-run searches and reports.

Patient Administration

Enable management of patients through the whole care process: from referral, to treatment, to discharge.

Data Sharing

Some organisations have a sharing agreement with another organisation, allowing both organisations to view and add details to the same patient records.

Episode Management

Episode Management enables collection of information to be used for the collection of national [NHS Digital](#) data and Community Data

The Data Flows for EMIS Web can be summarised as follows:

Patient > Data Entry to EMIS Web System > Secure Data Storage > Data Retrieval > Clinical Decision > Data Sharing (optional) with other Healthcare Providers > Reporting > Data Archiving

2.3.

What data/information are you planning to share?

All patient health care records will be transferred and shared from Vision to EMIS during the migration, and following go live the same information will be shared with EMIS by the GP Practice:

- Full name
- Date of birth
- Address and postcode
- Email address
- Phone number
- NHS number
- Gender
- Racial / Ethnic origin

- Relationship to Patient
- Information relating to the individual's physical or mental health condition
- Information relating the individual's sex life
- Information relating to the family life of the individual and the individual's lifestyle and social circumstances
- Occupational status
- Information relating to the individual's religious or other beliefs
- Full health record including prescriptions, diagnosis, test results, vaccination information, clinical studies, appointment details, consultation records, nationality

2.4.

Is any of the data subject to the National Data Opt Out?

Yes - we need to apply it

If your organisation has to apply it describe the agreed approach to this

Complete the form published on the NHS website and register the choice to opt out www.nhs.uk/your-nhs-data-matters

If another organisation has applied it add their details and identify what data it has been applied to

Click here to enter text.

If you do not know if it applies to any of the data involved then you need to speak to your Data Protection Officer to ensure this is assessed.

2.5.

Who are you planning to share the data/information with?

Following the migration from Vision, data will be shared with EMIS Web

2.6.

Why is this data/information being shared?

Vision, supplied by Cegedim, is the existing clinical system in Mortimer Surgery and will be migrating all the patient records to EMIS Web GP as the Vision product is being withdrawn from the market in England. Mortimer Surgery has selected EMIS Web as the replacement. Vision will exit the market on 31 October 2024 and the practice needs to finalise the migration of all electronic patient records from the Vision system to the EMIS system by that exit date.

In the live EMIS environment, the information is shared for the continued provision of healthcare to the patients. The data is broadly used for the diagnosis and treatment of any medical condition and the recording of medical information such as testing and vaccinations.

2.7.

How will you share it? (Consider and detail all means of sharing)

All data migrating from the Vision to the new EMIS system will be transferred electronically between the clinical systems by secure file transfer.

Electronic Transfer – In the live EMIS environment, the data is collected directly from the data subject during registrations, consultations, referrals, and other interactions such as the booking of appointments or changing of name or address and shared electronically via the EMIS Web clinical system.

Tick if you are planning to use Microsoft Teams or another similar online networking/meeting solution that may have the facility to store or record conversations or related data as part of the sharing arrangements

✓

Users are advised not to record or store PID on Microsoft Teams

Provide details of how you have considered any privacy risks of using one of these solutions

Both EMIS Web and Vision are approved NHS clinical services provider solutions.

Cegedim Healthcare Solutions sets out their privacy obligations and privacy rights on their website, together with their commitment to protecting personal data and how the law offers protection.

<https://www.cegedim-healthcare.co.uk/privacy-policy#data-retention>

EMIS sets out in their Privacy notice what they do with personal data and how they keep it secure. The Privacy notice also explains where and how personal data is collected, as well as outlining individual's rights over any personal data they hold. Full details of the Privacy Notice can be found on the EMIS Health website here:

<https://www.emishealth.com/privacy-policy>

2.8.

What data sharing agreements are or will be in place?

The existing BOB ICB agreement with Vision and EMIS will be amended through a Call Off Variation Agreement to incorporate the migration of this Berkshire West practice migrating to the EMIS Web solution.

2.9.

What reports will be generated from this data/information?

The practice will be able to conduct various population reports directly via EMIS.

2.10.

