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 **profiling or automated decision-making** to make significant decisions about people or their access to a service, opportunity or benefit;	☐
Process **special-category data or criminal-offence data on a large scale**;	☐
Monitor a publicly accessible place on a large scale;	☐
Use **innovative technology** in combination with any of the criteria in the European guidelines;	☐
Carry out **profiling** on a large scale;	☐
Process biometric or genetic data in combination with any of the criteria in the European guidelines;	☐
Combine, compare or match data from multiple sources;	✓
Process personal data **without providing a privacy notice** directly to the individual in combination with any of the criteria in the European guidelines;	✓
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;	☐
Process **children's** personal data for profiling or automated decision-making or for marketing purposes, or offer online services directly to them;	☐
Process personal data that could result in a **risk of physical harm** in the event of a security breach.	☐

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;	✓
Plan to do evaluation or scoring;	✓
Want to use systematic monitoring;	✓
Process sensitive data or data of a highly personal nature;	☐
Processing data on a large scale;	✓
Include data concerning vulnerable data subjects;	✓
Plan to use innovative technological or organisational solutions;	✓

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 :	16/01/2026
Title of the activity/processing:	Use of iGPR (Classic Service) for requests for information
Who is the person leading this work?	Navaira Mylecent
Who is the Lead Organisation?	Bret Stevenson
Who has prepared this DPIA?	Mike Cottam – IG Consultant (SCW CSU)
Who is your Data Protection Officer (DPO)?	Laura Taw
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).	The iGPR Electronic Reporting Solution provides GP Practices a solution to manage Subject Access Requests (SARs) under UK GDPR *and other requests for information* that are received from patients and third parties. The solution integrates directly with the practice clinical system (both TPP SystmOne and EMIS respectively). Several variations of the service exist for the practice to consider, each with slightly different processing methods, either through the regular 'classic' iGPR service or the 'Managed Service' (an end-to-end service managed entirely by iGPR personnel). **This DPIA will only cover the 'Classic' service (which includes both the free version and the Premium version of iGPR).** **Please use this link to establish the different services available:** **I'm a GP | iGPR** **A separate DPIA has been produced for practices looking to utilise the 'Managed Service' version of iGPR.** With the 'Classic' service, the practice can opt to manage all requests they receive directly, feeding them into iGPR as desired. This can then be worked on by the practice staff in isolation, using the iGPR software. The practice can review, collate and redact large amounts of information from within a patient's medical record as part of consideration for disclosure. Additional functionality exists within iGPR to facilitate requests for information from third party organisations (e.g. DWP, DVLA, insurance companies, the British Armed Forces). iGPR has in place contractual agreements with a number of different entities facilitating requests to be sent to the practice *via* iGPR systems. For the 'classic' service, the practice can then process those requests for information as they see fit within the iGPR system. In instances involving third party requests, if the patient has indicated that they would like to have sight of the report/output prior to it being shared with the third party, there is a 'copy to patient' function within iGPR which can facilitate this. An email is then automatically sent to the patient from iGPR which gives them the option to accept or reject the document. The patient can then contact the practice directly if they have any questions or concerns.

Are there multiple organisations involved? (If yes – you can use this space to name them, and who their key contact for this work is).	Park Crescent Health Centre iGPR Technologies Ltd (iGPR) Redcentric Ltd Acronis Ltd
Can you think of any other Key Stakeholders that should be consulted or involved in this DPIA? (If so then include the details here).	Click here to enter text.
Detail anything similar that has been undertaken before?	iGPR DPIA v4.2_Redacted 1.pdf

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

1.1.

