



## Data Protection Impact Assessment (DPIA) Template

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 <b>profiling or automated decision-making</b> to make significant decisions about people or their access to a service, opportunity or benefit;	<input type="checkbox"/>
Process <b>special-category data or criminal-offence data on a large scale</b> ;	<input checked="" type="checkbox"/>
<b>Monitor a publicly accessible place</b> on a large scale;	<input type="checkbox"/>
Use <b>innovative technology</b> in combination with any of the criteria in the European guidelines;	<input type="checkbox"/>
Carry out <b>profiling</b> on a large scale;	<input type="checkbox"/>
<b>Process biometric or genetic data</b> in combination with any of the criteria in the European guidelines;	<input type="checkbox"/>
<b>Combine, compare or match data</b> from multiple sources;	<input checked="" type="checkbox"/>
Process personal data <b>without providing a privacy notice</b> directly to the individual in combination with any of the criteria in the European guidelines;	<input checked="" type="checkbox"/>
Process personal data in a way that involves <b>tracking</b> individuals' online or offline location or behaviour, in combination with any of the criteria in the European guidelines;	<input type="checkbox"/>
Process <b>children's</b> 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 <b>risk of physical harm</b> 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 type="checkbox"/>
Include data concerning vulnerable data subjects;	<input checked="" type="checkbox"/>
Plan to use innovative technological or organisational solutions;	<input 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	
<b>Date of your DPIA :</b>	20/11/2023
<b>Title of the activity/processing:</b>	<b>Provision of Rego Eye Electronic Referral Service software.</b>
<b>Who is the person leading this work?</b>	██████████
<b>Who is the Lead Organisation?</b>	<p>This initiative is for Year 2 of the switch to use of Rego software for ophthalmology referrals. NHSE was sponsor in the pilot Year 1, in which Kent &amp; Medway, Buckinghamshire Oxfordshire and Berkshire CCGs, Sussex CCGs were local sponsors.</p> <p>The contract with NEC, supplier of Rego, sits with the ICB since 1.4.2023.</p>
<b>Who has prepared this DPIA?</b>	<p>██████████, Strategic IG Lead, South Central and West Commissioning Support Unit</p> <p>██████████, Project Manager</p>
<b>Who is your Data Protection Officer (DPO)?</b>	██████████
<b>Describe what you are proposing to do:</b> (Include as much background information as you can about why the new system/change in system/sharing of information/data processing is required).	<p>Responding to pressures in secondary care eye-care services due to COVID and a historic imbalance in demand and capacity, NHSX secured funding for health care systems to procure eye-care referral and image sharing technologies. NEC Rego software was commissioned for pilot rollout across Kent &amp; Medway, Sussex and BOB CCGs.</p> <p>Each NHS region has, or is planning to, contract with an Eye electronic Referral System (“EeRS”) with BOB ICB.</p> <p>The software solution is NEC Rego Care Navigator, which is a supplier system on NHSE’s Dynamic Purchase System (DPS), and helps optometrists refer patients directly to best care based on local and national pathways. The new direct referral route removes the requirement for the Optician contact the GP to make the referral.</p>
<b>Are there multiple organisations involved?</b> (If yes – you can use this space to name them, and who their key contact for this work is).	<p>Yes.</p> <p><b>BOB ICB Local Providers:</b></p> <ol style="list-style-type: none"> <li>1. Oxford University Hospitals Trust</li> <li>2. Royal Berkshire NHS Foundation Trust</li> <li>3. East Sussex Healthcare Trust</li> <li>4. Operose Limited</li> <li>5. East Kent Hospital University Foundation Trust</li> <li>6. Other Local ophthalmology providers as determined by the ICB.</li> <li>7. Individual Community Optometrist Practices wishing to refer customers via NHS referral pathway (patients)</li> </ol>