Are you proposing to use Data that may have come from NHS Digital (e.g. SUS data, HES data etc.)?

No

If yes, are all the right agreements in place?

Choose an item.

Give details of the agreement that you believe covers the use of the NHSD data

[Click here to enter text.](#)

If no or don't know then you need to speak to your Data Protection Officer to ensure they are put in place if needed.

3. Data Processor, IG Assurances, Storage, Access, Cloud, Security, Non-UK processing, DPA

3.1

Are you proposing to use a third party, a data processor or a commercial system supplier?

Yes

If yes use these spaces to add their details including their official name and address. If there is more than one then include all organisations. If you don't know then stop and try and find this information before proceeding.

- EMIS Health - EMIS Web, EMIS Head Office, Fulford Grange, Micklefield Lane, Rawdon, Leeds, LS19 6BA
- Cegedim Healthcare Solutions (Parent Company of INPS), Station Approach, Buckshaw Village, Chorley, PR7 7NR
-

[Click here to enter text.](#)

3.2





Is each organisation involved registered with the Information Commissioner? Copy and paste the last empty row in the table to add organisations where required (the text has been left unlocked for this purpose on that row only)



Name of organisation	Registered	Registration details or comments if not registered
EMIS Health	Yes	Z2670786

Cegedim	Yes	Z4925208
Click here to enter text.	Choose an item.	Click here to enter text.
Click here to enter text.	Choose an item.	Click here to enter text.
Click here to enter text.	Choose an item.	Click here to enter text.

3.3

What IG assurances have been provided to you and does any contract contain IG clauses that protect you as the Controller? (e.g. in terms and conditions, their contract, their tender submission). Copy and paste the last empty row in the table to add organisations where required (the text has been left unlocked for this purpose on that row only)

Name of organisation	Brief description of assurances obtained
EMIS Health	<p>EMIS and Cegedim are approved suppliers as part of the GPIT Futures Framework and are available via the NHS Digital Buying Catalogue. The GPIT Futures framework expired as of 31st March 2024. There are numerous practices in BOB utilising EMIS Web.</p> <p>EMIS will be the replacement clinical system for Mortimer Surgery and they are compliant with the Data Security and Protection Toolkit to ensure that NHS data processing standards are met. We are holding the compliance documentation from EMIS Health - they have achieved the Cyber Essentials Certification and have met the BOB ICB DTAC criteria which are attached.</p> <p>All user activity on patient records in EMIS Web is audited, including the selection and viewing of a patient and viewing their record, and the log includes the name and role of the user and cannot be edited or deleted.</p> <p>The EMIS Master Service Level Agreement attached below sets out the supplier’s obligations for the purposes of the contract, including where Sub-Processors are engaged, the identity of the Sub-Processor will be advised to the ICB and EMIS will remain accountable for any Sub-Processor in the same way as for its own actions and omissions.</p> <div style="display: flex; justify-content: space-around; align-items: center;"> <div style="text-align: center;">  EMIS WEB DTAC. Customer Version (1). </div> <div style="text-align: center;">  EMIS_Pen Test Certificate.pdf </div> </div> <div style="display: flex; justify-content: space-around; align-items: center; margin-top: 20px;"> <div style="text-align: center;">  PIA364E EMIS Web DPIA .pdf </div> <div style="text-align: center;">  EMIS_Cyber essentials Certificate.ç </div> </div>

VISION	 <p>LCC1090-EMIS-Universal-Master-Service-</p> <p>Vision's supplier have provided their Information Security Management ISO 27001 certificate, valid until 19/07/2024. They advised they have passed their recertification and are awaiting the updated certificate.</p>  <p>Vision ISO27001 IS Management -IS 5431</p>
Click here to enter text.	Click here to enter text.
Click here to enter text.	Click here to enter text.
Click here to enter text.	Click here to enter text.

3.4

What is the status of each organisation's Data Security Protection Toolkit?