What data/information will be used? Tick all that apply.	Tick or leave blank	**Complete**
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)	✓	1.2 but speak to your IG advisor first
Pseudonymised Data	☐	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	☐	Consider if a DPIA is appropriate
Other	☐	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**
	☐
Why are you relying on consent from the data subject? Appropriate consent must be given by the data subject either to a third party acting on their behalf (explicit) or to the GP practice to access their medical records (implied). Data subjects are not expected to consent to the use of iGPR as a tool for managing requests for information	
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 (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).	**Tick or leave blank** ☐
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 (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** ✓
Identify the legislation or legal obligation you believe requires you to undertake this processing. UK GDPR (Article 15)	
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** ☐
How will you protect the vital interests of the data subject or another natural person by undertaking this activity? Click here to enter text.	
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** ✓
What statutory power or duty does the Controller derive their official authority from? Click here to enter text.	
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** ☐
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** ✓
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** ☐
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** ☐
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** ☐
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 (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** ☐
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 (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** ☐
j) PROCESSING IS NECESSARY FOR ARCHIVING PURPOSES IN THE PUBLIC INTEREST, SCIENTIFIC OR HISTORICAL RESEARCH PURPOSES OR STATISTICAL PURPOSES IN ACCORDANCE WITH ARTICLE 89(1) 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. (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** ☐

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).

Name of Organisation	Role
Park Crescent Health Centre	Sole Controller
iGPR Technologies Ltd	Processor
Redcentric	Processor
Acronis Ltd	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?

Personal data relating to the patient as featured within the medical record. This includes basic identifiers such as name, DOB, Address, NHS no., but will also likely extend to various special category (health) data such as, but not limited to: physical/mental health conditions, diagnoses, medical operations and procedures, allergies and medications, discharge summaries and hospital letters.

Other special category data that may feature on a patient record such as nationality, race, ethnicity, religion, genetic or biometric data and data concerning sex life and/or sexual orientation

Data processed through the iGPR solution will be located on servers situated within the iGPR data centre hosted by Redcentric in the UK.

When the GP practice receives the request, they are responsible for checking all relevant consent/authority to act is in place and that the patient is indeed registered at their practice. They can then use iGPR to generate the report and approve any pre-set redactions/apply their own additional redactions if required.

In all instances, it is expected that the GP practice will review the final report to ensure that there will be no harm caused to the patient or any other individual upon release.

In situations where requests are received via iGPR directly from third parties acting on behalf of individuals, iGPR will let the practice know as soon as possible and the practice can then respond as they see fit. This can either be separately or back via iGPR if desirable.

In these instances, it may be that individual data subject has indicated that they wish to have sight of the final report prior to disclosure. This will be facilitated through the 'Copy to Patient' function within iGPR which will result in a notification email/text being sent to the patient to advise them the report is ready to view. Patients can then accept or reject the report and discuss with the practice if necessary.

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)

Clinical records

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

Practices will ensure that their privacy information for patients makes it clear that they rely on iGPR as a third-party service to process their SARs.

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.

- All data processed by iGPR Technologies Ltd will be hosted securely within Redcentric data centres (London UK) within a private network
- Any data transfer which takes place is encrypted to AES256 encryption requirements, secured both in transit and at rest.

Commented [SW1]: How does GP practice know that iGPR has received a request and at that stage can they have control over the information released?

Commented [SW2]: How are we satisfying CLDC and what is legal basis for sharing info with iGPR? Whose responsibility is it to obtain consent where its appropriate?

Commented [SW3]: I thought the patient provided their explicit consent in written format to enable SAR or AMRA to be processed?

Commented [MC4R3]: I have understood it to be the case that a controller does not need to seek *explicit* consent for a SAR - the fact that the request is being made is *implied* consent - i.e. the requestor is giving permission for the organisation to access their information in order to process the request. The organisation can seek *explicit* consent if they wish, but are not obliged to?

In this instance, it is the practice using a tool to process a request, access by a 3P is not a default

Commented [SW5]: Mentions encryption in Section below

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.

Responding to requests for information does not necessarily amount to the provision of direct care. It can in some circumstances be a legal requirement on the practice (UK GDPR)

1.10.

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

Unknown - non-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.)

By e-mail
Electronic form
Face to face - in person
Choose an item.
Choose an item.

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

Subject Access Requests can be made verbally or through written means. Requests can be received directly by the practice or by iGPR

1.12.

How will you edit the data?

Data will be extracted by staff from the practice's clinical system as copy, any appropriate redactions applied before disclosure

1.13.

How will you quality check the data?

GP practice is responsible for ensuring that the correct patient information is retrieved from the corresponding patient record before disclosure. IGPR will prompt multiple checks on the data too to help support this.

Commented [SW6]: Could this relate to correct patient being selected? Or appropriate information released?