<p><b>Can you think of any other Key Stakeholders that should be consulted or involved in this DPIA?</b> (If so then include the details here).</p>	<p>Local Optometry Council – IG documentation has been provided to the LOC and LOCSU as part of prior rollout to gain their assurance to the local optometrists.</p>
<p><b>Detail anything similar that has been undertaken before?</b></p>	<p>Rego EeRS is already in use within the NHS for Dentistry and Medicine patient pathway referral management.</p> <p>This DPIA updates the previous one prepared for the NHSE pilot programme.</p> <div style="text-align: center;">  <p>DPIA Controllers EeRS all BOB CCGs s</p> </div>

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

**1.1.**

What data/information will be used?	Tick or leave blank	Complete
Tick all that apply.		
Personal Data	✓	1.2
Special Categories of Personal Data	✓	1.2 AND 1.3
Personal Confidential Data	✓	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 type="checkbox"/>	1.2 and consider at what point the data is to be pseudonymised
Anonymised Data	✓	Consider at what point the data is to be anonymised
Commercially Confidential Information	<input type="checkbox"/>	Consider if a DPIA is appropriate
Other	<input 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:	
<p><b>a) THE DATA SUBJECT HAS GIVEN CONSENT</b></p>	<p>Tick or leave blank</p> <input type="checkbox"/>
<p><b>Why are you relying on consent from the data subject?</b> Click here to enter text.</p>	
<p><b>What is the process for obtaining and recording consent from the Data Subject?</b> (How, where, when, by whom). Click here to enter text.</p>	
<p><b>Describe how your consent form is compliant with the Data Protection requirements?</b> (There is a checklist that can be used to assess this). Click here to enter text.</p>	
<p><b>b) IT IS NECESSARY FOR THE PERFORMANCE OF A CONTRACT TO WHICH THE DATA SUBJECT IS PARTY</b></p> <p>(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).</p>	<p>Tick or leave blank</p> <input type="checkbox"/>

<b>What contract is being referred to?</b> <a href="#">Click here to enter text.</a>	
<b>c) IT IS NECESSARY UNDER A LEGAL OBLIGATION TO WHICH THE CONTROLLER IS SUBJECT</b> (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).	Tick or leave blank <input type="checkbox"/>
<b>Identify the legislation or legal obligation you believe requires you to undertake this processing.</b> <a href="#">Click here to enter text.</a>	
<b>d) IT IS NECESSARY TO PROTECT THE VITAL INTERESTS OF THE DATA SUBJECT OR ANOTHER NATURAL PERSON</b> (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"/>
<b>How will you protect the vital interests of the data subject or another natural person by undertaking this activity?</b> <a href="#">Click here to enter text.</a>	
<b>e) IT IS NECESSARY FOR THE PERFORMANCE OF A TASK CARRIED OUT IN THE PUBLIC INTEREST OR UNDER OFFICIAL AUTHORITY VESTED IN THE CONTROLLER</b> (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"/>
<b>What statutory power or duty does the Controller derive their official authority from?</b> The ICB is a statutory body with the function of commissioning health services in England and is treated as an NHS body for the purposes of the 2006 Act. The powers and duties of the ICB to commission certain health services are set out in sections 3 and 3A of the 2006 Act.  Optometrists are commissioned under contract to the ICB (which acts under delegated authority from NHS England) to provide services to the NHS. Each optometrist practice may hold and share patients' personal data with other regulated health care practitioners for health care purposes, and as a business to carry out their business effectively in looking after their patients' care.	
<b>f) IT IS NECESSARY FOR THE LEGITIMATE INTERESTS OF THE CONTROLLER OR THIRD PARTY</b> (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"/>
<b>What are the legitimate interests you have?</b>	
Article 9 (2) conditions are as follows:	
<b>a) THE DATA SUBJECT HAS GIVEN EXPLICIT CONSENT</b> (Requirements for consent are the same as those detailed above in section 1.2, a))	Tick or leave blank <input type="checkbox"/>
Tick or leave blank	

