Section two (to be completed by the project lead and or team)

Privacy Impact Assessment Template

GP Repository for Clinical Care (GPRCC) Project – Direct Care

Reference number: v7.6

Date PIA completed: updated May 2018

The CCG **MUST** comply with the Data Protection Act 1998 and other legal requirements. The Privacy Impact Assessment (PIA) process assists by evoking a privacy by design approach to all projects/activities. PIAs are a tool which can help organisations identify the most effective ways to comply with their data protection obligations and meet individuals' expectations of privacy.

The PIA should be completed clearly and accurately as they may be published on the CCG's website (unless they contain commercially sensitive information) after being approved.

Stage 1

Project Summary:

Nottinghamshire CCGs support a centralised repository that allows a small subset of data to flow from GP, community, acute, and Local Authority systems, into the NHIS data warehouse. Collectively, these data form the "GP Repository for Clinical Care (GPRCC)". The scope of this PIA concerns use of these data for direct patient care only (including clinical audit). A separate PIA will consider any potential for secondary use of data which have been collected principally for direct care.

The typical scenarios for use of the data are in the planning and execution of Multi-Disciplinary Team (MDT) meetings. The data will be used to identify patients at risk of admission, for identifying community pathways that might prevent that admission and for identifying potential gaps in care (for example, by flagging patients who have a primary care diagnosis indicating severe COPD but who are not under the care of a community COPD team). Identifying patients at risk of admission will be partly done by risk stratification and partly by case discussion of patients with factors indicating higher risk (e.g. New York Heart Association status, COPD MRC dyspnoea scale).

Under the scope of this PIA, there will be no use of this data for any secondary purposes e.g. no use for commissioning, contracting or performance management. No new data collection will be required.

Data in the GPRCC will contain personal identifiers including name, NHS Number, date of birth, address, postcode, telephone number and date of death, which will be stored in pseudonymised form in a secure SQL environment (NHIS data warehouse). Where the patient name is not available from the GP system, it will be retrieved from the NHS spine using the Demographics Batch Service (DBS), supplied and accredited by NHS Digital. We have obtained approval from NHS Digital for the Data Management Team to have access to the DBS to ensure that data quality and attribution of patients to the correct Practices are maintained to a high standard. Where it is not possible to update patient names daily from the GP system (for example, where patients have moved out-of-area), these will be updated cyclically (every week or so) for as long as the record is retained by using the DBS. These measures ensure that our obligations to maintain accurate records and maximise clinical safety are met.

Where the NHS number is missing or may not be considered completely robust (for example, in data collected by Social Care), it will be necessary to supply the full name, postcode and date of birth to the DBS in order to determine the NHS number accurately.

To improve integration between Health and Social Care and to meet our obligations to data quality, a reverse flow from the GPRCC back to Social Care is proposed, returning accurate NHS numbers from the DBS for those patients whose details were shared by Social Care with an incomplete or inaccurate number.

Access to identifiable GPRCC data is exclusively via eHealthScope, which provides Role-Based Access Control. Only staff from General Practice and individuals nominated by them in the Local Care Teams (e.g. Care Delivery Groups) who are involved in the care of patients will be given access to re-identified data, given these staff have a 'legitimate' relationship with the patient.

System engineers in the Data Management Team at Rushcliffe CCG administrate eHealthScope and act as a Data Processor on behalf of GPs. Most of the time, they will only see pseudonymised data. However when extracts are taken from GP systems for upload to the GPRCC, the data will be clear. The first process run is the pseudonymiser, which polls the extract folder for new files and runs fully automatically. From that point on, there is no access to clear data.

Caldicott Guardian approval for the project has previously been given by Nichola Bramhall.

Data Processing contracts between each Practice and the Data Management Team will be in place before any data flows to and from a Practice. Each data flow will have a data sharing agreement between the Provider and GP Practices. All contracts and agreements will be available for practices to view in eHealthScope. Amendments to the Data Processing Contracts will also be managed via eHealthScope.