1.14.

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

Yes

If yes include in the risk section of this template. In the event that an individual objects to the use of iGPR as a tool for processing a request for information, then the practice must ensure there is an appropriate process in place to follow which reverts to manual processes.

Commented [MC7]: Practice to add a risk to revert to manual means of processing in the event of iGPR service disruption/unavailability/error

1.15.

What training is planned to support this activity?

All applicable staff have access to appropriate training on the use of iGPR software. Weekly webinars take place and 121 training is available with iGPR experts if required, alongside a 9-5pm helpdesk

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).

- GP practice receives request for information from data subject or data subject representative (third party) *N.B – request can come through to practice directly or via iGPR if coming from third party which has contract with iGPR - iGPR will email practice to notify them accordingly.*
- Information extracted by practice staff member from clinical system and processed within iGPR solution (hosted on servers within Redcentric (UK based) data centre)
- Report produced as part of response to requestor
- Output is reviewed by practice (ideally by a clinical member of staff to ensure no third-party data or potentially harmful/distressing information is released
- (If applicable) report shared with the patient to give them prior sight before sharing with third party organisation (insurance company/DWP/Navy etc.)
- Disclosure of information is made to requesting party via iGPR system

2.3.
What data/information are you planning to share?
Relevant (identifiable health) information from the patient's medical record that falls within the scope of the request that has been made

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?
iGPR Technologies Ltd

2.6.
Why is this data/information being shared?
To enable practices the ability to comprehensively review and redact information that is due to be disclosed to a patient or a third party in line with relevant legislation

2.7.
How will you share it? (Consider and detail all means of sharing)
iGPR has direct system integration with common GP practice clinical systems, including EMIS and TPP SystmOne

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?
N/A – see section 3.10

2.9.
What reports will be generated from this data/information?

Commented [SW8]: Please clarify which data flow relates to which service? And provide further details regarding the process - needs to be written from GP practice perspective rather than iGPR view

Commented [SW9]: LH believes practices can receive electronic requests directly from IGPR partners?

Commented [SW10]: As above how does GP practice get notified of this request?

Response report generated to be shared with requestor

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.

iGPR Technologies Ltd - Beasleys Farm Upper Gambolds Lane Stoke Prior Bromsgrove Worcestershire B60 3EZ

Redcentric Solutions Ltd - Central House Beckwith Knowle Otley Road Harrogate North Yorkshire HG3 1UG

Commented [SW11]: Space removed!

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
iGPR Technologies Ltd	Yes	ZA548217
Redcentric Solutions Ltd	Yes	ZA010053
Acronis Limited	Yes	ZA562856
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.

Commented [SW12]: Added

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
iGPR Technologies Ltd	DSPT, DPA Cyber Essentials Plus – Cert no: **117b1f02-33ee-4cac-a9c6-1bcfb4e874bf** Expiry date 01/08/2026

Redcentric	GDPR compliant contract and SLA with iGPR, DSPT, NHS Digital verified supplier of Health and Social Care Network (HSCN) Interoperable Network Services, ISO9001 / ISO10000 / ISO27001 Cyber Essentials Plus – Cert no: **eacf9619-51c6-4294-bf31-e87af09dd4b6** Expiry date 01/10/2026
Acronis	Cyber Essentials Plus – Cert no: **58750c61-e383-4da4-984b-7c3e12f1194d** Expiry date 29/11/2025
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.

Commented [SW13]: Updated information

Commented [SW14]: What role does Acronis have? Should they be included in all 3rd party info above?

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
iGPR Technologies Ltd	8KG24	24/25 Standards Exceeded	12/06/2025
Redcentric	YGMAP	24/25 Standards Exceeded	30/06/2025
Acronis Limited	N/A	N/A	N/A
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).

- iGPR uses a closed API to integrate with the relevant GP practice clinical system.
- Any data transfer which takes place is encrypted to AES256 encryption requirements, secured both in transit and at rest.
- All data processed within iGPR Technologies Ltd will be hosted securely within Redcentric data centres (London UK) within a private network
- Patient access to data goes through a two-factor authentication process via a secure URL link
- All systems and data held within Redcentric data centre are backed up daily using Acronis, a cloud based solution with the back up data being stored physically at separate London based Redcentric data centre. (See iGPR DPIA for more details on back ups)

3.6

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

The EMIS/TPP audit will show each point that the iGPR app has accessed the clinical system (date and time stamped) so that it is possible for practices to monitor all access to patient records by the iGPR App. This audit may be reviewed by the GP surgery at any point should there be any issues or concerns raised.