<p><b>b) FOR THE PURPOSES OF EMPLOYMENT, SOCIAL SECURITY OR SOCIAL PROTECTION</b></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>	<input type="checkbox"/>
<p><b>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</b></p> <p>(Requirements for this are the same as those detailed above in section 1.2, d))</p>	<p>Tick or leave blank</p> <p style="text-align: center;"><input type="checkbox"/></p>
<p><i>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</i></p>	NA
<p><i>e) The data has been made public by the data subject</i></p>	NA
<p><i>f) For legal claims or courts operating in their judicial category</i></p>	NA
<p><b>g) SUBSTANTIAL PUBLIC INTEREST</b></p> <p>(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).</p>	<p>Tick or leave blank</p> <p style="text-align: center;"><input type="checkbox"/></p>
<p><b>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</b></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><b>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</b></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><b>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.</b></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 j). 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).

The ICB, as Authority, contracts with NEC, the Provider, and is named Controller in the Contract.

NEC is data processor.

Each provider (Optician, ophthalmology provider) is controller of their own data in their own systems, and for information contained within its referral in Rego.

Name of Organisation	Role
BOB ICB	Sole Controller
All Optometrists participating within ICB	Sole Controller
All Ophthalmology services Provider organisation	Sole Controller
NEC	Processor
Click here to enter text.	Choose an item.
Click here to enter text.	Choose an item.
Click here to enter text.	Choose an item.

**1.5.**

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

Optometrists will send eye patient referrals via the NEC software solution, Rego EeRS, which will then pass the referral information to the provider rather than the current process which requires the Optometrist to request referral through the GP.

The Rego software will be configured with local pathways to route the referral to the correct provider for each ophthalmology specialism (e.g., cataracts).

Patient information will include demographics, NHS number, and clinical information relevant to the referral. Clinical information may include Dicom images and the medical condition.

Dicom images are a type of image in this case take of the eye(s) like an X-ray and sent with the referral. This is not always done. <https://en.wikipedia.org/wiki/DICOM>

When a referral is created, Rego will check patient details against the Spine, and attach a summary from the patient’s Summary Care Record. This will not be done where the patient has opted out of Summary Care Record at their GP Practice.

Each provider is responsible for IG assurance on their own part in the referral process and may accept this DPIA or create their own.

**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)

Health data - Optometry records

**1.7.**

**How are you satisfying the common law duty of confidentiality?**

**For the ICB:**

Consent - Implied

**The ICB does not access any personal or confidential data. Only the software is provided.**

**For the Optician:**

Consent - Implied

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

The Optician will inform the patient that a referral is being made for further treatment. The patient agrees to be referred.

The Optician will inform the patient that they will see information held within the Summary Care Record as part of the referral. Rego presents a consent box for the optician to tick this element.

The Summary care record only contains a limited dataset, that would be sought by the optician from the patient as part of the consultation, this being demographics and information about allergies and medications and any reactions a patient may have had to medication in the past. Full information about the SCR is published here by NHSE: [NHS England » Summary Care Records \(SCR\)](#)

Whilst the SCR can be shared lawfully without consent for direct care, opticians are not yet all included in routine sharing but NHSE has planned that they all will be, and some optician chains are already included. For transparency, the optician should ask for the patient’s consent before viewing and present the dialog box to the referring optician. If the patient doesn't consent, the referrer can click No and continue with the referral and send it, but a copy of the patient's SCR will not be attached to the referral. Opticians may need some guidance on what the patient needs to know about the SCR in order to make this informed consent. The optician will need to consider how this is reflected in their own privacy notice but can ask the patient to contact their GP Practice if they wish to discuss their preference for sharing their information.

**NHS Summary Care Record Access Management**

---

**STOP. Has the patient given you permission to view their Summary Care Record?**  
 The usual legal ethical and professional obligations apply when accessing a patient's clinical record.

Yes
Emergency access
No

**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.**

Data transfer from Optometrist system to Rego EeRS is encrypted through API, or if API is not yet implemented then data is input directly by the Optometrist via secure login to Rego EeRS.

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.

[Click here to enter text.](#)

**1.10.**

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

Patients assessed by Optometrist as requiring referral for further individual eye care.  
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.)

