

Data Protection Impact Assessment

DPIA Title:	Centralised LPRES (Local Person Record Exchange Service) Viewer – Care Homes PoC
DPIA Lead: (name and job title):	Beverly Roberts – LPRES Operations Manager
Version number:	3.0
Next review date:	2022 (TBC)
Validator's name (Information Governance):	Jane Howarth
Validation date:	
Data Protection Officer consulted (date):	TBC
Data Protection Officer comments:	TBC
Data Protection Officer signature:	TBC
SIRO approval (date):	TBC
SIRO comments:	TBC
SIRO signature:	TBC
Caldicott Guardian consulted (date):	TBC
Caldicott Guardian comments:	TBC
Caldicott Guardian signature:	TBC



OVERVIEW

This part allows you to identify and present the object of the study.

PURPLE SECTIONS TO BE COMPLETE BY PROJECT LEAD

PINK SECTIONS TO BE SUPPORTED BY INFORMATION GOVERNANCE

What is the process under consideration?	Guidance
<p>Present a brief outline of the processing: its name, purposes, stakeholders, context of use, etc</p> <p>The Local Person Record Exchange Service (LPRES) was initiated in 2015, formerly known as the Lancashire Patient Record Exchange Service, going forward this will be known as the Lancashire and South Cumbria Shared Care Record (ShCR/SCR) and provides read-only access to clinical information for healthcare professionals and patients across all healthcare settings (primary care, secondary care and social care) across the Lancashire and South Cumbria geographical footprint. This has also been opened up across the UK North West Coast geographical boundary i.e. Cheshire and Mersey Share2Care (S2C) during Covid-19 under the COPI notice (see S2C DPIA and https://digital.nhs.uk/coronavirus/coronavirus-covid-19-response-information-governance-hub/control-of-patient-information-copi-notice). The platform is able to share this read-only data by using the international IHE (Integrating the Healthcare Enterprise) standards and is aligned to the NHS Digital strategies for interoperability in healthcare in the UK.</p>	<p>Present a brief outline of the processing under consideration, its nature, scope, context, purposes and stakeholders.</p>

The LPRES CORE Health Information Exchange (HIE) hosted by AWS Cloud computing contains the NHS number and meta data pointing to documents held at individual organisation level storage. This topology enables retrieval of the relevant patient GP 10 Tab View and EPACCS record from EMIS and the patients' documents from the relevant organisations local affinity domains in a non-persistent view. This view is currently launched within patient context and within Organisations local Electronic Patient record (EPR) system via a web services call from the LPRES viewer. Access to the patient data is role based and fully audited.

In addition to GP's, NHS Trusts and local councils across the geographical footprint sharing this data for direct patient care, other organisations where there is a need for direct care, such as, GP referrals to private hospitals, local hospices (charities) providing care to citizens, other charities that have been commissioned by a data controller, e.g. CGL (Inspire) a drug and alcohol service commissioned by LCC, publish crisis care plans for access by A&E (See CGL DPIA). Local councils publish adult social care plans to LPRES. As part of a proof of concept Nursing homes and Care homes within L&SC will be given access to LPRES, the Shared Care Record (SCR).

WellPRES/Mi-PRES – provides the citizens and health professionals of Healthier Lancashire and South Cumbria with access to a remote surveillance platform for several cancer recovery programmes - Breast, Colorectal and Prostate Cancer supported self-managed follow up. The implementation consists of a combination of two key elements of Parsek's Vitaly health care solution set.

A Patient portal for facilitating patient engagement and allowing them to access their electronic health record. This has now been renamed Mi-PRES.

A Managed Care system, which enables personalised and remote coordinated healthcare for clinical teams.

The solution is designed to support patients with stable disease to self-manage their follow up care.

WellPRES/Mi-PRES is now pointing at the LPRES Core HIE to enable clinicians and ultimately the patient to view their information within the WellPRES platform i.e. access to the electronic health record via a link to LPRES (see WellPRES/Mi-PRES DPIA).

This project is to give Care Homes/Nursing Homes access to the SCR via the Centralised LPRES Viewer.

The Centralised LPRES Viewer is cloud internet facing (located on the LPRES VPC) in AWS (Amazon Web Services) which the organisations point to. This makes any future updates to the viewer code

<p><i>streamlined and will only require amendments to be done once, reducing duplication of effort and potential errors/testing etc.</i></p> <p><i>Due to the sensitivity of the clinical data being accessed over the internet, access will be more controlled as opposed to using a simple username and password. This will be achieved by implementing a two-step verification service using the time-based one-time password algorithm provided by the Google Authenticator App.</i></p> <p><i>The LPRES Ops team will on-board the care home / nursing home manager in the first instance. The manager will then be responsible for providing a list of their staff, assigning the most appropriate role-based access (based on their position within the Home) and ensuring they have completed IG training. These NH staff will then be on-boarded via the LPRES Team. If a user doesn't use their account within 12 weeks, the account will be deactivated automatically.</i></p> <p><i>This project is a proof of concept to give access to nursing homes and care homes in L&SC to LPRES, the Shared Care Record via the centralised LPRES Viewer, therefore it involves one Care Home for this PoC which, once proved successful then others will be included/onboarded across the L&SC footprint. This will give clinicians/employees who have a legitimate relationship to the resident/service user/patient to view relevant information about them that will help provide them with the care that they need.</i></p> <p><i>Care Home staff will be able to gain access (role dependant) to the GP record and over 8 million documents published by secondary care organisations within Lancashire and South Cumbria. This will result in a better and more personalised support for the residents.</i></p>	
<p>Will the process necessitate the use/processing/collection/sharing of any personal or pseudonymised data?</p>	
<p>Please answer Yes or No</p> <p>IF NO, NO FURTHER QUESTIONS NEED TO BE COMPLETED, PLEASE PASS TO INFORMATION GOVERNANCE FOR REVIEW</p>	<p>Personal data</p> <p>Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be</p>



Yes

As part of the rules for an organisation joining the LPRES service – they need to establish a core set of local servers within their own boundaries, behind their firewalls. The local LPRES servers (known as the Affinity Domain) store any documents published via the LPRES HIE locally i.e. the documents are still in the control of the publishing organisation.

Meta data relating to the document is stored at the CORE HIE for example NHS Number 999999999 has a cardiology clinic letter stored on the local affinity domain at Blackpool. If a Clinician then requires to look at the details within the document they have the facility to “open” the letter within the LPRES Viewer. This is done by requesting the document point to point i.e. if the clinician is looking at the LPRES viewer from East Lancashire Hospitals NHS Trust and want to view a letter stored at Blackpool, ELHT makes a direct call to Blackpool for the document.

Once a clinician views a patient record and associated documents - this view is none persistent i.e. once they move away from this patient information to another patient record or they close the viewer, the information is removed from their screen. Printing of information is disabled and there is no functionality to pull information into other systems locally.

Nursing homes/Care homes will be sharing personal data by accessing the SCR if they meet the minimum criteria required as outlined below:

- Active user of NHS mail
- DSPT Standards Met (published 20/21 or 21/22)
- Interested in being the first home across Lancashire and South Cumbria to view this information (PoC)
- Have approximately 40 staff

As part of the LPRES Viewer the clinician is able to see Healthcare Gateways MIG ten tab view of information from the eMIS GP record. If a patient has an ePACCS tab within the GP record and this has been coded to enable sharing – then this eleventh tab will also be visible to the clinician. Again this information is none persistent.

As part of Covid-19, when a user launches the viewer, it queries the NEXUS API to see if there are any covid results for this patient and pulls the covid data from Nexus to display the results on the screen, again this information is non-persistent. (See DPIA for Hi-Pres)

The centralised viewer consumes the same information from the IHE and the MIG.

identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. See [Art. 4.1 of \[GDPR\]](#)

Pseudonymised data

Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person.

The centralised viewer collects staff details and generates a regional staff ID – so that we can easily identify who is accessing the system. The details it collects are – Local username, given name, surname, honorific, and role. See Appendix C

Centralised real-time consumption statistics/analytics

It's now collecting mismatches in patients date of birth between the LPRES exchange and the Cheshire and Merseyside exchange. This allows the production of data quality reports every month and will increase the data quality between the two exchanges.

