Data Privacy Impact Assessment (DPIA)

Contact details	
DPIA Lead	Guy Bridgewater
Role	Senior Information Risk Owner
Organisation/Department	iGPR Technologies Ltd (iGPR)

Question	Response	Guidance
Name of System/Process	iGPR Managed Service Solution	
Name of Data Controller	GP Surgery	This is the 'owner' of the data that will be processed in the course of the activity covered by this impact assessment
Name of Data Processor (if different from above)	iGPR Technologies Ltd (iGPR)	This is the organisation processing data on behalf of the data controller in line with UK-GDPR Article 28 provisions
Purposes of System/Process	The iGPR Managed Service Solution will enable GP surgeries to devolve to iGPR Technologies Ltd (iGPR), the administrative workload involved in responding to requests for medical and other reports based on the patient medical record from Requesting Third Parties (RTP) with informed patient consent in place, and Data Subject Access Requests (DSARs) received from Requesting Third Parties acting on behalf of the patient or directly from the patient themselves. The Basic, Sars Pro and Premium iGPR product (referred to throughout this DPIA as 'DPIA product') offers both GP surgeries and RTPs an efficient and secure method of transferring personal and special category information at the	This needs to be a description of what the project or process will involve. Explain broadly what the project/ processing aims to achieve, what the benefits will be to patients, the organisation, to individuals and to other parties. Is the data to be collected to be used only for a specified purpose – e.g., to provide healthcare, facilitate payment for activities, improve services, clinical audit?

Data Privacy Impact Assessment (DPIA)

Question	Response	Guidance
Purposes of System/Process *(continued...)*	request of patients, and GP surgeries an effective method for responding to DSAR requests. This supports GP surgeries to demonstrate compliance with the requirements of the UK-General Data Protection Regulations (UK-GDPR) and the Data Protection Act (2018) (DPA) – the iGPR solution is API based and integrates with the specific Electronic Patient Record (EPR) used by the GP surgery. A separate DPIA is in place to cover the iGPR product (see embedded documents below). Historically, the full administrative process involved in responding to requests for medical reports and DSARs has been managed by GP surgeries in house, utilising the functionality of the iGPR product (where this is in place) and undertaking the operational processes to accept, initiate and complete the reporting process back to patients themselves and/or the RTPs. Where iGPR is not in place, GP surgeries have customarily carried out the entire process manually. The iGPR Managed Service offer which is covered by this DPIA will allow surgeries to devolve the processing and reporting process for specified reports and DSARs, to iGPR Technologies Ltd, thereby removing a significant proportion of these operational and administrative tasks from the GP Surgery workflow and consequently delivering savings in both staff time and staff costs. Report requests will be picked up directly by iGPR where the Managed Service is in place and in instances where a report request comes firstly to the Practice or where a DSAR is received by the Practice, will allow GP surgeries where the iGPR product is installed, to readily direct the request to the iGPR Managed Service using the iGPR desktop app already available to them. If a request for a medical report or DSAR is received into a GP surgery in paper or electronic format and not through the	

Data Privacy Impact Assessment (DPIA)

Question	Response	Guidance
Purposes of System/Process *(continued...)*	existing iGPR portal, the surgery may still use the iGPR product to forward the request to the iGPR Managed Service.	
What Legal bases are to be used to process any data collected?	In offering the Managed Service, iGPR is acting as a data processor and will process data under the legal basis identified by the Practice as data controller. The legal basis identified by practices may vary depending on the interpretations applied by them and depending on the nature of the processing (e.g., it will be different when processing a DSAR compared to an insurance report) but may include: UK-GDPR Article 6.1.a – Consent UK-GDPR Article 9.2.a – Consent UK-GDPR Article 6.1.e – Public Task UK-GDPR Article 6.1.f – Legitimate Interests UK-GDPR Article 9.2.h – Provision/treatment/management of healthcare	Where there will be processing of any personal information, a GDPR Article 6 Legal basis will need to be identified; for any processing of special category information, a GDPR Article 9 legal basis will need to be identified. You can have an Article 6 legal basis without an Article 9 legal basis (i.e., if the processing is to include just personal information), but you cannot have an Article 9 legal basis without identifying an Article 6 legal basis (because special category information falls under the 'umbrella' of personal information. Your IG&C Lead will be able to help you determine the correct legal basis.
Which Data Subject Rights apply to this/these legal basis/bases and how will these be met?	As a data processor, iGPR Technologies Ltd will assist the GP surgery to meet all relevant data subject rights and will inform the GPs as data controllers should any request be made by a data subject directly to iGPR outside the specific agreed scope and terms of the Managed Service Agreement and iGPR will not attempt to fulfil such requests themselves under any circumstances. As the data to be transferred and/or shared between controllers is healthcare data, the following data subject rights will apply: Right to Information Right to Access (with potential redaction as per Schedule 3 of	Data Subject Rights Available: Right to Information Right to Access Right to Rectification Right to Withdraw Consent Right to Object Right to object to Automated Processing Right to be Forgotten