As described above, the technologies being used are existing systems on N3/secure infrastructure, for example: SystmOne, EMIS Web and the Microsoft SQL Server data warehouse and eHealthScope, which are hosted on secure NHIS infrastructure. eHealthScope is web-based software built in a web browser such as Internet Explorer that is accredited. Data is stored in SQL Server which is accredited. Leicestershire Health Informatics Service (LHIS) have run an initial security PEN audit with satisfactory results, and further cycles of vulnerability testing are planned for soon after eHealthScope has been migrated to new servers.

Please see the supporting data flow diagram in Appendix B, illustrating the high level data flows, organisational responsibilities, and the secure pseudonymisation and delivery mechanisms.

List of attachments: *(e.g. project initiation document or proposal)*	**Page**
Project Initiation Document	
Copy of HSCIC approval email for DMT to access Demographic Batch Service (DBS)	

Brief description of the data affected *(is this personal confidential data e.g. health information, criminal records or other information people are likely to consider as private?):*

The processing, which focussed initially on patients classed at risk of an unplanned admission, is to be extended into other key QoF areas, including Long Terms Conditions (LTCs). Data will be extracted every 24 hours from each of our primary, community and acute providers. Potentially, data from Local Authorities covering the Social Care teams who are actively supporting our patients will be added to this picture, with frequency to be determined.

From primary care this entails patients:

- in the 2% of the practice's population patients identified by practices as being most at risk of admission along with their last review date and the date they were placed on the register.
- on the practice's end-of-life register along with key detail identified by the ePaCCs project as essential for shared care including the patient's prognosis, whether anticipatory drugs are in place, are on fast track, have a DS1500 signed and their preferred locations of care and death.
- on the practice COPD register along with their MRC breathless scale status, Peak Flow as

% of predicted peak flow
- on the practice's heart failure register along with their NYHA status, whether they are on spironolactone, ACE inhibitor, ARB inhibitor or beta-blocker.
- on the practice's stroke register along with whether they are on aspirin, a statin and their latest blood pressure.
- on the practice's dementia register along with their latest memory score in the practice. This master list will help us to provide names for clinicians to help identify individuals which risk stratification has found to be at high risk of admission. Knowing the NHS Number of those patients in a practice will help us serve clinical data they currently can't access (e.g. because one of their patients was admitted when under another practice).
- having received care in any area covered by the Quality and Outcomes Framework (QoF)
- eligible for an NHS Health Check
- with mental illness, requiring preparation of a regular physical health summary (Physform)

Where it is practical we will encourage use of existing clinical templates to collect Read-coded data using national or local standard codes such as defined for QoF and ePACCs.

This listing is not intended to be complete and other registers may be added in the future to support the clinical requirement. Candidates requested so far by clinicians include falls, chronic kidney disease (CKD), peripheral arterial disease, cardiovascular disease (CVD), referrals and other neurological diseases such as Parkinson's. Any part of the record which may be contained within the extracts but is not within the agreed scope of GPRCC data is discarded automatically by the 'black box' loading process. Similarly, the raw source data is deleted automatically once processing is complete.

Data sets from community providers will just consist of the care teams that the patient is currently under. The initial set from PICS includes Heart Failure nurses, COPD nurses, Admission Avoidance team, End-Of-Life care team (for non-cancer patients). County Health Partnerships' and CityCare's teams include Falls, Stroke rehabilitation, Diabetes etc. but we would like to extend these to cover all clinical areas where there is not a specific IG or legal concern (forensics, for example). As an approach, this is becoming increasingly important for clinical safety as health professionals reasonably expect and assume that, where data is shared by a provider, this information is complete.

The dataset from our acute providers, currently Nottingham University Hospitals (NUH) and Sherwood Forest Hospitals Foundation Trust (SFHFT), are a cut down version of that submitted to SUS. They include coded data on diagnoses and procedures. We are discussing with NUH the possibility of expanding this dataset to cover a broader scope of SUS data for direct care purposes. If this goes ahead, the only identifier would remain the NHS number, pseudonymised in the same way as the current data flow.