The system tracks which documents a user views for each patient. This allows the viewer to show the user which documents they have seen before. The data collected (See Appendix C) will also be used to train a machine learning algorithm to make recommendations on the documents the user would be most interested in.

As part of the patient record, if a document contains an image, e.g. x-ray, CT scan, these documents can be viewed by the LPRES viewer. Bridgehead acting as a processor provides a technical solution to display the image via ResolutionMD (ResMD) so that when a user requests an image from their device, the images are pulled into the ResMD and stored in the RAM of the server and a viewing session is created. This is a non-persistent view as no data is stored on the ResMD server or the device of the viewer.

What are the responsibilities linked to the processing?

Describe the responsibilities of the stakeholders: the data controller, the possible data processors and joint controllers

The Trusts, GP's, Social Care organisations across the HL&SC geographical footprint are acting as Joint Data Controllers and all stakeholder organisations will share responsibility as Data Controllers for the data they share.

Organisation	Role
Blackburn with Darwen Borough Council	Data Controller
Blackpool Council	Data Controller
Blackpool Teaching Hospitals NHS Foundation Trust	Data Controller
East Lancashire Hospitals NHS Trust	Data Controller

Definition: Data Controller

Natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

See [Art. 4.7 of \[GDPR\]](#)

Definition: Data Processor

Natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller, see [Art. 4.8 of \[GDPR\]](#). The processor and any person acting under the

Lancashire and South Cumbria NHS Foundation Trust	Data Controller	authority of the controller or of the processor, who has access to personal data, shall not process those data except on instructions from the controller, unless required to do so by Union or Member State law, see Art. 29 of [GDPR] .
Lancashire County Council	Data Controller	
Lancashire Teaching Hospitals NHS Foundation Trust	Data Controller	
NHS Lancashire and South Cumbria Integrated Care Board (ICB)	Data Controller	
North West Ambulance Service NHS Trust	Data Controller	
Southport & Ormskirk Hospital NHS Trust	Data Controller	
University Hospitals of Morecambe Bay NHS Foundation Trust	Data Controller	
St. Catherine's Hospice	Data Controller	
St. John's Hospice	Data Controller	
East Lancashire Hospice	Data Controller	
Queens court Hospice	Data Controller	
Trinity Hospice & Palliative Care	Data Controller	
BMI Healthcare	Data Controller	
Fairfield Hospital	Data Controller	
Ramsey Healthcare	Data Controller	
Spire Fylde Coast Hospital	Data Controller	
Virgin Care Services Ltd	Data Controller	
ANS	Data Processor	
Amazon Web Servers (AWS)	Sub Processor	
Tiani Spirit UK	Sub Processor	
Maywoods	Data Processor	
Bridgehead Software Ltd	Data Processor	
CGL (INSPIRE) commissioned by LCC	Data Processor (Charity)	
Primrose Bank Limited (Care Home)	Data Controller	

For a list of GP's covering HL&SC involved in the DSA, see Appendix A.

In addition to the organisations stated above please see the S2C DPIA for clarification of the additional organisations that LPRES is currently sharing data with across the Cheshire and Mersey geographical boundary– I have included the attached document rather than creating 2 separate DPIA's. There is an additional dataflow on the ISG to cover these. (Please note: The COPI notice has been extended by the government until 30th June 2022 as a correction to the date in the attached document)

S2C organisations can be found in the attached document:



Covid-19.docx

Amazon Web Services (AWS) have been contracted to host the LPRES servers, data centres based in the UK (EC2 – London) and are sub-processors under ANS.

ANS is a Data Processor who have been contracted to provide the support wrapper for AWS Cloud services, managing the environment within AWS up to and including the Hypervisor layer. For Personal Data that ANS Customers store ("at rest") or transmit through ("in transit") ANS managed infrastructure, or cloud services, ANS provides a fully managed service to its Customers (including managed compute/store infrastructure and/or managed network infrastructure).

Tiani Spirit UK provide the software for the LPRES HIE functionality and are sub-processors under ANS.

An NHS in-house senior developer with support from Maywoods provides the LPRES Viewer code

Maywoods acts as data processor and provides an audit facility for LPRES

To support users of the LPRES service and the need to protect and monitor both the publishing and consuming of data via the LPRES HIE, Maywoods was commissioned to provide an Audit Tool. The audit tool servers are currently hosted at Blackpool Teaching Hospital within their IT infrastructure.

As part of this project Maywoods will also set up a database to store the names of staff, in order to provide statistics to monitor the application, who is using it, etc. It will be stored on the LPRES VPC - See Appendix C.

Each Organisation requiring the LPRES Viewer links directly from their local ePRs/clinical systems to the centralised LPRES viewer. This also supports a clinician not having to log on to another system as credentials

<p>are handed over to the LPRES Viewer from their clinical system. The IG reminders/awareness messages regarding the IG responsibilities of the clinician/user viewing patient records is presented when the user logs into their local EPR/clinical system, applying to this instance of care if the LPRES viewer is deployed.</p> <p>Care Homes/Nursing Homes which do not have an ePR/clinical system will logon to the centralised LPRES viewer to access the shared care record via controlled access achieved by using a two-step verification service using the time-based one-time password algorithm provided by the Google Authenticator App.</p> <p>Bridgehead Software Ltd act as a data processor providing the software interface for the diagnostic viewer to transmit an image via the ResMD viewer to display via the centralised LPRES viewer.</p>	
<p>What governance measures are in place to oversee the confidentiality, security and appropriate use of the data?</p> <p>LPRES provides access to a view of the permitted data held within local affinity domains. Consequently, the responsibility to maintain secure data storage and maintenance remains within the remit of the 'home' organisation which holds the host data.</p> <p>All NHS and Public Sector organisations whose data will be viewable via LPRES are compliant with National Health and Social Care standards to hold patient identifiable and sensitive data.</p> <p>This means each organisation where the source data is hosted will:</p> <ul style="list-style-type: none"> • have proven their compliance with the Data Security and Protection Toolkit (DSPT): NHS controlling organisations, Councils, NHS Business partners, hospices/charities have suitable compliance, as per assurance on the ISG. Data processors/sub-processors compliance with the DSPT has been confirmed, as follows: ANS Group Limited (8GY56) 20/21 Standards met 04/06/2021 Amazon Web Services (8JX11) 21/22 Standards Exceeded Standards exceeded 12/04/2022 Tiani Spirit (8JT66) 20/21 Standards met 05/02/2021 21/22 Standards Met 26/11/2021 Maywoods (8JF15) 20/21 Standards met 30/06/2021 Bridgehead Software Ltd (8J340) 20/21 Standards met 30/06/2021 	<p>Governance measures may include compliance with the Data Security and Protection Toolkit, having IG, data security and data breach policies and procedures in place, 95% minimum staff compliance with IG training.</p> <p>Note that “All organisations that have access to NHS patient information must provide assurances that they are practising good information governance and use the Data Security and Protection Toolkit to evidence this by the publication of annual assessments” (https://www.dsptoolkit.nhs.uk/Help/Attachment/5)</p>

Please see: <https://www.dsptoolkit.nhs.uk/OrganisationSearch/RXL>

- have significant IG security policies in place
- have strong breach procedures in place
- ensure that their staff are trained.

In addition, ANS has been contracted to provide the support wrapper for AWS Cloud services. For Personal Data that ANS Customers store (“at rest”) or transmit through (“in transit”) ANS managed infrastructure, or cloud services, ANS provides a fully managed service to its Customers (including managed compute/store infrastructure and/or managed network infrastructure).

ANS is also responsible for the management of its downstream suppliers (e.g. data centres) in the provision of its services and has ensured that contractual obligations and processes are in place with these suppliers to guarantee the protection of Personal data owned and controlled by ANS Customers. This is achieved through a mix of supplier due-diligence, on-site audit, and contractual obligations as appropriate for the service being provided by the downstream supplier.

The Customers of ANS retain Data Controller responsibility for any Personal Data they use to do business, as they decide the purpose of this Personal Data (why it is collected, how long it’s retained for and how it is disposed of) and they are responsible for identifying and applying the required level of protection to keep it confidential in accordance with their own risk management approaches and privacy impact assessments.