Data Privacy Impact Assessment (DPIA)

Question	Response	Guidance
Which Data Subject Rights apply to this/these legal basis/bases and how will these be met? *(continued...)*	the Data Protection Act) Right to Rectification (in line with relevant healthcare regulatory requirements) Right to Object (in line with relevant healthcare regulatory requirements) Right to object to Automated Processing (if this should take place) Right to Data Portability	Right to Data Portability (not all rights are applicable in healthcare settings but all opportunities to prioritise the rights and wishes of the data subject with regard to the processing of their data should be considered)
In which locations does the processing take place and who is impacted by the processing?	Data processed by iGPR in support of this activity will be located on servers situated in the iGPR data centre hosted by RedCentric in the UK. RedCentric is an NHS Digital verified supplier of Health and Social Care Network (HSCN) Interoperable Network Services. No data is transferred or processed outside the UK at any point by iGPR. iGPR staff working to support the Managed Service offer are based in the UK. The processing described will positively impact GP surgeries by reducing the administrative and operational burden involved in processing medical reports and DSARS. The processing has the potential to positively impact patients as data subjects by introducing workflow efficiencies into the process of meeting requests and ultimately speeding up the delivery of medical reports and DSARs to the relevant requestor.	Where is the data to be processed? This will include any manual processing and any electronic processing. (Processing includes but is not limited to: any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction) Please list locations for each aspect of processing identified. If the data is to be processed outside the UK, describe the mechanisms and

Data Privacy Impact Assessment (DPIA)

Question	Response	Guidance
In which locations does the processing take place and who is impacted by the processing? *(continued...)*		security in place to safeguard the data? Has any data transfer outside the UK been flagged and approved by the Data Protection Officer for the company?
Describe the context of the processing	iGPR is committed to supporting GPs to safely and securely discharge their responsibilities when responding to requests for information from a patient's medical record whether this is from a third party acting for or on behalf of the patient, or the patient themselves. The Managed Service offer which is the subject of this DPIA is designed to provide an end-to-end solution for GPs. It will provide many of the administrative and operational functions currently delivered in-house by surgeries and will utilise the iGPR product functionality (see separate DPIA for this – embedded below) to process, generate and resolve patient approved requests for information. Once the Managed Service is activated at a Practice, the Practice, having firstly complied with their obligations under the Managed Service Agreement, report requests will come directly to the Managed Service and the Practice will direct any additional report requests/DSARs (as described above) to the Managed Service via the iGPR application and the requested work will be carried out by iGPR staff within the terms of the Managed Service Agreement. A key aspect of the iGPR Managed Service is to support the GP as data controller to clearly discharge their obligations under the data protection legislation, and robust operational processes	What is the nature of the relationship between the organisation and the data subject? How much control will the data subject have over the processing? Would they expect their data to be used in this way? Do the data subjects include children or other vulnerable groups? Have there been any prior concerns over this type of processing, or security flaws? Is the processing novel in any way? What is the current state of technology in this area if appropriate? Are there any current issues of public concern that you should factor in?