Face to face - in person  
Web based data collection  
Other method not listed  
By telephone  
Choose an item.

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

Optometrists will log in to Rego in the first phase. Later phases will use API encrypted transfer from the Optometrist's patient system.  
Please note that this DPIA will be updated for API rollout at later stage.

**1.12.**

**How will you edit the data?**

Data in each Controller's systems will not be changed as part of this process. Referrals within Rego EeRS are not edited. Mismatches of data will be referred to the source system for resolution.

**1.13.**

**How will you quality check the data?**

For direct manual entry via secure login to Rego EeRS there will be a look-up to the NHS mini-Spine to match patient details and NHS number. If no NHS number, the patient will be asked to check with their GP to update correct information in the Spine, so that their NHS number can be accessed from the spine.

Optician is responsible for accuracy of data within the referral, e.g., attaching the correct DICOM image for that patient. When Rego EeRS will take data directly from the Optometrist system, data must be accurate at source.

**1.14.**

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

The standard contract terms with NEC detail the requirements for business continuity planning, testing and implementation, and the supplier has provided a copy of their business continuity plan.  
Each controller must consider their own business continuity or contingency plans for use of the Rego EeRS. A generic risk has been included in this DPIA.

Choose an item.

**If yes include in the risk section of this template.**

**1.15.**

**What training is planned to support this activity?**



Users of the EeRS will require training to use the system, which is provided by NEC. GPs will need to be made aware of the new process as they will receive an automatic notification through EeRS once referral has been made and provider has completed the referral. Provider staff may process referrals by direct entry to Rego or will be informed of how the referral appears in their EMS in order to process further within their own system.

## 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).

Data Flow and process map accompanies this DPIA as separate document in Section 3.5.

### 2.3.

**What data/information are you planning to share?**

Personal and referral data in relation to eyecare referrals including:

Name, address, date of birth, phone number, NHS number, Dicom images of the eye, relevant medical information

[Click here to enter text.](#)

### 2.4.

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

No - it is not subject to the national data opt out

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

[Click here to enter text.](#)

**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?**

Community Optometrists' patient data will be shared to the Rego EeRS, referral details will be passed by Rego to the patient's GP Practice by EeRS notification. Providers will receive the information in accordance with local pathway through Rego.

### 2.6.

**Why is this data/information being shared?**

To allow electronic referral of an optometry patient to Ophthalmology provider for direct care. No additional data will be shared than currently, this is an update to the means of transfer and a streamlining of the current process which uses paper and email.

### 2.7.

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

Patient information will be shared from Optometrist system to Rego either via API from Optometry system or by direct web login to Rego by the Optometrist if an API is not available for that system (Phase 1). The



Optometrist selects the care pathway for referral based on Rego EeRS pre-set information and the referral is then passed securely to the Provider by locally determined pathway.

**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**

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

[Click here to enter text.](#)

### 2.8.

**What data sharing agreements are or will be in place?**

A data sharing agreement is not required for direct care.

Where an optician practice does not yet have a GOS contract with the ICB, a Data Sharing Agreement may be put in place between them and the ICB to detail the information sharing and use of Rego software for NHS referrals.

### 2.9.

**What reports will be generated from this data/information?**

The providers and NEC will report anonymous usage data to the ICB to enable effective contract management. No identifiable data will be shared with the ICB. Any provider organisation will only be able to see information relating to their own referrals.

### 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.**

Rego EeRS software and API is provided by NEC Software Solutions, registered at:

BizSpace, 1st Floor, iMex Centre, 575-599, Maxted Rd, Hemel Hempstead, HP2 7DX

The hosting of the software is via the Supplier's sub-processor Redcentric Ltd with company number 08397584 and registered address Central House, Beckwith Knowle, Harrogate, North Yorkshire, HG3 1UG trading as CareLink.

[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.