ANS employees should never be granted access to this Personal Data as there is no business need for them to have access to it in the normal delivery of services. As Data Controllers, the ANS Customers are responsible for managing suppliers (Data Processors) through supplier contractual obligations and ongoing due diligence checks.

ANS is an ISO/IEC 27001:2013 accredited organisation with supporting UK Government Cyber Essentials accreditation, ANS already has an Information Security Management System (ISMS) in place, along with recognised cyber practices and GDPR compliant process and procedure that supports the delivery of services to its Customers. ANS has created a specific Data Protection policy and procedures to enhance these processes to fully meet the needs of the GDPR for its own business, and this supports, rather than replaces, the necessity for ANS Customers to ensure that their own security practices comply with meeting their own responsibilities under the GDPR as Data Controller of their Personal data.

ANS has procedural and technical controls in place to support the protection of Personal Data owned and controlled by ANS Customers, and practices that support the Customer in their investigation of any unauthorised data disclosure. Where the Customer’s privacy impact assessment and risk assessment identify the need for specific security measures to protect their Personal Data, as Data Controller, it is the Customer’s

responsibility to ensure these security measures are implemented (e.g. end-to-end encryption over a network, encryption of stored data).

If any further information is required, requests should be addressed to:

The Data Protection Officer, ANS Group Limited Synergy House Guildhall Close, Manchester Science Parks Manchester. M15 6SY

E-mail: dataprotection@ansgroup.co.uk

Any data that requires temporary storage within LPRES is hosted within the HL&SC AWS environment and is protected contractually by all the security measures provided by AWS and ANS.

The Cloud Servers Hosted by AWS include certification and compliance certification as follows:

- G-Cloud Certification
- CSA (Cloud Security Alliance) Controls
- ISO 27001, ISO 9001, ISO 27017, ISO 27018
- SOC1, SOC 2 and SOC3 coverage
- DSP Toolkit Compliance
- Cyber Essentials Plus

LPRES Viewer

The LPRES Viewer is a standards-based web server developed by the NWSIS to compliment the Tiani HIE. The software, which implements this web service currently consumes documents from one or more XDS document repositories based on the Tiani Spirit platform. The LPRES Viewer uses Tiani's STS (Secure Token Service) API to authenticate into the HIE and uses the SOAP (Simple Object Access Protocol) API to retrieve selected documents for a given patient.

The LPRES Viewer also connects to the MIG for the given patient performing an extended patient trace. The patient is found then a trigger query is made against the patient to see if an end-of-life care pathway has been activated within the GP surgery. If an end-of-life care pathway has been activated, then this option is presented to the clinician by default.

The LPRES Viewer service has been designed so that organisations can point to the web application from their main clinical system. By passing across the patients NHS Number, organisations can view all published



documents for a given patient in context with their main clinical system (providing the LPRES Viewer user has the correct role and access rights).

The web service has been developed using the open-source programme language Go, developed by Google. The source code that comprises the web service is itself released under an OSI approved open-source licence. This allows each organisation to freely develop the code further should they wish to do so.

If any of the published documents contain an image this can now be viewed by an XDSi data flow retrieval.

Retrieval data flow is initiated by a clinician searching for a patient's data using LPRES.

The clinician can use any patient ID associated with the patient or demographic data such as name, date of birth and address.

The patient information is sent to the Tiani MPI and the MPI returns the patient's Global ID.

LPRES then uses the Global ID as the basic criteria for finding any documents registered in the XDS Registry for this patient. The Registry returns all documents matching the criteria.

The clinician then selects the document(s) they wish to view.

LPRES uses the metadata associated with document to access the document from the XDS Repository where it is stored. In the case of a DICOM Study this will be a KOS object.

LPRES recognizes it is dealing with a KOS object. It extracts the critical information from the KOS object, Study UUID and VNA(Vendor Neutral Archive), and parses a URL string to send to the DICOM Viewer, ResMD.

ResMD receives the URL request and then issues a DICOM C-Move request for the Study against the VNA. The VNA returns a copy of the DICOM Study. ResMD renders the Study and presents it as an i-frame within LPRES. The clinician is able to manipulate the Study. The clinician is unable to modify the Study.

BridgeHead Software – supplying the HealthStore solution/Diagnostic viewer interface.

DSP Toolkit 20/21 – Standards Met | ICO Registration Ref: Z1415612

Accreditations include: ISO 27001, ISO 9001, ISO 14001

IG Security Policies, breach procedures and trained staff in place.

HealthStore will be hosted on the AWS Cloud in their EU-West (South of England) data centre.



LPRES Programme

Underpinning an effective, efficient, integrated care system is the movement of data across all the organisations involved in the delivery of that care. In many other countries, the introduction of a Health Information Exchange (HIE), has solved this complex problem. This approach has been incrementally rolled out across the Lancs & S Cumbria footprint from 2015 to date. The implementation of the LPRES HIE platform has brought about improved patient care by addressing the issues associated with silos of information, stored within legacy systems, across multiple Organisations. The HIE enables relevant patient information to be available to authorised members of the clinical and social care teams in order to support timely patient care. For direct care delivery, data from the GP record, acute and community providers is made available across the health economy with access to the information controlled and auditable. The information published always stays within the “owners” systems and behind the “owners” fire walls.

Tiani Spirit UK

Since 2007, Tiani Spirit has been recognised as the world's most comprehensive standard-based clinical document and imaging exchange solution on the market. The IHE integration profiles, with the accompanying actors, are practically applied in the Tiani SpiritEHR. These are tested biannually at the international IHE compatibility test, the Connectathon. This testing ensures quality and provides investment security. The results are open to the public. In the eHealth market, software vendors present many different solutions to implement health information exchange (HIE). Tiani Spirit's solutions feature functionalities that are not found elsewhere in the market. And according to the IHE guidelines - Tiani Spirit implements the most comprehensive EHR. At the IHE Connectathons in both the United States and Europe, Tiani Spirit has consistently demonstrated the ability to connect with significantly more actor/profile pairs than any of our competitors (at the Connectathon US 2017, 118 vs. 45 and in Europe 121 vs. 69 by our closest competitor). Tiani are proud to be number 1 and that they are able to offer number 1 solutions for the widest range of healthcare IT applications.

Tiani Spirit provide the software for the HIE functionality across Lancs & S Cumbria and act as a Data Processor. Tiani Spirit UK Limited is obliged to abide by all relevant UK and European Union legislation and is registered with the Information Commissioners Office (ICO). The requirement to comply with this legislation shall be devolved to employees and agents of Tiani Spirit UK Limited who may be held personally accountable for any breaches of information security for which they may be held responsible. Tiani Spirit UK Limited shall comply with the following legislation and other legislation as appropriate:

- The Data Protection Act (2018)
- General Data Protection Regulation 2016



- The Data Protection (Processing of Sensitive Personal Data) Order 2000.
- The Copyright, Designs and Patents Act (1988)
- The Computer Misuse Act (1990)
- The Health and Safety at Work Act (1974)
- Human Rights Act (1998)
- Regulation of Investigatory Powers Act 2000
- Freedom of Information Act 2000
- Health & Social Care Act 2012

Maywoods provides an audit facility for LPRES

From the outset of the LPRES Programme, the central team recognised the need to support users of the service and the need to protect and monitor both the publishing and consuming of data via the LPRES HIE. To support this Maywoods was commissioned to provide an Audit Tool. The audit tool servers are currently hosted at Blackpool Teaching Hospital within their IT infrastructure.

The Audit Tool provides the following to Organisations utilising the LPRES Service:

- An end to end auditing facility to ensure important clinical documentation is received from secondary care organisations and delivered to primary care colleagues.
- Different status indicators are provided within the audit tool so that local staff at a glance can confirm successful receipt of a document or identify that a problem was encountered and act accordingly.
- End to end rejection messages are received and acted up ie No Longer Our Patient at this practice.
- Permission to access the audit tool can only be granted by an Administrator (there are four central administrators of the audit tool). Please note only Administrators actually see the Administration button.
- Permission to access the audit tool will only be granted upon completion of an Access Request form – signed off by the requestors Line Manager.
- There is a remove user function should Administrators be requested to remove a user.
- For any IG queries a small number of staff within an Organisation have been granted IG status.
 - This enables a query to establish who has looked at a record using NHS numbers. NHS number stored in the audit tool.
 - Or what record a User has looked at. Please note this is activated by request either from staff or patients. User/staff name stored for this purpose.
- In addition to the audit tool, Maywoods will be storing staff names on a database in order to record access to LPRES in order to produce statistics regarding usage (See Appendix C). Should we require

amendments or enhancements to be made to the audit tool we commission Maywoods to provide this development as an ad hoc piece of work.