[DSP Toolkit](#)

Copy and paste the last empty row in the table to add organisations where required (the text has been left unlocked for this purpose on that row only)

Name of organisation	ODS Code	Status	Published date
EMIS Health	YGM06	23/24 Standards Exceeded	17/06/2024
Cegedim	YGH	23/24 Standards Exceeded	17/06/2024
Click here to enter text.	Click here to enter text.	Click here to enter text.	Click here to enter text.
Click here to enter text.	Click here to enter text.	Click here to enter text.	Click here to enter text.
Click here to enter text.	Click here to enter text.	Click here to enter text.	Click here to enter text.

3.5

How and where will the data/information be stored? (Consider your answer to 2.7 and the potential storage of data in any online meeting or networking solution).

At all times during the practice system migration, patient data will only be held in Vision and EMIS Web which are NHS approved clinical suppliers and the data transfer will adhere to approved processes to ensure that patient data remains secure. After the migration, patient data will be retained by Vision solely for the purpose of being able to address any queries arising. Any data supplied by, or on behalf of the practice, will be destroyed by Vision 90 days after the migration date.

3.6

How is the data/information accessed and how will this be controlled?

The Vision hosted system will remain available for reference for a minimum of 90 days following go-live with the new system with RBAC controls to remain in place. No additional data can be added – it will become a storage vehicle.

Access to patient data in EMIS Web will only be permitted to users with the appropriate RBAC mapping which is managed locally by practices on private networks. This will be via the Smartcard for the practice or if no Smartcard is used by the clinician the RBAC mappings will be granted to an EMIS account directly via the user setup configuration.

Regular audits of access must be conducted by the practice's Privacy Officer.

3.7

Is there any use of Cloud technology?

Yes

If yes add the details here.

Both Vision and EMIS Web GP is a hosted Service.

Following migration, the EMIS Web will be hosted by London-based Amazon Web Services cloud servers. Care records are cached locally on a spoke server each day, but the data remains stored on AWS servers.

3.8

What security measures will be in place to protect the data/information?

VISION MIGRATION DATA

Cegedim Healthcare Solutions staff work in accordance with the guiding principles of Caldicott and are compliant with Medical Reports Act, Access to Health Records Act, and the Data Protection Act. All staff are familiar with the Good Practice Guidelines for General Practice Electronic Patient Records. Access to data storage space is controlled by an electronic key system with CCTV and video recording monitoring access routes to and within their building.

Data provided by a practice for a merge, split or conversion is used only for that purpose. Once the process is complete, data is kept solely for the purpose of being able to address any queries arising. Any data supplied by or on behalf of the practice, will be destroyed 90 days after the migration date. Internal records, which may include paper and magnetic media, are retained for two years following go live.

EMIS DATA

Patient data will only be held in EMIS Web GP. EMIS are NHS approved clinical suppliers which requires adherence to strict security measures and approved procedures.

Access to patient data will only be permitted to users with the appropriate RBAC mapping in the practice. This will be managed via the Smartcard RA for the practice or if no smartcard is used by the clinician the RBAC mappings will be granted to an EMIS account directly via the user setup configuration.

Regular audits of access must be conducted by the practice's Privacy Officer.

There are controls to further ensure that adequate security measures are in place to deal with the following risks:

Loss of data or accidental access

There are a number of access routes to the data held in EMIS Web for various purposes, but there are controls in place to prevent inappropriate or accidental access to data, such as RBAC in both the front and back end.

Access to live data for support purposes is very restricted, and only given with customer consent with reference to a particular issue.

EMIS Web is subject to frequent penetration tests, with all relevant findings remediated, which gives confidence in the security of this system.

However, as the information both identifies the patient and their medication, this is Special Category data which may be sensitive.

Inappropriate processing of personal data

The data subject consents to this data being processed when they join the Practice, and they have the option to opt out of processing where applicable.

All processing is for Health and social care provision (and sometimes for public health or legal obligations); contracts between EMIS and our Partners and customers cover all processing. Various DSAs are in place at the customers discretion where required for any processing involving third parties. EMIS only processes the data according to the contracts and DSAs in place with the customer.

Inappropriate Data Transfer

All means of transfer are sufficiently tested and established so as to ensure confidence that there will be no inappropriate transfer of EMIS Web data.