Data Privacy Impact Assessment (DPIA)

Question	Response	Guidance
Describe the context of the processing *(continued...)*	are established by iGPR to ensure that functions carried out by iGPR staff to support the Managed Service, are aligned to the data protection legislation at all points. Additionally, the iGPR Managed Service staff are recruited specifically from the Healthcare sector where they will have gained commensurate skills and experience to ensure that they fully understand the risks and requirements of effective DSAR and report processing particularly in a healthcare setting. The iGPR solution has been developed as a digital solution by iGPR Technologies Ltd in line with NHS Digital information governance and data protection standards and has been used by both increasing numbers of RTPs and GP surgeries since 2015. There are currently no security flaws identified in the technology used to provide this solution.	
What personal data will be processed?	Personal data processed via the iGPR solution includes: • Name • Date of Birth • Address • NHS Number • Patient contact telephone number • Patient email address	Personal Data means forename, surname, date of birth, age, gender, address, postcode, NHS Number, another identifier (e.g., Hospital Number), racial or ethnic origin, physical or mental health condition Please list which Personal Data will be processed. Will the dataset include financial data or any other categories of data?
What Special Category data will be processed	Special Category data processed as part of the iGPR Managed Service solution and utilising the iGPR product (Basic/SARs Pro/Premium) may include (as appropriate to the nature of the request being serviced):	Special Category data means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information

Data Privacy Impact Assessment (DPIA)

Question	Response	Guidance
What Special Category data will be processed *(continued...)*	• Physical/mental health condition diagnoses and conditions (current and previous) • Symptoms. • Operations and medical procedures. • Medications and prescriptions issued. • Allergies and reactions to medication. • Results of investigations such as blood tests and X-rays • Letters and discharge summaries. • Test results. • Clinical reports and letters. • Recorded patient consultations and some coded diagnostic information. • Details of services received. • Details of lifestyle and social circumstances. • Details of nationality, race and/or ethnicity. • Details of religion. • Details of genetic data or biometric data. • Data concerning sex life and/or sexual orientation.	about a person's health status or any data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation Please list which Special Category Data will be processed.
Are individuals explicitly informed about why their personal data is being collected and how it may be used?	Data subjects must be informed by any Requesting Third Party in their onboarding and transparency notifications, why particular information is required by them and, where the RTP is using the iGPR Connect portal or iGPR API , that the information will be processed by iGPR in order to facilitate the	If data collection/processing standards and procedure are not transparent, controllers/data subjects may not trust the processing organisation and refrain from sharing

Data Privacy Impact Assessment (DPIA)

Question	Response	Guidance
Are individuals explicitly informed about why their personal data is being collected and how it may be used? *(continued...)*	requesting and provision of relevant medical information from their GP. Where a GP surgery uses the iGPR product and the iGPR Managed Service solution, this must be included in the Privacy Information made available to patients by the surgery. Where the practices are using Consent as the legal basis to process the data required, their Privacy Information must include clear and accessible options for patients who do not wish their data to be processed by iGPR (either via the solution and/or the Managed Service where this applies). If a patient has requested that they have sight of any information generated as a result of a sanctioned request before it is made available to an RTP, the iGPR software will register that such a request has been made and iGPR Managed Service staff will be prompted to use the 'Copy to Patient' function within iGPR to notify the patient that the report will be available for them to view using the secure portal details provided in the email/text notification before the information is made available to the RTP (see below for description of technical security in place). Patients are given up to 21 days to review insurance reports in line with current AMRA applicable legislation. iGPR maintains its own Privacy Notice where it acts as a Data Controller out of scope of this DPIA.	their personal data. Notification should be via a Privacy Notice and may also be via correspondence, leaflets and verbal communication.
What is the process for deleting the data?	Medical records held by GPs are subject to the Data Retention Schedules in line with the Records Management Code of Practice 2020. The full data packet processed by iGPR utilising the Managed Service is retained by iGPR for the period it takes iGPR to respond to the request and the delivery of any data to the	Is it necessary to keep all of the data that is being processed? Is it subject to any Data Retention Schedules in line with the Records Management Code of Practice 2020?