Early contacts have been made to explore the use of key data from Community Geriatricians, Mental Health, Continuing Health Care and out-of-hours providers. In this iteration, we also aim to include the Social Care teams that patients are engaged with, subject to the necessary IG processes to enable data sharing between Health and Social Care for direct patient care. Any new data flows from organisations not previously included in the last assessment or agreed datasets will require a review of this PIA. A separate PIA has been undertaken by Nottinghamshire County Council, specifically in relation to the sharing of Social Care data with healthcare professionals.

The Data Management Team acts as a Data Processor on behalf of practices. Data from providers is pseudonymised at source by providers, using their own password key, then repseudonymised automatically on landing in a part of the NHIS data warehouse which is not available to CCGs (see diagram in Appendix B). Data is linked on the pseudonym for the NHS Number.

In one view, a clinician can see key data required to decide if a patient needs to be put on a local

care team caseload (Heart Failure nurse, COPD matron, Community Matron, End-Of-Life nurse, etc). The data needed includes recent admissions, OPD attendances, A&E attendances alongside the local Health and Social Care teams that the patient is currently under and some key data about that patient's Heart Failure, COPD, End-Of-Life status etc. The patient's calculated risk of admission, derived under the terms and conditions of the s251 CAG approval for Risk Stratification (CAG 7-04(a)/2013) is displayed alongside the other key factors. GPRCC data is not currently used in any part of this calculation.

Details of data being processed:					
	Whole records/referrals		Local identifier only	✓	NHS Number
✓	Name	✓	Date of birth	✓	Postcode (full)
	Postcode (LSOA)[1]	✓	Age (exact or <1 year)		Age bands 5 years
	Age bands 10 years		Ethnicity	✓	Gender
	Religion		Disability	✓	GP practice
✓	Other (please describe):	Telephone number, to allow patients to be contacted efficiently and with minimal access to patient records by staff working on behalf of Practices for limited purposes such as invitation to participate in bowel screening. Full address, to allow automation of letters to be sent by the Practice for invitations to participate in screening programmes or the NHS Health Check, for example. All of these items will be fully pseudonymised up to the point of legitimate direct care use, as for NHS number and name etc.			

Will data be:					
	Anonymised	✓	Pseudonymised[2]	✓	Fully identifiable (PID)
If processing is for secondary purposes (i.e. not related to direct care) and fully identifiable information is to be used, please explain why anonymised or pseudonymised data will not meet the project objectives?					
N/A – no data is being used for secondary purposes under this PIA.					

Frequency of transfers: (delete as applicable)
One off / daily / weekly / monthly / quarterly / annually / other (please state):
Daily extractions from each provider.

Please provide details on how long data will be retained by any organisation involved with processing, and destruction arrangements *(attach supporting documents where appropriate)*
Data will be retained for so long as patients remain registered with a Practice supported by the Data Management Team, plus a period of 12 months thereafter for clinical audit.

Organisations involved and stakeholders:	
Organisation	**Contact Name and Details**
Data Management Team (part of Rushcliffe CCG)	Exemption Section 40(3A) 3rd Party Personal Information. To disclose the
NHIS (host of the IT environment)	

[1] Lower Layer Super Output Area: relates to first half of postcode and number only of second half. Much public health reporting and published Indices of Deprivation are based on LSOA and this is the standard that is widely accepted and expected for large scale research/statistical reporting.

[2] A pseudonym is used to replace identifiable data so that patients cannot be identified without a pre-defined code/key.