All transfer is justified by various means, most notably any DSAs and contracts in place. As required by the NHS data always remains in the UK.

Users have the option to transfer data from EMIS Web but are trusted to act with the professionalism that is expected with their role in a clinical setting.

Loss of data integrity

Access to the live data held in EMIS Web is restricted to RBAC authorised Practice staff and relevant support personnel within EMIS.

There is significant redundancy in place that any lack of accessibility of data is very unlikely.

EMIS Web has been sufficiently tested to protect data integrity, including regular penetration testing being completed to ensure continued security of the system.

Is a specific System Level Security Policy needed?

No

If yes or don't know then you need to speak to your Data Protection Officer to ensure one is put in place if needed.

3.9

Is any data transferring outside of the UK? (you must determine this so only select don't know if you have further investigations to make but the DPIA will not be approved without this information)

No

If yes describe where and what additional measures are or will be in place to protect the data.

[Click here to enter text.](#)

3.10

What Data Processing Agreement is already in place or if none, what agreement will be in place with the organisation and who will be responsible for managing it?

VISION – existing Agreements will be as set out in the Contract between the ICB and INPS.

EMIS - The position in relation to data processing and the list of the Supplier's Sub-processors shall be as set out in the associated Master Service Agreement (attached at 3.3 of this DPIA) in the NHS Digital Catalogue Solution Listing. The Master Service Level Agreement and the appendix at Annex 1 outlines the details of EMIS's data processing activities, including the types of personal data processed, the purposes of processing, and the legal basis for processing. The listing also details contractual safeguards in place regarding Sub-Processors.

EMIS confirms that it has implemented appropriate technical and organisational measures to protect personal data against unauthorised or unlawful processing, accidental loss, destruction, or damage. Additionally, EMIS takes all reasonable steps to ensure the reliability and integrity of personnel who have access to or process personal data.

4. Privacy Notice, Individual Rights, Records Management, Direct Marketing

4.1

Describe any changes you plan or need to make to your Privacy Notice and your proposed completion date?

(There is a checklist that can be used to assess the potential changes required or if you wish for it to be reviewed then add the link below).

The practices privacy notice will need to be updated if appropriate to reflect the change of clinical system supplier to inform the patient.

4.2

How will this activity impact on individual rights under the GDPR? (Consider the right of access, erasure, portability, restriction, profiling, automated decision making).

No impact. Individual Rights remain the responsibility of the Data Controller.

4.3**How long is the data/information to be retained?**

Vision and EMIS will retain the data in accordance with Records Management Code of Practice for Health and Social Care.

4.4**How will the data/information be archived?**

Data will be archived in accordance with Records Management Code of Practice for Health and Social Care, and in line with national requirements and guidance regarding archiving of electronic patient records.

4.5**What is the process for the destruction of records?**

No patient records will be deleted. Vision will only delete test data on instruction from the practices.

4.6**What will happen to the data/information if any part of your activity ends?**

If a new clinical system is procured in the future, the patient data will be transferred securely and in accordance with all approved processes and regulations required by BOB ICB.

4.7

Will you use any data for direct marketing purposes? (you must determine this so only select don't know if you have further investigations to make but the DPIA will not be approved without this information)

No

If yes please detail.

[Click here to enter text.](#)

5. Risks and Issues

5.1

What risks and issues have you identified? The DPO can provide advice to help complete this section and consider any measures to mitigate potential risks.

Describe the source of risk and nature of potential impact on individuals. (Include associated compliance and corporate risks as necessary and copy and paste the complete bottom row to add more risks (the text has been left unlocked in both tables to enable you to do this)).	Likelihood of harm	Severity of harm	Overall risk
1. Time taken for practice to learn how to use the new system could lead to delays in patient care	Possible	Significant	Low
2. During the cutover period, changes to practice records on Vision will be frozen and need to be manually added to new system	Possible	Significant	Medium
3. Delays in migration: Migration needs to occur by 31/10/2024 when Vision is decommissioned	Possible	Severe	Low
4. Loss of Data Integrity causing corruption of personal information	Possible	Significant	Low
5. Inappropriate or unlawful processing of personal data	Possible	Severe	Low
6. Inappropriate or unlawful data transfer	Possible	Significant	Low
7. Business Continuity could be disrupted in the event of physical or technical incident, both in the migration, or in the live EMIS environment	Probable	Significant	Low