- The ICS pay Maywoods an annual Service and Support Maintenance amount to provide a fully managed service wrap for the Audit Tool.

DATA, PROCESSES AND SUPPORTING ASSETS

This part allows you to define and describe the scope of the processing in detail.

What is the data processed?	
List the data collected and processed. Define for each the storage durations, the recipients and persons with access	<p>Data and processes</p> <p>Define and describe the scope in detail:</p> <ul style="list-style-type: none"> - the personal data concerned, their recipients and storage



LPRES is a view-only processing system. Data is retrieved to the LPRES viewer or the WellPRES/Mi-PRES platform by accessing LPRES but it is not persisted or stored.

Access to the elements of a clinical record viewed is controlled via login to the host organisation/data controller's EPR system to ensure that only those with a legitimate clinical relationship with the patient, or the patient themselves in respect to Mi-PRES (via an NHS Login), can view that record.

LPRES improves the existing flows of documents directly into GP's workflow and the MIG/eMIS processing matches them to the correct GP clinical record, it also allows cross boundary transmission and sharing of clinical documents.

GP's now receive timely documents from the providers, reducing administration costs (scanning of documents and matching of records) and helping to reduce referrals. Providers benefit by saving costs, improving data quality and reducing administration time.

LPRES allows front line clinicians to view these documents and the GP summary care record i.e. Healthcare Gateway MIG ten tab view (Summary, Diagnosis, Medications, Risks & Warnings, Investigations, Examinations, Patient Details, Problems, Events, Procedures). Data set HGLEIS30. Also, the eleventh tab - EPaCCS (EoL). Data set HGLEIS47 if available and coded for sharing.

In addition, clinicians will be able to view Special Patient Notes, data set HGLIS33 and Care Plans, data set HGLEIS31 to be replaced with HGLEIS73 if this additional information flow has been purchased via Healthcare Gateway.

Care Homes/Nursing Homes will now be able to access the full records of residents/patients/service users accessing their services. This means that Care Homes/Nursing Homes, with the necessary governance arrangements in place, will be able to view the most up to date information about their residents in the hospital or GP record. Appropriate information sharing is an essential part of the delivery of safe and effective care and residents may be put at risk if those who provide their care do not have access to relevant, accurate and up-to-date information about them.

Sensitive data excluded from retrieval follows the recommendations made by The Royal College of General Practitioners (RCGP) ethics committee and the Joint GP IT Committee (see Appendix B for exclusion list):

- Gender reassignment.
- Assisted conception and in vitro fertilisation (IVF)
- Sexually transmitted diseases (STD)
- Termination of pregnancy

durations

- description of the processes and personal data supporting assets for the entire personal data life cycle (from collection to erasure).

Recipient

Natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing. see Art. 4.9 of the [\[GDPR\]](#)

Personal data

Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

See [Art. 4.1 of \[GDPR\]](#)

Local councils publish social care plans to LPRES.

Documents published to LPRES to date include discharge summary documents, clinical letters, social care plans, alcohol & drug dependency care plans (CGL on behalf of LCC), pathology/radiology results. The Publishing Matrix document lists the documents published to LPRES and is updated when data controllers add to the documents they publish. There are plans, in future for Nursing Homes/Care Homes to also publish a document to a patient record e.g. discharge letter.

Data is stored centrally on the LPRES virtual private cloud (VPC) hosted by AWS/ANS to enable statistics to be produced regarding monitoring of the application, who is using it, information that LPRES requires to make it easier to run the service. Data items stored are per Appendix C

With the Diagnostic Viewer, clinicians/healthcare professionals are able to view CT Scans, x-rays, etc via the LPRES Viewer. The ResMD renders the Study and presents it as an i-frame within LPRES. The clinician is able to manipulate the Study. The clinician is unable to modify the Study. When the session has ended no data is stored on the ResMD server or in the LPRES viewer (i.e.non-persistent)

In regards to **WeILPRES/Mi-PRES**, most of the data is 'view only' being retrieved via LPRES. The data captured on the caremap and patient questionnaire responses (which are a part of the caremap) will be retained in line with the NHS retention standards.

Access to the elements of a clinical record viewed via the WeILPRES/Mi-PRES platform is controlled to ensure that only those with a legitimate clinical relationship with the patient, or the patient themselves, can view that record.

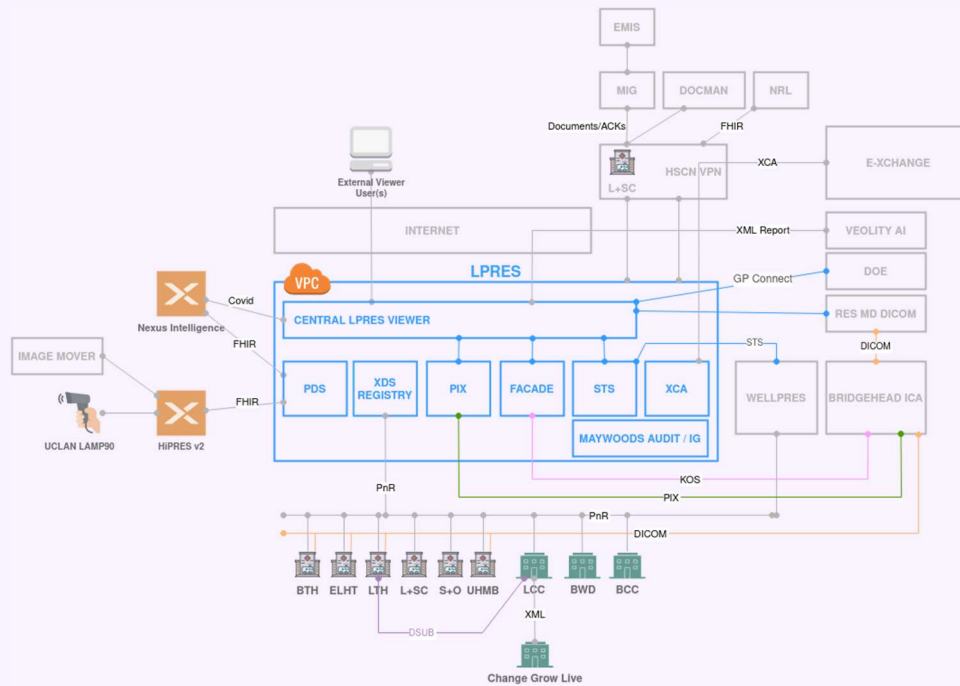
The Vitaly platform consists of a patient facing application, "Vitaly Patient" and a healthcare professional application, "Vitaly Managed Care".