All GP Practices across Nottinghamshire	information would contravene one of the data protection principles set out in article 5 of the GDPR
Nottingham West Health Ltd (aka Primary Integrated Care Services, PICS) (8HY59)	
Nottingham University Hospitals Trust (RX1)	
Nottingham CityCare Partnership (NR3)	
Sherwood Forest Hospitals Foundation Trust (RK5)	
County Health Partnerships (RHA20)	
Nottinghamshire County Council	
Nottinghamshire Healthcare Trust	

You do not need to complete stage 2 if the data involved in the project/activity is anonymised and the sharing is between organisations who have a legitimate* reason to receive the data or you are acting in a commissioning capacity which does not involve the CCG sending or receiving any personal confidential data or data which the CCG is the data controller.

However please highlight how you will keep the data secure and mitigate any risks.

Primary care data flows are only between existing clinical systems which have smartcard/RBAC access controls in place, into a secure SQL Server environment (NHIS Data Warehouse). Network access to the areas used by the Data Management Team is restricted to this team only (and NHIS technical support staff). Once loaded, the only user access to the data is via eHealthScope, which sits on the local COIN behind N3 and is secured with smartcard/RBAC controls in place.

As part of the transfer/upload process the data will be pseudonymised at source and transmitted to the Data Management Team over a secure encrypted connection. As part of the upload process, data is re-pseudonymised automatically before being placed onto the database discs. At this point, the original data is deleted automatically.

Any data within the record which is not a recognised GPRCC data item is discarded automatically by the import process. In some cases, high level details are retained, such as the name of an unrecognised community service and the number of records deleted, to ensure that expected data remains correctly mapped and, where practical, unexpected data is addressed at source before it is sent.

Have you considered if an information sharing agreement, data transfer agreement or other contract is required?

Data in not extracted from any primary care system until the Practice has signed a Data Processing Contract with the Data Management Team. A Data Sharing Agreement (signed by each Provider) will be included alongside the Data Processing Contract as this is best practice for data being shared in bulk for direct patient care. Each Practice is asked to place a Fair Processing Notice on its website. Providers, likewise, do the same.

For Social Care data, in addition to the standard measures above, an additional Data Processing Contract will be established between Nottinghamshire County Council and Rushcliffe CCG (as host of the DMT).

Technically, data cannot be extracted until Practices action a task within their clinical system to join the Reporting Unit. Once they accept the invitation, this only allows the individuals who have access to the Reporting Unit (Data Management Team) to create reports from the data fields (e.g. read-coded data) contained in the Practice's unit. Practices can withdraw themselves from the Reporting Unit at any time.

Stage 2

Describe and map the data flows and who will have access to the data *(who is collecting, receiving, transferring or storing the data):*

Data sources	→ *transfer* →	NHIS Data Warehouse / DMT	→ *transfer* →	Data recipients
GP systems	Data extracted using SystmOne reporting unit clinical reporting tool, pseudonymised by DMT and uploaded to a secure folder which is polled by an automated data warehouse upload function (Includes register of patients with Name, DoB, NHS Number)	Data held in GP registers with all personal identifiers pseudonymised	Data from all providers delivered by eHealthScope using RBAC and depseudonymised to individuals who have been granted permission by practice administrators of the permissions log	**Local Care Teams** (or **Care Delivery Groups**) including GPs, and named individuals from community teams either working separately or together in identifying or caring for patients at risk of admission.
Community systems inc: PICS CityCare CHC NEMS	Data pseudonymised at source then uploaded by eHealthScope (behind N3) to the NHIS data warehouse (includes NHS Number only)	Data held in Community registers with all personal identifiers pseudonymised		
Acute and Mental Health provider systems inc: NUH SFHFT NHCT CHP	Data pseudonymised at source then directly transferred (from SQL to SQL server) to the NHIS data warehouse (includes NHS Number only)	Data held in Acute Trust registers with all personal identifiers pseudonymised		
	Data pseudonymised at source then directly transferred (from			

Social Care	SQL to SQL server) to the NHIS data warehouse (includes NHS Number plus full name, postcode, gender and date of birth – the minimum standard to allow trace of NHS number via DBS)	Data held in Social Care registers with all personal identifiers pseudonymised		