Data Privacy Impact Assessment (DPIA)

Question	Response	Guidance
What is the process for deleting the data? *(continued...)*	designated requesting body (incorporating any period of time where the data is being viewed by the patient themselves) or the patient themselves (if a DSAR has come directly from the patient). DSARs will be processed within the period laid out in current data protection legislation. In the rare instances where this may not be possible for reasons such as delay in response to queries from the requestor, the Practice will be notified to allow the patient/requestor to be informed. If a report has been initiated by the Managed Service but the processing has discontinued for any reason, it will remain live on the iGPR system for a maximum of 28 days before expiring if not completed or rejected. The maximum length of processing is therefore 28 days. Medical information (completed reports/DSARs) is retained for a period of 14 days on the iGPR server after successful delivery to the RTP or patient themselves, after which the data is deleted with the exception of a metadata stub containing the Requestor ID number/Solicitor's/Government Department Case File ID and date stamp and whether the request was processed to completion or rejected by the iGPR Managed Service on behalf of the GP client. This metadata is held by iGPR for the duration of the contract for audit and quality improvement purposes. Outside of the processes defined above, no person identifiable data is retained.	Are there procedures for reviewing how long data should be retained? Is there a policy, procedure, rationale for archiving personal information? What information will be retained for auditing purposes? How will this be minimised?
Describe the information workflow	A request for information will be received by the GP surgery. This may take the form of a medical/other report request made by a Third party acting for or on behalf of a patient (requesting information from some or all of the patient medical record), or it may be a DSAR made by the patient themselves or a third party acting on their behalf. A DSAR is a specific legal instrument under the data protection legislation	The collection, use and deletion of personal data should be described, and it may also be useful to refer to a flow diagram or another way of explaining data flows. How will this information be added

Question	Response	Guidance
Describe the information workflow *(continued...)*	and (together with formal evidence of patient consent where this applies) may range in scope from a limited and specified data set to a broad request for the patient record. The first stage point for any request to the iGPR Managed Service, will be to ensure any request is assessed by the practice to ensure relevant consent is appended or, in the case of a patient originated DSAR, that relevant identity checks are validated by the practice. This will permit the iGPR Managed Service to process the request safely while meeting the rights of patients as data subjects. Where report requests are sent directly to the Managed Service, initial checks are carried out by the Service personnel and are required by the iGPR product to ensure the validity of the request. Any queries are returned to the Practice for additional checking if necessary. Once these checks have been carried out at the GP surgery, the GP user will use the Managed Service function on their iGPR desktop application to forward the request and any associated documentation to the Managed Service. The iGPR Managed Service personnel will use the iGPR product and process requests for reports and DSARs against a clearly defined operational algorithm. These personnel will be appropriately skilled and supported follow standard operating procedures to ensure that complex requests and DSARs are escalated to the iGPR DPO/Head of Governance &Compliance and/or Senior Management Team (SMT) depending on the nature of the query for assessment before release to the patient or requesting third party, or to be referred back to the GP surgery, as data controller, for further instruction/resolution. (See Process Flow embedded below).	to the high-level data flow capture process for this area? You should also say how many individuals are likely to be affected by the project.

Data Privacy Impact Assessment (DPIA)

Question	Response	Guidance
Describe the information workflow *(continued...)*	Where the request is accepted, the iGPR product will be used to interface with the specific patient record to compile a customised report to meet the request. As the iGPR product may only interface with the patient record once the user is logged into the specific practice electronic patient record system (e.g., EMIS, SystmOne, Vision), a generic 'iGPR User' account will be added to the clinical system of the respective practice for EMIS practices and for TPP and Vision, via the Managed Service dashboard. There is robust audit functionality within the clinical systems to mitigate against a lack of audit clarity regarding iGPR access to patient records. TPP have stated that: 'When using a third party integration[...]users may notice large numbers of retrievals in the Patient Retrievals and Printout audit listed against a single user. This is expected behaviour and is characteristic of the integration software using the associated API as it retrieves and discards patient records simultaneously in the background. Where an audit of record retrievals is being undertaken the presence of a retrieve and discard with the same time stamp can be used as evidence of an API transaction.' There is similar functionality in EMIS. Vision does not currently have this functionality but iGPR maintains its own audit of all access by its App to patient records and this can be shared with practices on request. Within the iGPR product environment, the specific user accessing any generic account to prompt a report, will be recorded and the access time stamped for security and audit purposes. This audit may be reviewed by the GP surgery at any point should there be any issues or concerns raised. iGPR Managed Service personnel will check the request received and if satisfied that all necessary consent is in place	