### 3.2

**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
BOB ICB	Yes	ZB343068
NEC Software Solutions	Yes	Z5666588
All Optometrist Practice participating within ICB	Choose an item.	Each provider is responsible for own registration
Ophthalmology healthcare provider	Yes	Each provider is responsible for own registration
Redcentric solutions (sub processor to NEC)	Yes	ZA010053
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
NEC Software Services	The ICB contracts with NEC to provide the EeRS solution under standard NHSE contract. Standard NHS IG clauses are included, and Data Processing Protocol is included as Schedule 3. NEC has provided a DTAC assurance. Each Optometry Practice and Ophthalmology Provider is commissioned by the ICB to provide healthcare services (GOS contract for opticians).
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](#)

The DSP Toolkit details are for each organisation to enter. NHS contract requires completion of the Toolkit, as does access to NHS systems.

**NOTE: There are a small number of independent optometry practices that are not yet covered by GOS contract with the ICB and may not already have the DSP Toolkit. This is captured in the risks at the end of this DPIA.**

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
All Optometrist within ICB	to enter own details	Click here to enter text.	Click here to enter text.
BOB ICB	QU9	Standards Exceeded	27/06/2023
NEC Software	DXL	Standards Exceeded	28/06/2023

	<a href="#">Click here to enter text.</a>	<a href="#">Click here to enter text.</a>	<a href="#">Click here to enter text.</a>
RedCentric solutions (sub-processor)	YGMAP	Standards Exceeded	06/06/2023
	<a href="#">Click here to enter text.</a>	<a href="#">Click here to enter text.</a>	<a href="#">Click here to enter text.</a>

### 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).

Generic Rego EeRS process flow accompanies this DPIA.



20220518\_EeRS processes\_v0.14 vsd:

Referral information will flow from Optometrist system to Rego EeRS or is entered into Rego manually if API is not available (during Phase 1). Rego EeRS selects care pathway (this will be setup beforehand within Rego EeRS). Where applicable, Rego or ophthalmology staff may access the referral using Smartcards in order to select pathway and forward referral. Onward Referral flows are determined by the ICB to reach the selected ophthalmology provider.

Optometrists, GP Practice and Providers remain controller of their data in their own system. NEC stores referral data within the Rego EeRS as processor.

The following generic DPIA is completed by NEC for Rego software (but gives GP as referrer not opticians):



NEC DPIA Rego Generic v1\_1.docx

### 3.6

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

Optometrist logs in to Rego EeRS through secure RBAC controlled login managed by NEC.

Currently each Optician Practice has one login, then Optician selects name from given list of opticians assigned to that practice (opticians may work for more than one practice. NEC has committed to providing individual logins for each optician, currently only with Specsavers.

Referral data will be captured by optometrists and will be stored within the Rego system maintained by NEC.

Authorised NEC staff may access the Rego software and referrals for system admin purposes only.

Ophthalmology Provider staff may log in to Rego EeRS with authorised Smartcard in order to process the referral to next pathway (this may vary for each provider). This process will be documented for each provider, typically this will be:

Provider provides instructions to NEC to create/delete users on the Rego system in writing by an email. It is Provider's responsibility to inform NEC of any changes regarding who should and should not have access to the system.

Every interaction completed on Rego is tracked and can be reported on.

**3.7**

**Is there any use of Cloud technology?**

Yes

**If yes add the details here.**

The hosting (via the Supplier’s sub-processor Redcentric PLC with company number 08397584 and registered address Central House, Beckwith Knowle, Harrogate, North Yorkshire, HG3 1UG trading as CareLink) is included in the ICB’s contract with NEC.

[Click here to enter text.](#)

**3.8**

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

Security measures applied to the Rego EeRS are to agreed NHS security standards.

The DTAC for Rego software has been completed and is attached here:



DTAC Application  
Form FINAL - June 21

**Is a specific System Level Security Policy needed?**

Yes

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?**

The ICB contracts with NEC to provide the EeRS solution under standard NHSE order form/contract. Standard NHS IG clauses are included, and a Data Processing Agreement is included as Schedule 3.