The practice is in full control of what (patient) data is added to/processed within the iGPR software

3.7

Is there any use of Cloud technology?

Yes

If yes add the details here.

Cloud based back up solution – Acronis (See 3.5 above)

3.8
What security measures will be in place to protect the data/information?
See 3.5 above

Is a specific System Level Security Policy needed?
Choose an item.

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?
GP practice is recommended to ensure that an appropriate Data Processing Agreement is in place with iGPR

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).
GP practice must ensure that their privacy notice is updated to reflect the fact that data will be shared with/accessed by iGPR Technologies Ltd for the purpose of processing requests for information. This should also point patients to iGPR's own privacy policy too where possible

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).
iGPR will support practices in managing their individual rights requests in line with the terms of the Data Processing Agreement

4.3
How long is the data/information to be retained?
All information kept within the GP practice clinical record to be managed in line with the NHS Records Management Code of Practice.

If a report has been started by the practice but the processing has discontinued for any reason, it will remain live on the iGPR system for a maximum of 180 days before expiring if not completed or rejected.

Completed reports are retained for a period of 14 days on the iGPR server after successful delivery to the requestor, after which the data is deleted with the exception of a metadata stub containing the Insurer's policy number/Solicitor's/Government Department Case File ID and date stamp and whether the request was accepted or rejected by the GP. This metadata is held by iGPR for the duration of the contract for audit and quality improvement purposes.

Reports remain available to patients/third parties for review at their request via a secure download portal for a maximum period of 90 days. After which point, they would need to contact the practice directly.

4.4
How will the data/information be archived?
See above

4.5
What is the process for the destruction of records?

See above

4.6

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

All information will be destroyed

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**
Incorrect data being extracted from clinical system	Possible	Significant	Medium
Incorrect patient data being provided at point of request	Possible	Significant	Medium
Clinical risk of harm or distress to patient if GP practice does not check report prior to disclosure	Possible	Significant	Medium
Data loss or hack of iGPR systems	Possible	Significant	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)**
Incorrect patient data being provided at point of request	iGPR will force multiple checks on data provided with the data held on the clinical system to ensure that incorrect data is not provided back to requestor	Reduced	Low	Choose an item.
Clinical risk of harm or distress due to failure to check	GP practice must actively review records prior to disclosure as per their responsibilities as controllers.	Reduced	Low	Choose an item.
Data loss/hack	Robust technical security measures and encryption in place to protect data and keep secure while stored in Redcentric data centres. In the event of total iGPR	Reduced	Choose an item.	Choose an item.

	system outage, the practice will be able to revert to manual processing methods to facilitate a response to request.			
				Choose an item.

5.3
What if anything would affect this piece of work?
Click here to enter text.

5.4
Please include any additional comments that do not fit elsewhere in the DPIA?
Click here to enter text.

6. Consultation

6.1
Have you consulted with any external organisation about this DPIA?
Choose an item.

If yes, who and what was the outcome? If no, detail why consultation was not felt necessary.
Click here to enter text.

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)
Choose an item.

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**	Click here to enter text.

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:
B) There are further actions that need to be taken but we can proceed

If you have selected item B), C) or D) then please add comments as to why you made that selection
The DPIA has identified routine mitigating actions and governance controls. These do not prevent the project from proceeding.

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**

Unauthorised access to personal data via dashboards	Remote	Minimal	Low
Use of personal data beyond the original intended purpose	Possible	Minimal	Low
Data inaccuracy leading to incorrect conclusions	Possible	Minimal	Low
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 Click here to enter text.

Name: Navaira Mylecent

Job Title: IG Lead

Signature: NM

Date: 16/01/2026

Signed and approved on behalf of

Name: Bret Stevenson

Job Title: Practice Manager

Signature: BS Date: 16/01/2026

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.