Data Privacy Impact Assessment (DPIA)

Question	Response	Guidance
Describe the information workflow *(continued...)*	and that the patient is registered with the practice, will use iGPR to generate the report using the iGPR product. The report will be reviewed by the Managed Service personnel using pre-set operational parameters and they will approve any pre-set redactions and make any additional redactions as necessary in line with the agreed operating parameters of the service specific to the practice. Any queries or issues beyond these parameters will be escalated to as described above, for review and action which may include referral back to the practice for further input/decision. If the patient has requested that they are given sight of the report before it is made available to the RTP, the iGPR Managed Service personnel will use the 'Copy to Patient' function within iGPR to send an email/text notification to the patient that the report is ready to view. The patient is afforded up to 21 days to view their report in line with AMRA requirements. When the patient has viewed the report (if they have requested this and agreed that it may be made available to the RTP) or when the report is completed by the iGPR Managed Service and the patient does not wish to see it, the iGPR Managed Service will make the requested report available to the RTP. DSARs made directly by the patient will be sent directly to the patient.	
Will the personal information be shared with or disclosed to other organisations?	The iGPR Managed Service will not disclose the data collected in the course of this processing to any other entity outside the patient themselves and the RTP (where patient consent is in place). The data held by the iGPR Managed Service and the iGPR product is held on servers at its secure data centre managed by RedCentric (formerly Piksel) based in London	Have the other organisation(s) provided written assurances that they will safeguard the information and not share it further? If they do share it with any sub-processors, who and where does this happen? How will the

Data Privacy Impact Assessment (DPIA)

Question	Response	Guidance
Will the personal information be shared with or disclosed to other organisations? *(continued...)*	in the UK. The data centre provider has no ability to read the data at any time. iGPR has a UK-GDPR compliant contract in place with RedCentric to ensure that iGPR Data processed by RedCentric is held securely and only processed in line with the contractual conditions between the two parties. A DPIA covering the processing carried out by RedCentric as a sub processor for the data collected using iGPR is in place.	information be shared? Does the other organisation have an adequate Data Protection Policy compliant with the GDPR? Does the other organisation complete a DSP Toolkit, have Cyber Essentials Plus or ISO27001 compliance? Is there a Contract/SLA or Confidentiality agreement in place? The contact must clearly state the respective responsibilities of both the Data Controller and Data Processor. If Consent is the legal basis identified for the processing, how/when will this be sought/captured/retained? If promotional videos, brochures or press stories have been developed, has any personal information been anonymised so that even if it were linked to other data, it would not be possible to identify the person?
What are the risks to the data subject?	Risks to data subjects may include actions taken by the Managed Service that result in incorrect data (e.g., incorrect patient) being provided to a RTP via iGPR. The validation of identities and consents will be carried out by GP practices as data controllers before the Managed Service is activated to process a report/DSAR. This responsibility will be clearly delineated for practices in the Managed Service Agreement which they will enter into with iGPR Technologies Ltd.	Explain what practical steps you will take to ensure that you identify and address privacy risks both now and in the future. Who should be consulted, internally and externally? Are individuals provided with the

Data Privacy Impact Assessment (DPIA)