The Vitaly Patient is used by the patient to :

- Access medical data from LPRES
- Perform Questionnaires regarding ongoing care plan
- Perform other assigned tasks and
- Communicate with the care team

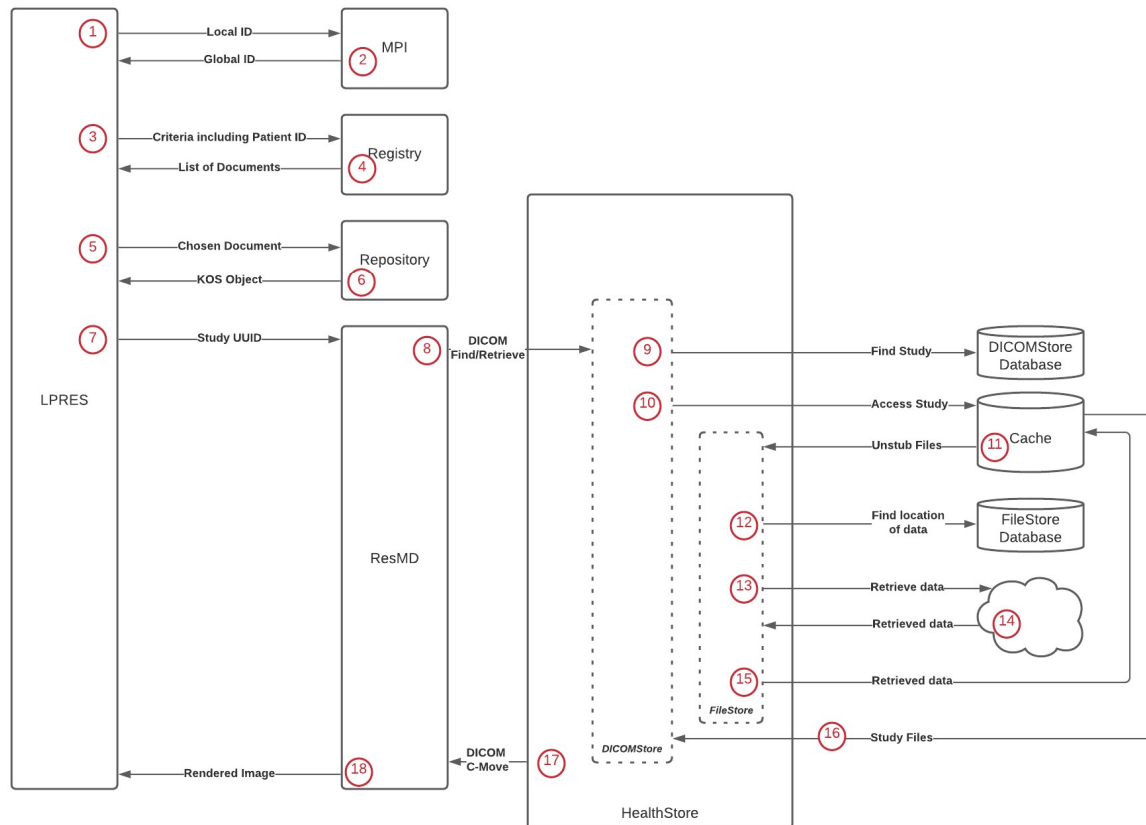
<p>For this reason there is a need of having a local patient record within the platform that is used for interoperability needs and application function. Patient Record Data is retrieved from LPRES and is mostly un-mutable. WellPRES/Mi-PRES accesses Patient Name and Last Name, Surname, DOB, NHS Number, and contact information of the Patient from LPRES.</p> <p>The Vitaly Managed Care retrieves all medical data from LPRES. Again there is a Local Patient Record (different from the Vitaly Patient one) used for the same purposes and having same data definition. Managed care produces some medical grade data that is stored in LPRES. Such data are Questionnaires Response documents. Other data that enable collaboration is kept locally within the Vitaly Platform (task definitions, care plan template, care team structure, events, notes, messaging). This data can contain sensitive and personal data. (See WellPRES/Mi-PRES DPIA).</p> <p>Data between Vitality Managed Care and Vitality Patient is exchanged both directly (local data) and indirectly (LPRES stored data).</p> <p>Regarding the LPRES viewer, data stored by the WellPRES/Mi-PRES solution (Questionnaire response documents) on the LPRES server is not accessed by the LPRES viewer.</p>	
<p>How does the life cycle of data and processes work?</p>	
<p>Present and describe how the product generally works (from the data collection to the data destruction, the different processing stages, storage, etc.), using for example a diagram of data flows (add it as an attachment) and a detailed description of the processes carried out.</p>	





Records are viewed using the LPRES viewer but remain within their host organisation's systems at all times.

XDSi Data Flow (Retrieval)



A clinician wishing to view a DICOM Study for a patient search for the patient using the LPRES Viewer. The clinician has the choice of performing a demographic search or using any of the patient's hospital IDs. The viewer issues a PIX or PDQ request against the Tiani MPI. ①.

The MPI returns the regional Global ID for the patient. ②.

The viewer then performs a search for the patient's documents using the Global ID upon the Regional XDS Registry. ③.

<p>The Regional XDS Registry returns a list of documents, with the information required to retrieve a copy from local XDS Repositories. ④.</p> <p>The clinician chooses the patient's document that they are interested in, in our case a DICOM Study. The viewer issues an XDS 'Retrieve Document Set' upon the local XDS Repository associated with the document. ⑤.</p> <p>The Local XDS Repository returns a KOS object. This is because a DICOM Study is being accessed. ⑥.</p> <p>The LPRES viewer recognizes that a KOS object has been retrieved and constructs an URL to send to the ResMD (PureWeb) DICOM Viewer. ⑦.</p> <p>ResMD uses the information within the URL string to determine the Study UUID and the VNA that contains the study. ResMD issues a DICOM C-Move against the VNA. ⑧.</p> <p>The VNA performs a look up to find the location of the DICOM files. ⑨.</p> <p>The VNA attempts to access the DICOM Files. ⑩.</p> <p>The DICOM Files have been stubbed. This causes the NTFS file system to trigger a reparse point, which triggers a FileStore unstub request. ⑪.</p> <p>FileStore determines where the files have been archived. ⑫.</p> <p>FileStore retrieves the data from the archive ⑬, ⑭. FileStore decompresses and decrypts the data. It calculates the files digital signatures and compare the signature to the original. If the signatures match the data is restored to the files. ⑮.</p> <p>DICOMStore now has access to the underlying DICOM files of the Study ⑯ and can complete the C-Move to ResMD ⑰.</p> <p>ResMD renders the study and presents it In-Frame to the LPRES viewer.</p>	
<p>What are the data supporting assets?</p>	
<p>List the data supporting assets (operating systems, business applications, database management systems, office suites, protocols, configurations, etc.)</p>	<p>Supporting asset</p>



<p>See diagram in previous section for data flows.</p> <p>Supporting systems include:</p> <ul style="list-style-type: none"> • LPRES VPC/Amazon Web Services (AWS) Cloud (supported by ANS as a Cloud Managed Service) • Tiani Spirit locally Hosted affinity domains • Maywoods' Audit Tool • Maywoods stats database • Bridgeheads ResolutionMD (ResMD) Enterprise Viewing Platform • Bridgeheads ICA (Independent Clinical Archive) HealthStore • EMIS/MIG • DOCMAN • Each of these additional systems are governed separately in relation to the collection, storage and management of personally identifiable data. • Google Authenticator App (two-step verification service) <p>LPRES simply provides a common platform and viewer which enables local care records to be viewed at a single location.</p>	<p>Asset on which personal data rely. Note: this may be hardware, software, networks, people, paper or paper transmission channels.</p>
---	--

Fundamental principles

This section allows you to build the compliance framework for privacy principles.

PROPORTIONALITY AND NECESSITY

This part allows you to demonstrate that you are implementing the necessary means to enable the persons concerned to exercise their rights.



Are the processing purposes specified, explicit and legitimate?	
<p>Explain why the processing purposes are specified, explicit and legitimate. How is the legal basis being specified?</p> <p>The LPRES viewer allows for viewing data directly by providing a route into local systems. However, given that personally identifiable health care data can be presented to an end user via the viewer, it is important to clarify explicitly the legitimate purpose for allowing this data.</p> <p>The LPRES viewer allows clinicians, regardless of their organisation's location to view more complete patient records from other health and social care organisations to improve clinical decision making at the point of care, i.e. direct care purposes.</p> <p>Given the fact that this system therefore supports the improved delivery of healthcare to individuals, this functionality is considered to be fundamental to the delivery of public responsibility of health and social care organisations. This execution of a public, or contractual, duty provides the justification and the supporting legal basis for selected individuals to access a patient record.</p>	<p>Principles relating to processing of personal data</p> <p>Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.</p> <p>See Art. 5.1 b) of [GDPR]</p>
What is the lawful basis for processing the data?	
<p>What is the legal basis for processing the data? – direct care, legislation or consent, (don't forget, consent should be a last resort and only used if there is no direct care or legislation in place). Remember to identify which Article 6 or 9 conditions will be used and if there is supporting legislation, what that legislation is, including the specific section of the legislation which supports the use of data for this purpose.</p>	<p>Justification of lawfulness</p> <ul style="list-style-type: none"> - The data subject has given consent to the processing of his or her personal data for one or more specific purposes - Processing is necessary for the performance of a



Personal Data means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Special Categories of Personal Data means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, 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.