Will the project involve the collection of new personal confidential information about individuals? *(if yes, please describe)*
No. Existing data from GP Practice clinical systems will be extracted for this purpose – no new data collection is or will be required. However notes which may contain clinical information may be added prior to or at MDT meetings. These are stored in a separate table in the data warehouse.
Will the project compel individuals to provide personal confidential information about themselves? *(if yes, please describe)*
No. Data will not be collected on patients who have given express dissent in their GP clinical or Social Care information systems to their data being used for clinical care.
Will information be disclosed to organisations or people who have not previously had routine access to the information? *(if yes, please describe)*
Yes. Data will be available to Local Care Teams, Practices will be able to view which Local Care Teams their patients are under. Community teams will be able to see a small relevant subset of Read-coded information to help in the identification and management of patients at risk of admission. Both Practices and Community Teams will be able to see brief details of the admissions, OPD visits and A&E attendances of their patients. GPs and Local Care Teams will also be able to see details of which Social Care teams are involved with the patients for whom they are providing health care. Access to the data will be controlled by GPs within their clinical system. They act as administrators of the permissions log and this will not change. Only by Practice staff adding an entry to this log can Local Care Team (or PRISM or Care Delivery Group) personnel see this information. Practices can also remove a person's access to this information. Changes to the permissions log are themselves logged in an audit table. Each practice can see all changes made to the permissions log that affects their patients.

Are you using information about individuals for a purpose it is not currently used for or in a way it is not currently used?
All data will be used for direct care, the reason it was collected in the first place. In the case of Continuing Health Care and Social Care, the routine availability of basic information to GPs is patchy and this will go a long way towards improving availability.

Will explicit consent be obtained from data subjects?[3]	
	Yes – verbal, recorded in record
✓*	Yes – written, scanned into record
✓	No – not required
	No – other reason
If explicit consent is not to be obtained, please state reason(s) below or give details about	

[3] The individuals who the records are about.

the legal basis you are relying on the process personal confidential data:
As the focus of the project is to deliver direct patient care, we are not seeking explicit patient consent to share out information from GP clinical systems. We are using implied consent. However any patients who have explicitly dissented to the sharing of their record for direct care purposes will have their record discarded automatically by the 'black box' loading process. Community providers seek out explicit consent to share information with GPs when they first see their patients. Communication packs have been issued to all practices so that posters appear in waiting rooms advising patients that a subset of their GP records are being shared in the community for direct patient care. This is part of a joint communications approach run with the MIG project. Practices are also advised to update their websites to describe electronic record sharing. Limited Social Care data (i.e. which teams are providing services to individual patients) will be shared for the purposes of direct care on an implied consent basis, and only where the person has not recorded their explicit dissent to do so. *Although implied consent will be the default approach for sharing between Health Professionals for direct care, Social Care will seek and record explicit consent at all opportunities where it is practical to do so.
Will the project require you to contact individuals in ways which they may find intrusive? *(if yes, please describe)*
Possibly. However, patients will only be contacted by their GP Practice (or staff explicitly deployed to act on their behalf) in the manner that they are currently – this work simply makes the task more efficient and improves information governance by removing potential to access patient data which isn't required by an individual for the specific task.

What security arrangements will be put in place to ensure the confidentiality and information security of personal confidential data? *(consider any residual threats to data security)*
By nature of the current design of GP systems, data must be extracted manually in clear form by the DMT. The files are saved transiently to a secure network location accessible only to the DMT and, potentially, NHIS network administrators. There is no requirement to open the files or see any patient data during this process. An automated process polls for new files to pseudonymise and upload the GP data to the secure SQL environment. The source file is then deleted automatically. Prior to Community, Acute Trusts or other Providers sending data, all identifiers are pseudonymised at source. Data transfer from community or acute providers is either by direct database-to-database transfer (within our local COIN or network using secure connections) or by upload of the pseudonymised dataset via eHealthScope (behind N3) directly into a secure folder on an NHIS server (see diagram in Appendix B). A process on the secure server polls the delivery folder every 10 mins and automatically re-pseudonymises the data as it is loaded into the GPRCC data warehouse, before deleting the source file. All personal identifiers for data in the data warehouse remain pseudonymised. The NHIS data warehouse is built to NHS Digital accreditation standards. The Data Management Team, in their role as Data Processor on behalf of General Practices (and Nottinghamshire County Council), can access this data but only see it in pseudonymised form (whether they access the data directly via SQL queries or via eHealthScope). No other CCG staff have access to this data.