5.2

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in 5.1

Risk	Options to reduce or eliminate risk	Effect on risk	Residual risk	Measure approved (SIRO)

1. Time taken for practice to learn how to use the new system could lead to delays in patient care	EMIS will provide training days after the transition and following this, SCW CSU will be able to provide further training if required.	Reduced	Low	Choose an item.
2. During the cutover period, changes to practice records on Vision will be frozen and need to be manually added to new system	Practice need to be informed of the cutover date to know at which point to minimise updating a patient record and keep track of any changes in order to manually implement these changes in EMIS after the migration	Reduced	Medium	Choose an item.
3. Delays in migration - Migration needs to occur by 31/10/2024 when Vision is decommissioned	BOB ICB have been liaising with EMIS & Vision and have obtained migration dates in advance of the Vision exit date.	Reduced	Medium	Choose an item.
4. Loss of Data Integrity causing corruption of personal information	<p>Access to the live data held in EMIS Web is restricted to RBAC authorised Practice staff and relevant support personnel within EMIS.</p> <p>There are robust measures minimising the risk of data inaccessibility.</p> <p>EMIS Web has been sufficiently tested to protect data integrity, including regular penetration testing being completed to ensure continued security of the system.</p> <p>EMIS Web data is in multiple places for Business Continuity.</p>	Reduced	Low	Choose an item.
5. Inappropriate or unlawful processing of personal data	<p>The ICB and EMIS have robust security measures in place to protect personal data from unauthorised alteration. Governance frameworks within each organisation has established defined policies and procedures for handling personal data.</p> <p>The data subject consents to this data being processed when they join the Practice, and they have the option to opt out of processing where applicable.</p>	Reduced	Low	

	All processing is for Health and social care provision (and sometimes for public health or legal obligations); contracts between EMIS and our Partners and customers cover all processing. Various DSAs are in place at the customers discretion where required for any processing involving third parties. EMIS only processes the data according to the contracts and DSAs in place with the customer.			
6. Inappropriate or unlawful data transfer	<p>All means of transfer are sufficiently tested and established so as to ensure confidence that there will be no inappropriate transfer of data during the migration or following the deployment of EMIS Web.</p> <p>All transfer is justified by various means, most notably any DSAs and contracts in place. As required by the NHS data always remains in the UK.</p> <p>Users have the option to transfer data from EMIS Web but are trusted to act with the professionalism that is expected with their role in a clinical setting.</p> <p>EMIS has conducted DTAC assessments to provide the ICB with assurance of their data security practices, compliance position and their ability to uphold the data privacy regulations. EMIS has submitted their Data Protection Security Toolkit to evidence adherence to the NHS security standards.</p>	Reduced	Low	
7. Business Continuity could be disrupted in the event of physical or technical incident, both in the migration, or in the live EMIS environment	Vision and EMIS Web both use cloud hosting infrastructure, which will provide real-time back up of the data sets in the clinical systems so patient records can be retrieved.	Reduced	Low	

5.3

What if anything would affect this piece of work?

Delays in migration date.

Vision has a fixed date on which they will exit the market, 31 October 2024. Migration of patient data is taking place on 24th September 2024 to allow sufficient time to migrate the data and manage any challenges that may arise.

5.4
Please include any additional comments that do not fit elsewhere in the DPIA?

None

6. Consultation

6.1
Have you consulted with any external organisation about this DPIA?

No

If yes, who and what was the outcome? If no, detail why consultation was not felt necessary.

6.2
Will you need to discuss the DPIA or the processing with the Information Commissioners Office? (You may need the help of your DPO with this)

No

If yes, explain why you have come to this conclusion.