Question	Response	Guidance
What are the risks to the data subject? *(continued...)*	To additionally mitigate such circumstances and any inherent risk, the iGPR product utilised by the iGPR Managed Service will force multiple checks on the data provided from the GP record to ensure that every possible step is taken to ensure that incorrect data is not provided to the RTPs via the iGPR solution (see below for technological provisions in place to reduce risks to data subjects wherever possible). Additionally, iGPR Managed Service personnel will work to explicit operational procedures to ensure that information is always processed in line with data protection legislation. A defined second level of escalation will be established as part of the MS model. The iGPR DPO/Head of Governance & Compliance/ SMT Lead will review all complex DSARs or other issues raised by MS Level 1 personnel, before the release of any data to either the patient themselves or a Requesting Third Party acting for or on behalf of the patient. Any issues or queries that cannot be dealt with by the Managed Service, will be referred back to the Practice to ensure that patient safety and privacy is supported at every point by the Managed Service There is a residual risk to data subjects resulting from external penetration of the iGPR data centre and the data held on iGPR systems as part of the contractual agreements between iGPR and clients/GPs. Security provisions as described below, are in place to mitigate such a risk.	possibility to access and correct their personal information? Can they request the deletion of some or all of their personal information where this is appropriate to the legal basis being used? Is it necessary to restrict access to data? If so, are these restrictions adequately defined and explained?
What technological and organisational security measures will be put in place to protect the data subject and their rights?	The technological security measures in place governing the iGPR product which will be used by the iGPR Managed Service, are contained in the iGPR DPIA which is embedded below. All data processed through iGPR is secured in transit and at rest using AES256 encryption requirement to NHS standards. iGPR data is held securely on servers in the RedCentric data centre located in the UK which are not web-facing and	What measures are in place to protect access to data (e.g. username/password, role-based access, NHS Smartcard, Secure Access Tokens) Are staff trained/reminded regularly to follow all security and governance policies and protocols when

Data Privacy Impact Assessment (DPIA)

Question	Response	Guidance
What technological and organisational security measures will be put in place to protect the data subject and their rights? *(continued...)*	access is only attained via the Health and Social Care (HSCN) network. HSCN is a private network rather than a secure network and it is the responsibility of the data provider (in this case iGPR) to ensure that the data that is transmitted via the network is securely encrypted. The RedCentric data-centre is UK hosted and meets the following accreditations: • ISO 9001 • ISO 10000 • ISO 27001 iGPR has a GDPR compliant contract and Service Level Agreement (SLA) in place with RedCentric that gives assurance that RedCentric provide every technical protection to iGPR data that is required to maintain the privacy and security requirements for the data processed. This includes assurance that all RedCentric staff who may be required to access the servers on which the iGPR data is held are appropriately vetted and trained and that regular audit of access takes place. A Managed Service Agreement (MSA) will be established between iGPR and any GP client wishing to use the service. This MSA will clearly set out the conditions for any processing iGPR will undertake to support the surgery to demonstrate compliance with all relevant data protection legislation as a data controller. iGPR has all relevant Information Governance and Data Security policies in place and these are regularly reviewed to maintain compliance with regulatory and statutory legislation and guidance. The organisation also completes an annual Data Security and Protection Toolkit (DSPT) submission to NHS Digital giving assurance of its compliance.	accessing data? Is annual training provided to all staff on good data protection and information security practices? If relevant, is NHSmail used or are e-mails encrypted? If so, what kind of encryption is used? Are there appropriate anti-virus and anti-malware solutions in place? Does the organisation have DSPT/ CyberEssentials/ISO accreditation in place?

Data Privacy Impact Assessment (DPIA)

Question	Response	Guidance
What technological and organisational security measures will be put in place to protect the data subject and their rights? *(continued...)*	All iGPR staff are trained on their responsibilities for maintaining the proper governance and protection of Information at Induction and annually and are required to maintain familiarity with all relevant Information Governance and Data Security policies and protocols during their employment. Additionally, staff working on the Managed Service will receive role specific training and follow a Managed Service Standard Operation Procedure (SOP) which will determine all actions required to deliver the Managed Service and will support compliance with data protection legislation at all points in the delivery process. iGPR has an Access Control Policy and Acceptable Use Policy in place to ensure that iGPR staff access to critical data systems is monitored and any anomalies flagged immediately to the Senior Management Team.	
Is the data regularly backed up and recoverable in the event of a failure?	iGPR systems and data held at the RedCentric data centre are backed up on a daily basis using Acronis, a cloud based solution and the backup data is stored physically at a separate London based RedCentric data centre. Additionally, iGPR runs its own MS SQL back-up scripts which write out to a SAN within the RedCentric iGPR environment and which allows rollback to any specific point in time within the last 24 hours. Back-ups are encrypted with AES-256 and the key for this encryption is unique to IGPR and consist of a combination of entire Virtual Machine backups and application specific backups for SQL data. Acronis takes nightly vSAN back-ups of all virtual instances (data, SQL and Transaction Logs).	Assurances must be made that data is properly backed up and restored at regularly intervals, whether the system is standalone or networked.