End users in local care teams can only access the data via eHealthScope. They are authenticated by the NHIS team (prior to being given a username/password and smartcard). Access then will be via smartcard (with PIN) or by username/password combination. Passwords must be set and changed in line with the agreed NHIS network security policy.

An end-user can only see clinical information associated with identified patients if they have an RBAC entry in the permissions log. Each practice maintains its own entries in the permissions log. They can assign full Read or Write access, Community access, End-of-Life (only) access, Analyst or Teaching access. The Analyst role never can see GPRCC information in any form; the Teaching role provides access to GPRCC data but only in pseudonymised form for the purposes of Practice support and training. Each CCG also has one nominated Practice Permissions Administrator whose role is to support Practices in ensuring that starters, leavers and those changing role are assigned the correct permissions. All changes to the Permissions Log are fully audited (including who made which changes) and is visible to Practices. In addition, the DMT monitor the audit logs to provide additional assurance that usage is appropriate and consistent.

eHealthScope has many built-in security features. Aside from the RBAC system for access to data, there are methodologies in place to defeat SQL injection and it lies behind N3.

Leicestershire HIS have conducted Vulnerability / Penetration Testing on the core servers used on the GPRCC project which are hosted with the NHIS (N3) secure network and found them to be generally satisfactory. The recommendations made have been acted upon and further rounds of testing will be conducted after significant system changes, such as relocation to new servers.

What will be the impact of decisions brought about by the project or activity and processing of PID? *(please highlight both positive and adverse impacts either directly or indirectly)*

The key benefit is to patients. The Local Care Teams strive to prevent urgent admissions and readmissions. Good care reduces admissions, reduces mortality and increases quality of life.

Integrated care has been highlighted as being a key to delivering effective care, and integrated records as a key to delivering integrated care. Effective preparation for MDT meetings means a clearer focus on those patients who need the care. Summarised, integrated information available with no transition time between patients frees up time in the meeting to discuss patient care, whereas the traditional model of loading the records and letters in a clinical information system can take 30+ seconds and, if 50 patients are discussed, half of the meeting time may be consumed by gaining access to information. However occasional access to the full record can be illuminating.

Presenting the information without access to patient names would rule out linking in the knowledge of all of the clinicians around the table and would reduce clinical safety when discussing multiple patients in quick succession.

Potential care gaps may be identified quickly and efficiently – for example, where a patient has a severe COPD diagnosis in the GP system but does not appear to be under the care of a community COPD team. Highlighting these patients to GPs enables them to be reviewed and potentially offered a better package of care that will improve outcomes and reduce emergency admissions.

Practices (or staff working directly on their behalf) may need to contact groups of patients by telephone or letter – for example, to invite participation in a screening programme. By storing patients' current contact details in encrypted form, it is possible for authorised individuals to do this work without having access to the full clinical record, and much more efficient than querying records individually in the native system.

Summarise the risks of this processing? (NB: these 3 can be merged as appropriate) Please attach full risk assessments. *(refer to your risk management policy for risk RAG scoring)*

a) To Patients, providers, Practice, CCG		
1*5=5	Data is lost in transfer	See details in the PIA
1*4=4	Access to data gained by third party	See details in the PIA
2*2=4	Patients object to implicit consent	Widely discussed with patient representatives as part of MIG project and in CCG clinical cabinets. Risks felt to be significantly less than risk to patients of not delivering effective care.