The General Data Protection Regulation (GDPR) states that the processing of 'personal data' shall be lawful where it is:

- Article 6(1)(e) - Necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

And for processing special categories of personal data where it is:

- Article 9(2) (h) - Necessary for the purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services, carried out by or under the supervision of healthcare professionals or social work professional or by another person who in the circumstances owes a duty of confidentiality under an enactment or rule of law.

The Health and Social Care Act 2012 as amended by The Health and Social Care (Safety and Quality) Act 2015 also states the need to collect, record, store and use your personal data in order to provide healthcare services to you. These are the underpinning legitimate reasons for utilising and sharing this data.

contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract

-Processing is necessary for compliance with a legal obligation to which the controller is subject

- Processing is necessary in order to protect the vital interests of the data subject or of another natural person

- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller

- Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child

See [art. 6 of \[GDPR\]](#)

Is the data collected adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')?



Explain why each of the data collected is necessary for the purposes of your processing.	
<p>Need confirmation in here that there is no personal data being processed that isn't absolutely necessary for the purpose of the project. Is any information being collected that isn't required to complete the project?</p>	
<p>The LPRES viewer enables retrieval of the relevant GP record from EMIS and patients' documents from the relevant organisation's local affinity domains in a non-persistent view. This viewer is launched within patient context and within their local EPR system via a web services call to the centralised LPRES viewer or for organisations which do not have an ePR system, such as Care Homes/Nursing Homes there is a logon to the viewer via a two-step verification service (Google Authenticator).</p> <p>There are data items stored on the LPRES VPC to enable statistics to be generated (see Appendix C) Data collected to create statistics are necessary in order to monitor the application and run the service and will be retained in line with NHS Records Management Code of Practice 2021</p> <p>Role based access, i.e. the data presented to a user, will be based on the role of the user as determined by the host organisation/data controller. Therefore, different user types will have access to different elements of the care record. The Role based access control (RBAC) document for LPRES/shared care record is a controlled document which records when changes regarding access are updated. This document will be updated as appropriate for this project – Care Homes PoC, giving appropriate access to a Matron and/or Care Home Manager who will be a super user/senior user who will have access with an extra facility to add and remove patients/residents to a work list to set up the list of residents which other healthcare professionals within the organisation will only be able to access relevant residents' records.</p> <p>The care record and the published documents will be viewed by a clinician/healthcare professional who has a legitimate relationship with a patient for the purposes of direct care at the point of need to provide as full a picture as possible to be able to make appropriate care decisions leading to improved patient care.</p> <p>Sensitive data excluded from retrieval follows the recommendations made by The Royal College of General Practitioners (RCGP) ethics committee and the Joint GP IT Committee (please see list in Appendix B).</p> <p>Regarding WellPRES/Mi-PRES - Most of the data is 'view only' being retrieved via LPRES. The data captured on the caremap and patient questionnaire responses (which are a part of the caremap) will be retained in line with the NHS retention standards. (See WellPRES/Mi-PRES DPIA)</p>	<p>Data minimisation</p> <p>It is important to reduce the severity of the risks by minimizing the number of personal data that will be processed, by limiting such data to what is strictly necessary for the purposes for which they are processed (otherwise they should not be collected). Then, it also becomes possible to minimize the data themselves, via controls aimed at reducing their sensitivity.</p> <p>Minimizing the amount of personal data</p> <p>Reduce the severity of risks by limiting the amount of personal data to what is strictly necessary to achieve a defined purpose, otherwise the data shall be not collected.</p>



Is the data accurate and kept up to date?	
Describe what steps are taken to ensure the quality of the data.	<p>Quality of data</p> <p>Personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy'). See Art. 5.1 d) of [GDPR]</p>
<p>The responsibility for Data Quality remains with the organisation where source record data is held. The LPRES viewer is not responsible for the data that it presents.</p> <p>As such, data quality responsibility remains within the domain of the submitting organisation, and ongoing compliance will be monitored by the LPRES Operations team at regular intervals.</p> <p>Regarding WellPRES/Mi-PRES, the patient questionnaire is completed by the patient. In addition, by providing patients with access to their own records via the Mi-PRES platform it is likely that any errors in the data will be identified and the WellPRES project team should ensure that there are connections within the WellPRES/Mi-PRES viewer to allow users to highlight those errors and engage with the process to rectify them.</p>	
What is the storage duration of the data?	
Explain why the storage durations are justified by legal requirements and/or processing needs.	<p>Storage Durations</p> <p>Storage duration must be defined for each type of data and justified by the legal requirements and/or processing needs. Thus a distinction is made between common data and archived data, to which access will be limited to only the stakeholders concerned. An erasure mechanism must be</p>
<p>Ideally there will be a list here of all the data assets being processed, how long they will be held for, where the timescales have come from (i.e, Information Governance Alliance code of practice for records management). This should be stated for each organisation that holds the data.</p>	



All records will be maintained in line with National NHS Data Information Governance requirements and timescales, while also being aligned with local data asset registers.

Local Data (within LPRES, i.e. Questionnaires from WeLPRES/Mi-PRES) and data stored on the LPRES VPC for statistical purposes will be retained within the system in line with local retention standards following the closure of the system in line with national Data Retention standards as defined in the Records Management Code of Practice 2021 - NHSX.

Each organisation will operate in compliance with:

- NHS Records Management Code of Practice 2021
- GDPR
- Health and Social Care Act
- DSP Toolkit
- Cyber Security-Essentials
- ICO Registration

This DPIA will be reviewed initially by the L&SC HCP ICS Collaborative IG group and all internal IG leads within each organisation involved. This DPIA will be reviewed at six monthly intervals to ensure it accurately reflects the programme as it develops. In respect of S2C this has been reviewed and the cross-border data sharing will continue across Cheshire & Mersey and Lancs & South Cumbria, for direct care purposes under the same legal basis as LPRES, the shared care record across Lancs & South Cumbria.

implemented to archive common data or purge archived data at the end of their storage duration. Functional traces will also have to be purged, as will technical logs which may not be stored indefinitely

Records Management Code of Practice for Health and Social Care 2016: <https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/codes-of-practice-for-handling-information-in-health-and-care/records-management-code-of-practice-for-health-and-social-care-2016>

CONTROLS TO PROTECT THE PERSONAL RIGHTS OF DATA SUBJECTS

This part allows you to demonstrate that you are implementing the necessary means to enable the persons concerned to exercise their rights.

How are the data subjects informed of the processing?	
Describe what information is given to the data subjects and what are the means to do it.	Informing data subjects



<p>LPRES is accessed for direct care only by clinicians and care workers who have a legitimate relationship to the patient, or accessed by the patient themselves in relation to the Mi-PRES platform.</p> <p>Each of the hosting organisations/data controllers have reviewed their privacy statements to ensure that data subjects have been informed about how their healthcare data is used. Regarding WellPRES/Mi-PRES the patients are informed whilst being given access to the platform, if they wish to use it as part of their treatment, they are informed and have access to the terms and conditions of the platform.</p> <p>Various NHS webpages have included information to inform the public, such as the Northwest SIS webpage, Healthier Lancashire and South Cumbria webpage with links to contacts if further information is required.</p>	<p>Ensure that the subjects are informed. Confirm that the processing is not covered by an exception and is not subject to specific conditions.</p>
<p>If consent is your lawful basis how is the consent of data subjects obtained?</p>	
<p>Describe the controls intended to ensure that users' consent has been obtained.</p>	<p>Definition: consent</p> <p>Any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. See Art. 4.10 of [GDPR]</p> <p>Principle: Consent</p> <p>Allow data subjects to make a free, specific and informed choice. Determine whether the processing relies on a legal basis other than consent pursuant to Art. 6 of the [GDPR]</p>
<p>Not applicable as we utilise the Legal Basis stated above.</p>	
<p>How can data subjects exercise their rights of access and to data portability?</p>	
<p>Describe the controls intended for enabling data subjects to access, receive and transmit their data.</p>	<p>Right of access</p>