Data Privacy Impact Assessment (DPIA)

Question	Response	Guidance
Is the data regularly backed up and recoverable in the event of a failure? *(continued...)*	Back-ups are retained for 1 month Testing of Back-ups for data integrity and restoration capability takes place on a regular (6 monthly) rolling programme in order not to disrupt the continuation of business. Business continuity for the RedCentric Datacentre adheres to BS 25999-2:2007 for Business Continuity. Recovery plans are tested in accordance with BS 25999-2:2007 for Business Continuity. The datacentre conforms to ISO 20000 and 27001 incorporating a full Disaster Recovery operational plan.	
What happens in the event of a data breach or loss of data?	iGPR has a robust Security Incident Management Policy in place which defines the scope of potential security incidents (both internal and external) that may affect data processed as part of the iGPR Managed Service, together with actions to be taken by relevant personnel to both secure the data at the earliest opportunity and to inform relevant stakeholders (data controllers/the ICO/NHS Digital/patients themselves) of any suspected or actual data breach in line with current data protection legislation and all contractual obligations. iGPR staff supporting the Managed Service are required to raise concerns in an open and proactive manner to ensure that potential breaches may be avoided by speedy and pre-emptive action by the company.	What action will be taken if there is a data breach? Is there a requirement at contract level that any data processors inform the organisation at the earliest stage of a suspected or actual data breach? Have you considered some worst-case scenarios regarding what might happen if the personal data collected by your organisation was compromised or deleted either by accident or purposely? Are individuals informed if their personal data is lost, stolen or other compromised? Will any other organisations need to be informed?

Data Privacy Impact Assessment (DPIA)

Question	Response	Guidance
Consultation Process	iGPR Technologies has a large GP client base already using the iGPR product to meet the reporting requirements described in this DPIA. In a closed Facebook group consisting of more than a thousand of these clients, the prospect of an iGPR Managed Service, which can securely deliver the end-to-end offer and thereby reduce the administrative and operational tasks within practices, has received strong and positive endorsement. This iGPR Managed Service has been established as a result of multiple requests regarding the availability of such a service from iGPR, from existing GP surgery clients using the iGPR product	Describe when and how the views of relevant individuals will be/have been sought (or describe why this is not appropriate). Who else within the organisation needs to be involved? Do you need assistance from any sub-processors? Do you need to consult/have you consulted any information security experts or other experts?
Summary of the DPIA Outcomes	The iGPR Managed Service offer covered by this DPIA is assessed as being a robust and secure method for iGPR to support GPs to carry out the administrative and operational functions relating to requests for patient information using the iGPR product to produce such reports. iGPR is responding to an identified need and direct requests from GP clients for such a Managed Service. The existing security measures in the iGPR product, together with the internal procedural controls of the Managed Service will further embed the principles of data protection by default and design in the Service and appropriately mitigate any risks identified in this DPIA. Additionally, the escalation and oversight architecture of the Managed Service, gives further assurance that data subject rights are central to the processing carried out as part of the iGPR Managed Service. The iGPR DPO will be responsible for ensuring that any risks to data are quickly identified and mitigated by the protocols to be established for the secure running of the Managed Service.	List the key DPIA outcomes: Have you identified all risks and mitigating actions above? Who is responsible for integrating these outcomes back into the project plan and updating any project management paperwork? Who is responsible for implementing the solutions that have been approved? Who is the contact for any privacy concerns which may arise in the future?

Data Privacy Impact Assessment (DPIA)

Outstanding Risks to iGPR	Outstanding Risks to Data Subjects	Mitigations in Place	Residual Risk
No unmitigated outstanding risks			
	No unmitigated outstanding risks		

Risk Assessment Completed By:	
Name	Marie Cooper
Role	Head of Governance and Compliance
Date	August 2022
Version Number	2
Processing Entered onto Record of Processing Activities?	Yes
If No, please provide reasons:	
Outstanding Risks Entered into Risk Register?	No outstanding risks

Agreed by Data Protection Officer	
Comments/Issues identified	None
Name	Aga Edwards
Date	16/08/2022
Date of next review	August 2023