If applicable, please give details of any service user/staff/public consultations that are going to take place, or have taken place in relation to this processing? *(include internal and external stakeholders)*
The MIG project communication strategy was developed in such a way as to include GPRCC. However, the GPRCC board will need keep the communication materials provided to patients under review to ensure that they remain sufficient to meet duty of confidentiality requirements and assess whether further communication should be provided to patients.

Please return the completed PIA to the IG lead/s to complete section 3

Appendix A: Action Plan

Identified Risks and Agreed Actions

What are the key privacy issues and associated compliance and corporate risks? (some privacy issues may have more than one type of risk i.e. it may be a risk to individuals and a corporate risk).

Consider if project process needs to be adapted to address privacy concerns?

Describe the actions you could take to reduce the risk and any future steps which would be necessary (e.g. new guidance, inform and or engage patients of a particular change, put in place an information sharing agreement or data processing contract etc.)

Risk and risk lead (responsibility for the action)	*Solution (s)/actions taken to reduce the risk*	*Result: Is the risk reduced, eliminated or accepted? Is impact proportionate in considering aims of project?*	*Implementation of outcomes back into project and review date*
Compliance with the duty of confidentiality- necessary action will need to be taken to ensure patients are told/informed at practice level (tool and mechanism proportionate to the data sharing) regarding the sharing of data outside the practice **Lead- Project lead as part of project specification with support from IG colleagues**	**MIG Comms Strategy encompasses GPRRC.** **Support provided to practices in reviewing and amending where appropriate their fair processing notice.** **Project Board to continually make an assessment that sufficient information is being provided to patients about data flows supporting direct care.** **It is also worth noting from a patient confidentiality perspective when data is sent to the JDMT it is automatically pseudonymised so no one outside the 'patient direct care relationship' can identity or have access to clear person identifiable data**	**Reduced**	**Implementation ongoing as part of the project progression.** **Sufficient information needs to be provided to patients before any person confidential data leaves the practice.**

Patient objection/opt out management (recorded on SystmOne and EMIS) re: data flowing in an identifiable form outside their GP practice (upholding patient NHS constitutional patient rights) **Point of note: the data flows identifiable but is automatically/without human intervention pseudonymised on landing.** **Lead- Head of Data Management and Mike O'Neil as SIRO**	**Although the DMT and other organisations (e.g. EMIS and TPP, who hold GP data off-site) act as a Data Processor under contract to GPs, this should be transparent to patients in the Fair Processing Notices and implied consent applies to Direct Care usage where consent is also informed consent. The data leads consider that patients who have recorded an objection to sharing data outside of the Practice for uses other than Direct Care are being excluded automatically from the extracts. Further experiments to confirm this explicitly are planned with a consenting test patient.**	**Reduced**	**Implementation ongoing as part of the project progression. Results of experiment re patient opt out to be fed back to project board members.** **Update November 2016: Strategic Reporting solutions have replaced the initial data extraction mechanisms due to technical constraints encountered when scaling out. For both SystmOne and EMIS Web, these allow data to flow regardless of the patient consent status. However, they also support export of the objection codes, so these can be applied within the 'black box' process to ensure that patient wishes are respected for particular use cases within the GPRCC.**
Commencement of the pilot project for Nottingham West GP practices before formal approval/endorsement by the project board of PIA **Lead- Mike O'Neil as SIRO for Nottingham West CCG**	**Agreement in principle was obtained about the process from the Project Board including IG advice and processes that needed to be in place prior to launching the pilot. Security mechanisms (e.g. pseudonymisation, Role Based Access Controls, anti-SQL injection techniques) already in place in eHealthScope for handling patient**	**Accepted**	**N/A but any learning of issues identified as part of the pilot to be raised/fed back for Project Board members due consideration**