Opticians and other ophthalmology providers are commissioned by the ICB under standard NHS contract to provide healthcare services and the ICB determines the referral process.

The Optometrist Practice or other Ophthalmology provider does not need to a separate data processing agreement with NEC. The ICB’s DPIA will be provided to Providers for information and assurance.

**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).

Each Controller should update their Privacy Notice as appropriate to update patients on the sharing of their data from Optometrist to providers by use of Rego EeRS. The patient at the Optometrist will be told the referral for further treatment will be made electronically.

**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).

Individual Rights will be managed by each Controller in accordance with their own policy and procedures in line with the Data Protection Legislation.

**4.3**

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

For the duration of the ICB’s contract with NEC.

**4.4**

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

The data remains current until end of contract, there is no requirement to archive.

**4.5**

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

Patient data held in Rego EeRS will be purged by secure means at the end of contract, on written direction of the commissioner. There will be no physical records requiring disposal.

**4.6**

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

At the written direction of the commissioner, NEC will purge the personal data (and any copies of it).

**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. <small>(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)).</small>	Likelihood of harm	Severity of harm	Overall risk
There is a risk that personal data may be misused by those with access	Possible	Significant	Medium
There is a risk that insufficient organisational measures are in place to ensure appropriate security of the personal data (e.g. policies, procedures, disciplinary controls)	Possible	Significant	Medium
There is a risk that insufficient technical measures are in place to ensure appropriate security of the personal data (e.g. encryption, access controls)	Possible	Significant	Medium

There is a risk that insufficient testing has taken place to assess and improve the effectiveness of technical and organisational measures	Possible	Significant	Medium
There is a risk that data that has had identifiers removed could be manipulated in some way to re-identify individual people	Remote	Significant	Low
There is a risk that the Rego EeRS pathways are not implemented correctly and the system does not direct the referral correctly to the Provider or inform the GP Practice	Possible	Significant	Medium
There is a risk that patient data held by the Optometrist cannot be matched to the Spine and so cannot be processed further in Rego EeRS.	Possible	Moderate	Medium
Independent Opticians may not yet have a GOS contract with the ICB, or DSPT, or ICO registration.	Possible	Moderate	Medium
Risk of insufficient audit trail of events such as inappropriate access: Currently each Optician Practice has one login, then Optician selects name from given list of opticians assigned to that practice (opticians may work for more than one practice. NEC has committed to providing individual logins for each optician, currently only for Specsavers.	Possible	Moderate	Medium

## 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)
There is a risk that personal data may be misused by those with access	all users complete IG training;	Reduced	Medium	Choose an item.
There is a risk that insufficient organisational measures are in place to ensure appropriate security of the personal data (e.g. policies, procedures, disciplinary controls)	users are subject to code of conduct, policy and procedures, possible disciplinary measures. Robust process for authorisation of new users; appropriate measures are required in the terms of the contract	Reduced	Low	Choose an item.
There is a risk that insufficient technical	RBAC user accounts; security measures including audit and	Reduced	Low	Choose an item.



measures are in place to ensure appropriate security of the personal data (e.g. encryption, access controls)	monitoring to investigate any inappropriate use; encryption of data at rest and in transit; security to NHS standards and system requirements; appropriate measures are required in the terms of the contract; only authorised users involved in the patients' care will access.			
There is a risk that insufficient testing has taken place to assess and improve the effectiveness of technical and organisational measures	Test plan fully implemented; system configuration agreed with parties; system configuration documented; pilot rollouts will be conducted with small number of Optom practices before local rollout to all.	Reduced	Low	Choose an item.
There is a risk that data that has had identifiers removed could be manipulated in some way to re-identify individual people	No personal data is shared with the ICB, reporting on EeRS usage for contract management purposes; personal data can only be shared between nominated healthcare providers	Reduced	Low	Choose an item.
There is a risk that the Rego EeRS pathways are not implemented correctly or data quality is not assured and the system does not direct the referral correctly.	Sufficient testing and sign-off process (see risk above) will ensure pathways are correct and working effectively. Data must be correct in the source system; check with NHS spine to ensure data quality; pilot rollouts will be conducted with small number of Optom practices before local rollout to all.	Reduced	Low	Choose an item.
There is a risk that patient data held by the Optometrist cannot be matched to the Spine and so cannot be processed further in Rego EeRS and patient referral cannot take place.	Exception process to be agreed, to revert to manual direct referral to Provider.	Eliminated	Low	
Independent Opticians may not yet have a GOS contract with the ICB, or DSPT, or ICO registration.	ICB to put in place GOS contracts. Use of Rego as NHS system requires completion of DSPT. ICB to require all Optoms to complete. ICB to ensure checklist of compliance is	Reduced	Low	Choose an item.