[Click here to enter text.](#)

7. Data Protection Officer Comments and Observations

7.1
Comments/observations/specific issues

GP DPO comments: dated 18 July 2024

Comprehensive DPIA completed.

Recommendation:
GP Practice to update their Privacy Notice.

Suggested text:
Purpose:

Mortimer Surgery – Migration to EMIS Clinical System

Mortimer Surgery (MORTIMER) will be adopting the EMIS Web clinical system supplied by EMIS Health.

EMIS Web are applications used to deliver GP services allowing clinical users such as GPs and nurses to view and add medical information to patient records. Other functionality is available, providing services such as appointment booking and diary management.

EMIS web is software solution for primary care organisations, containing and sharing personal and sensitive data. This data is encrypted in transit. The Data Controllers for EMIS Web are GP organisations, EMIS acts as a Data Processor.

EMIS and Cegedim are approved suppliers as part of the GPIT Futures Framework and are available via the NHS Digital Buying Catalogue

	<p>Legal Basis of Processing</p> <p>Article 6 (1)</p> <p>e) it is necessary for the performance of a task carried out in the public interest or under official authority vested in the controller</p> <p>Article 9 (2)</p> <p>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 on the basis of union or member state law or pursuant to contract with a health professional and subject to conditions and safeguards</p> <p>Further notes:</p> <p>The Practice to kindly note additional measures to take and reduce or eliminate risks identified as medium or high risk in 5.1 followed by table 5.2.</p> <p>The Practice to update their Information Assets Register.</p> <p>BOB ICB DPO comments: This is a comprehensive DPIA covering the transfer of data from Vision to EMIS Web. The comments made by the GP DPO regarding the Practice Privacy Notice and Information Asset Registers is endorsed.</p>
--	--

8. Review and Outcome

Based on the information contained in this DPIA along with any supporting documents, you have determined that the outcome is as follows:

A) There are no further actions needed and we can proceed

If you have selected item B), C) or D) then please add comments as to why you made that selection

[Click here to enter text.](#)

We believe there are

Choose an item.

If you have selected item B) or C) then list these in the amber boxes below and then consider additional measures you could take and include these in the green boxes below

Residual risks and nature of potential impact on individuals. (Include associated compliance and corporate risks as necessary and copy and paste the complete bottom row to add more risks (the text has been left unlocked in both tables to enable you to do this)).	Likelihood of harm	Severity of harm	Overall risk
Click here to enter text.	Choose an item.	Choose an item.	Choose an item.
Click here to enter text.	Choose an item.	Choose an item.	Choose an item.
Click here to enter text.	Choose an item.	Choose an item.	Choose an item.
Click here to enter text.	Choose an item.	Choose an item.	Choose an item.

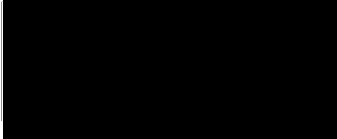
Additional measures you could take to reduce or eliminate residual risks identified as medium or high risk above (B and C)

Risk	Options to reduce or eliminate risk	Effect on risk	Residual risk	Measure approved (SIRO)
Click here to enter text.	Click here to enter text.	Choose an item.	Choose an item.	Choose an item.
Click here to enter text.	Click here to enter text.	Choose an item.	Choose an item.	Choose an item.
Click here to enter text.	Click here to enter text.	Choose an item.	Choose an item.	Choose an item.
Click here to enter text.	Click here to enter text.	Choose an item.	Choose an item.	Choose an item.

Signed and approved on behalf of Buckinghamshire Oxfordshire and Berkshire West Integrated Care Board

Name: 

Job Title: Data Protection Officer

Signature:  Date: 19/07/2024

Signed and approved on behalf of Click here to enter text.

Name: Click here to enter text.

Job Title: Click here to enter text.

Signature: Click here to enter text. Date: Click here to enter a date.

Please note:

You should ensure that your Information Asset Register and Data Flow Mapping Schedules are updated where this is relevant as a result of this project.

This DPIA can be disclosed if requested under the Freedom of Information Act (2000). If there are any exemptions that should be considered to prevent disclosure detail them here: Click here to enter text.