<p>All the host organisations/Data Controllers are compliant with all Data Protection Act and GDPR principles.</p> <p>Each Controller fulfils their commitments to Personal Privacy and Confidentiality responsibilities in relation to LPRES and the WellPRES/Mi-PRES platform and this commitment is published within their local Privacy Policies, Cookie Policies and Fair Processing Notices.</p> <p>All patients/residents have a legal right to access their own health and care record. In order to exercise this right, the data subject must make a subject access request in writing, by email or verbally to the organisation providing their care. Requests may only be made on behalf of a data subject by someone else if the data subject has provided consent or there is another legal basis for disclosure, such as, an LPA (Lasting Power of Attorney) or a mental health advocate.</p>	<p>The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the information described in Art. 15 of [GDPR]</p> <p>Right to data portability</p> <p>The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, see Art. 20 of [GDPR]</p>
<p>How can data subjects exercise their rights to rectification and erasure?</p>	
<p>Describe the controls intended for enabling data subjects to rectify and erase their data.</p> <p>All the host organisations/Data Controllers are compliant with all Data Protection Act and GDPR principles.</p> <p>Each Controller fulfils their commitments to Personal Privacy and Confidentiality responsibilities in relation to LPRES and the WellPRES/Mi-PRES platform and this commitment is published within their local Privacy Policies, Cookie Policies and Fair Processing Notices.</p>	<p>Right to rectification</p> <p>The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.</p> <p>Right to erasure</p> <p>The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay, see Art. 17 of [GDPR]</p>



How can data subjects exercise their rights to restriction and to object?	
Describe the controls intended for enabling data subjects to restrict and to object to the processing of their data.	<p>Right to restricting of processing</p> <p>The data subject shall have the right to obtain from the controller restriction of processing, see Art. 18 of [GDPR]</p>
<p>All the host organisations/Data Controllers are compliant with all Data Protection Act and GDPR principles.</p> <p>Each Controller fulfils their commitments to Personal Privacy and Confidentiality responsibilities in relation to LPRES and the WellPRES/Mi-PRES platform and this commitment is published within their local Privacy Policies, Cookie Policies and Fair Processing Notices.</p>	
If there is a Data Processor involved, are the obligations of the processors clearly identified and governed by a contract?	
For each processor, describe the responsibilities (duration, scope, purpose, documented processing instructions, prior authorisation) and provide the contracts, codes of conduct and certifications determining its missions and obligations.	<p>Principle: Subcontracting</p> <p>A processing contract must be signed with each processor, setting out all of the aspects stipulated in Art. 28 of the [GDPR]: duration, scope, purpose,</p>



<p>The following third party processor / sub-processors are involved in providing services for the ICS and or for this project.</p> <p>The ICS will be asked to confirm they have responsibility for ensuring GDPR compliant contracts and processor agreements are in place and for the ongoing management of the third party arrangements.</p> <p>ANS have been contracted by the HL&SC ICS to act as a Data Processor on behalf of the LPRES programme.</p> <p>AWS and Tiani Spirit are contracted as sub-processors within the ANS contract/service wrap.</p> <p>Please note: The Contract has been reviewed/renewed April 2021.</p> <p>ANS responsibilities are set out within the attached 'Data Processing Agreement' included below with AWS and Tiani included as sub-processors.</p>  <p>LSC ICS Processing Agreement between</p> <p>Maywoods – have an annual contract covering the Audit Tool and support associated with this. We renew each year 1st April to 30th March.</p> <p>Bridgehead Software supplying the ICA /ResMD imaging platform</p>	<p>documented processing instructions, prior authorisation where a processor is engaged, provision of any documentation providing evidence of compliance with the [GDPR], prompt notification of any data breach, etc.</p> <p>Definition: Processor</p> <p>Natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller, see Art. 4.8 of [GDPR].</p> <p>The processor and any person acting under the authority of the controller or of the processor, who has access to personal data, shall not process those data except on instructions from the controller, unless required to do so by Union or Member State law, see Art. 29 of [GDPR].</p>
<p>In the case of data transfer outside the United Kingdom, are the data adequately protected?</p>	
<p>For each country outside the United Kingdom where data are stored or processed, name it and tell if it is acknowledged as offering an adequate level of data protection or describe the provisions concerning the transfer.</p>	<p>Transfers</p> <p>Depending on the country in question, you will have to justify the choice of remote hosting and indicate</p>



No data is being transferred outside of the UK. All data remains within the source system and each source system is currently located within the UK.

the legal supervision arrangements implemented in order to ensure adequate protection of the data subject to a cross-border transfer. That is :

- European Union
- Country recognized as providing adequate protection by the EU
- Transfer to the United States to a company which has joined the Privacy Shield
- Other country

See [art. 44 to 49 of \[GDPR\]](#)

Risks

This section allows you to assess the privacy risks, taking into account existing or planned controls.

Risk Factors to consider:

- Illegitimate access to data;
- Unwanted modification of data
- Data disappearance

PLANNED OR EXISTING MEASURES

This section allows you to identify controls (existing or planned) that contribute to data security.



#	Risk Ref	Risk Description	Mitigating Control(s)	Likely	Severity	Score
			(See details below)	(See details below)		
1	Governance	That Data Controllers are not adhering to their responsibilities within their organisations	Annual review of DSP toolkit and GDPR is undertaken across all stakeholders. ICO Registration expected. https://www.dsptoolkit.nhs.uk/OrganisationSearch/RXL	Remote	Some Impact	
2	Supplier	Lack of contracts leave Controller/Processor relationships unresolved leading to inability to enforce data protection requirements.	Evidence of Supplier Data Processors signed contracts required. Possibility of enforcement action is high. Existing contracts have now been re-negotiated (April 2021) to ensure GDPR compliance.	Remote	Serious Harm	
3	GDPR	Controller organisations do not comply with GDPR Principles around User Rights	All controllers regularly audited for internal GDPR compliance	Remote	Some Impact	
4	Sharing	Personal and Sensitive identifiable data is accessed, or shared, inappropriately	Strong Access Control mechanisms built into LPRES (currently role-based access via EPR). Also, to include the WellPRES/Mi-PRES platform (NHS Login). To include Care Homes/Nursing homes where role-based access will be via Google authentication/audit/ on-boarding process/the nursing home to set up a work list (to restrict access).	Reasonable Possibility	Some Impact	
5	Malware	Service could potentially be under threat of cyberattacks/software viruses	Cyber Security service provided by the data controllers for the EPRs.	Reasonable Possibility	Some impact	



6	Supplier	Service not accessible due to technical failure	ANS service support to identify failure and inform users when service will be returned within contractual SLA's.	Remote	Some Impact	
7	GDPR	Service not available – causing potential data breach	Reporting procedure strengthened, to enable potential backup procedures/Business Continuity Plans and to include IG managers/DPOs, to inform of service unavailability/outages and enabling DPO function decision making to report to ICO, if required/as appropriate, within required timeframes.	Remote	Some Impact	
8	GDPR	Non authorised data disclosure	All data processing activities are end to end audited. If data has leaked by malicious professional user there will be data to prove who, accessed what and when	Remote	Some Impact	
9	GDPR	Archived, redacted, removed or inappropriate data being transmitted via the shared record due to lack of robust procedures around record removal.	LPRES/S2C works by displaying non-persisted “allowed messages” determined at the local level by the data controller. The data controller retains the ability to stop sending all messages from archived, redacted, or removed patient records and LPRES and the S2C data exchange will only utilise active NHS numbers when displaying data.	Remote	Serious Harm	
10	Malware	Internet facing service could potentially be under threat by hackers/hacking.	Penetration testing has been done by Sapphire	Reasonable Possibility	Some impact	
11	GDPR	Minimum criteria not achieved by the nursing/care home to access the SCR	The Nursing home/care home will not be given access to the SCR (LPRES) if the minimum criteria is not achieved	Remote	Low impact	

EXAMPLE - Linked to Risk Register Information Risks

Education	Breach of IG policies and guidance due to lack of visibility, communication and training
------------------	--



GDPR	Non-compliant with GDPR implementation
Malware	Threat from malicious links/attachments
Process	Information is lost/ processed in a non-compliant manner due to gaps in processes and poor controls
Purchasing	Limited governance over low spends allows DPIA process bypass
Sharing	Sharing information inappropriately or illegally due to immature technology or understanding of legislation
Supplier	Suppliers breach Privacy Law due to poor information handling practices/ IT security

EXAMPLE Mitigating Control(s)

Logical Security Control

Encryption	Means implemented for ensuring the confidentiality of data stored (in the database, in flat files, backups, etc.), as well as the procedure for managing encryption keys (creation, storage, change in the event of suspected cases of data compromise, etc.). Describe the encryption means employed for data flows (VPN, TLS, etc.) implemented in the processing.
Anonymisation	Indicate here whether anonymization mechanisms are implemented, which ones and for what purpose. Remember to clearly distinguish between anonymous and pseudonymous data.
Partitioning	Implementation of data partitioning helps to reduce the possibility that personal data can be correlated and that a breach of all personal data may occur.