	given to all Optoms including DSPT, ICO registration and NHS mail.			
Risk of insufficient audit trail of events such as inappropriate access: Currently each Optician Practice has one login, then Optician selects name from given list of opticians assigned to that practice (opticians may work for more than one practice.	NEC has committed to providing individual logins for each optician – this needs to be confirmed as implemented by ICB project manager.	Reduced	Low	
<b>5.3</b> <b>What if anything would affect this piece of work?</b> Each Controller must agree to use the Rego EeRS therefore in order for the electronic referral system to be effective there needs to be enough take-up by the community Optometrists.				
<b>5.4</b> <b>Please include any additional comments that do not fit elsewhere in the DPIA?</b> Click here to enter text.				
<b>6. Consultation</b>				
<b>6.1</b> <b>Have you consulted with any external organisation about this DPIA?</b> Yes  <b>If yes, who and what was the outcome? If no, detail why consultation was not felt necessary.</b> LOCSU and Local Optical Committee have been consulted for input to IG requirements				
<b>6.2</b> <b>Will you need to discuss the DPIA or the processing with the Information Commissioners Office?</b> (You may need the help of your DPO with this) No  <b>If yes, explain why you have come to this conclusion.</b> Click here to enter text.				
<b>7. Data Protection Officer Comments and Observations</b>				
<b>7.1</b> Comments/observations/specific issues	Each Controller to complete			
<b>8. Review and Outcome</b>				
<b>Based on the information contained in this DPIA along with any supporting documents, you have determined that the outcome is as follows:</b> B) There are further actions that need to be taken but we can proceed  <b>If you have selected item B), C) or D) then please add comments as to why you made that selection</b> There is a need for the DPIA for this project to be in place, but it is recognised that further actions are still required. The project can proceed but the DPIA must be reviewed on a regular basis and updated as necessary.				

**We believe there are**

A) No unmitigated or identified risks outstanding

**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**

<b>Residual risks and nature of potential impact on individuals.</b> (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)).	<b>Likelihood of harm</b>	<b>Severity of harm</b>	<b>Overall risk</b>
There is a need for the DPIA for this project to be in place, but it is recognised that further actions are still required. The project can proceed but the DPIA must be reviewed on a regular basis and updated as necessary.	Possible	Significant	Medium
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.

<b>Additional measures you could take to reduce or eliminate residual risks identified as medium or high risk above (B and C)</b>				
<b>Risk</b>	<b>Options to reduce or eliminate risk</b>	<b>Effect on risk</b>	<b>Residual risk</b>	<b>Measure approved (SIRO)</b>
There is a need for the DPIA for this project to be in place, but it is recognised that further actions are still required. The project can proceed but the DPIA must be reviewed on a regular basis and updated as necessary.	Review DPIA on a regular basis and update as necessary	Reduced	Low	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.

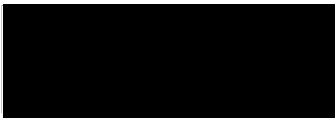
Signed and approved on behalf of Buckinghamshire Oxfordshire and Berkshire West Integrated Care Board

Name: [REDACTED]

Job Title: Data Protection Officer



Signature:



Date: 20/03/2024

Signed and approved on behalf of

Name:

Job Title:

Signature:      Date:

**Please note:**

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

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.](#)