	information in similar contexts for direct patient care. Approach discussed with patient reps and clinicians in Nottingham West CCG Clinical Innovation Group. Patient comms (to inform patients of sharing records for direct patient care) handled via the MIG project and being reviewed as project processes.		
Contractual arrangements between NHIS as subcontractors providing/managing the data warehouse **Lead- The NHIS IT lead for the CCG'S/ NHIS SLA with support from IG colleagues who will recommend any amendments**	**NHIS contract needs reviewing to ensure that the relationships and service provided is covered by the SLA particularly regarding the data warehouse.** **Carl Davis to forward copy of NHIS SLA / DPC to IG colleagues for review of data protection compliance. However, as NHIS are not doing anything specific for GPRCC (just providing the storage, infrastructure and IT support), this solution is being considered as part of the wider due diligence. If existing terms and conditions of the NHIS relationship extend naturally to cover GPRCC activities then no specific action required.**	**Reduced**	**Update November 2016: The 2017-18 NHIS SLA has been revised to improve description of data warehousing functions.**

MoU between CCGs to reflect access to data by JDMT (particularly the SUS which technically belongs to the individual CCGs) **Lead- Head of Data Management to reflect the role and processing by his team with support from IG colleagues**	**Needs to be updated to reflect the changes specifically in terms of the joint functions provided by the Joint Data Management Team (Hosted by Rushcliffe CCG) and any access to SUS data provided individually to the specific CCGs under HSCIC contract(s)**	**Reduced**	**ASAP but completed within 3 months of approval of this PIA** **Update November 2016: Data Processing Contracts are now being drafted between other CCGs and Rushcliffe (as the legal host of the DMT) to better formalise the data processing relationship. This has also been clarified with NHS Digital (formerly HSCIC) in a recent DARS approval for commissioning datasets.**
eHealthScope is not an accredited application operating within the N3 network **Lead- Head of Data Management and Mike O'Neil as SIRO for Nottingham West CCG**	**Discussion between Carl Davis, Mike O'Neil and Paul Gardner, this was raised as earlier versions of the PIA referenced the solution as being 'accredited'. It was agreed to remove this as a risk and thus accept this as an outstanding issue to consider further exploration, as not clear that accreditation is required/mandatory for an internal application or how this might be gained. Mike O'Neil as the SIRO and Carl Davis as the Head of Data Management do not consider that in the absence of any such formal accreditation there is a residual information security risk to data or risk of a confidentiality breach. If possible to**	**Accepted (outstanding issue for further consideration)**	**Review in 3 months as part of phase 2 after further exploration about accreditation requirements and necessity**

	accredit, this would be pursued – an assessment to be made as to whether similar applications, such as GEMIMA are accredited?		
Possible lack of security assurance as penetration testing not completed in regards to key areas supporting the GPRCC project **Lead- Andy Evans as GPRCC Board Chair supported by Mike O'Neil as SIRO for Nottingham West CCG**	**Leicester Health Informatics Service to undertake tests within next few months and this invoice has been approved as part of the project board. However in the wider context eHealthScope has been operating for a number of years with no known security issues or breaches. Completion of the PEN testing will give wider assurance as part of the recent cyber security focus.**	**Reduced**	**January/February 2016 results of PEN testing to be provided to the project board members as a part of the assurance process.** **Any significant issues or risks identified to be actioned immediately and all SIRO's informed accordingly** **Update November 2016: Test results were satisfactory and recommendations acted upon. Further testing planned when eHealthScope servers are migrated.**
SQL running on server older than 2008 **Lead- Andy Evans as GPRCC Board Chair supported by Mike O'Neil as SIRO for Nottingham West CCG**	**N/A- All servers now running SQL Server 2008 R2 and looking to migrate to a still newer version at the earliest opportunity. Any issues in this regard will, in any case, be picked up by the Leicester Health Informatics Service penetration testing, so agreed to remove as a separate risk.**	**Accepted/Removed**	**January/February 2016 results of PEN testing to be provided to the project board members as a part of the assurance process**

Appendix B: Data Flow Diagram