Logical Access Control	Methods to define and attribute users' profiles. Specify the authentication means implemented. Where applicable, specify the rules applicable to passwords (minimum length, required characters, validity duration, number of failed attempts before access to account is locked, etc.).
Traceability (logging)	Policies that define traceability and log management.
Archiving	Where applicable, describe here the processes of archive management (delivery, storage, consultation, etc.) under your responsibility. Specify the archiving roles (offices of origin, transferring agencies, etc.) and the archiving policy. State if data may fall within the scope of public archives.
Paper document security	Where paper documents containing data are used during the processing, indicate here how they are printed, stored, destroyed and exchanged.
Minimising the amount of personal data	The following methods could be used: Filtering and removal, reducing sensitivity via conversion, Reducing the identifying nature of data, Reducing data accumulation, Restricting data access

Physical Security Control

Operating security	Policies implemented to reduce the possibility and the impact of risks on assets supporting personal data.
Clamping down on malicious software	Controls implemented on workstations and servers to protect them from malicious software while accessing less secure networks.
Managing workstations	Controls implemented on workstations (automatic locking, regular updates, configuration, physical security, etc.) to reduce the possibility to exploit software properties (operating systems, business applications etc.) to adversely affect personal data.
Website security	Implementation of ANSSI's Recommendations for securing websites.



Backups	Policies and means implemented to ensure the availability and/or integrity of the personal data, while maintaining their confidentiality.
Maintenance	Policies describing how physical maintenance of hardware is managed, stating whether this is contracted out. Indicate whether the remote maintenance of apps is authorized, and according to what arrangements. Specify whether defective equipment is managed in a specific manner.
Processing Contracts	<p>Regulate the procurement relations via a contract signed intuitu personæ.</p> <ul style="list-style-type: none"> - Require the processor to forward its Information Systems Security Policy (PSSI) along with all supporting documents of its information security certifications and append said documents to the contract. Ensure that the measures pursuant to its PSSI comply with the ICO's recommendations in this respect. - Precisely determine and set, on a contractual basis, the operations that the processor will be required to carry out on personal data: <ol style="list-style-type: none"> 1) The data to which it will have access or which will be transmitted to it. 2) The operations it must carry out on the data. 3) The duration for which it may store the data. 4) Any recipients to which the data controller requires it to transmit the data. 5) The operations to be carried out at the end of the service (permanent deletion of data or return of the data in the context of reversibility then destruction of data at the processor's). 6) The security objectives set by the data controller. - Determine, on a contractual basis, the division of responsibility regarding the legal processes aimed at allowing the data subjects to exercise their rights. - Explicitly prohibit or regulate use of tier-2 processors. - Clarify in the contract that compliance with the data protection obligations is a binding requirement of the contract.
Network security	Depending on the type of network on which the processing is carried out (isolated, private or Internet). Specify which firewall system, intrusion detection systems or other active or passive devices are in charge of ensuring network security.
Physical access control	Policies to ensure physical security (zoning, escorting of visitors, wearing of passes, locked doors and so on). Indicate whether there are warning procedures in place in the event of a break-in.
Monitoring network activity	Monitor intrusion detection systems and intrusion prevention systems in order to analyse network (wired networks, Wi-Fi, radio waves, fibre optics, etc.) traffic in real time and detect any suspicious activity suggestive of a cyber-attack scenario.



Hardware security	Indicate here the controls bearing on the physical security of servers and workstations (secure storage, security cables, confidentiality filters, secure erasure prior to scrapping, etc.).
Avoiding sources of risk	Documentation on implantation area, which should not be subject to environmental disasters (flood zone, proximity to chemical industries, earthquake or volcanic zone, etc.). Specify if dangerous products are stored in the same area.
Protecting against non-human sources of risks	Policies describing the means of fire prevention, detection and fighting. Where applicable, indicate the means of preventing water damage. Also specify the means of power supply monitoring and relief.

Organisational Control

Organisation	Specify whether a person is responsible for the enforcement of privacy laws and regulations. Specify whether there is a monitoring committee (or equivalent) responsible for the guidance and follow-up of actions concerning the protection of privacy.
Policy	Set out important aspects relating to data protection within a documentary base making up the data protection policy and in a form suited to each type of content (risks, key principles to be followed, target objectives, rules to be applied, etc.) and each communication target (users, IT department, policymakers, etc.).
Managing Privacy risks	Policy describing processes to control the risks that processing operations performed by the organization pose on data protection and the privacy of data subjects (building a map of the risks, etc.)
Integrating privacy protection in projects	Existence of a policy designed integrate the protection of personal data in all new processing operations.



Managing personal data violations	Existence of an operational organization that can detect and treat incidents that may affect the data subjects' civil liberties and privacy.
Personnel management	Existence of a policy describing awareness-raising controls are carried out with regard to a new recruit and what controls are carried out when persons who have been accessing data leave their job.
Relations with third parties	Existence of a policy and processes reducing the risk that legitimate access to personal data by third parties may pose to the data subjects' civil liberties and privacy.
Supervision	Existence of a policy and processes to obtain an organization able to manage and control the protection of personal data held within it.

Severity Definitions

Severity	Description
Minimum Impact	<p>Data subjects may encounter significant inconveniences, which they will be able to overcome despite a few difficulties</p> <p>Examples :</p> <ul style="list-style-type: none"> - physical : minor physical ailments (minor illness due to disregard of contraindications), defamation resulting in physical or psychological retaliation, etc. - material : Unanticipated payments (fines imposed erroneously), denial of access to administrative or commercial services , Receipt of unsolicited targeted mailings likely to damage the reputation of data subjects, etc. - moral : minor but objective psychological ailments, feeling of invasion of privacy without irreversible damage, intimidation on social networks, etc.
Some Impact	<p>Data subjects may encounter significant consequences, which they should be able to overcome albeit with real and serious difficulties</p> <p>Examples:</p> <ul style="list-style-type: none"> - physical : serious physical ailments causing long-term harm (worsening of health due to improper care, or disregard of



	<p>contraindications), Iteration of physical integrity for example following an assault, an accident at home, work, etc.</p> <ul style="list-style-type: none"> - material : misappropriation of money not compensated, targeted, unique and non-recurring, lost opportunities (home loan, refusal of studies, internships or employment, examination ban), loss of housing, loss of employment, etc. - moral : serious psychological ailments (depression, development of a phobia), feeling of invasion of privacy with irreversible damage, victim of blackmailing, cyberbullying and harassment, etc.
Serious Harm	<p>Data subjects may encounter significant, or even irreversible, consequences, which they may not overcome</p> <p>Examples :</p> <ul style="list-style-type: none"> - physical : long-term or permanent physical ailments, permanent impairment of physical integrity, death - material : financial risk, substantial debts, inability to work, inability to relocate, loss of evidence in the context of litigation, loss of access to vital infrastructure (water, electricity), etc. - moral : long-term or permanent psychological ailments, criminal penalty, abduction, loss of family ties, inability to sue, change of administrative status and/or loss of legal autonomy (guardianship), etc.

Likelihood Definitions

Likelihood	Description
Remote	It seems difficult for the selected risk sources to materialize the threat by exploiting the properties of supporting assets (e.g.: theft of paper documents stored in a room protected by a badge reader).
Reasonable Possibility	It seems possible for the selected risk sources to materialize the threat by exploiting the properties of supporting assets (e.g.: theft of paper documents stored in offices that cannot be accessed without first checking in at the reception).
More Likely than not	It seems extremely easy for the selected risk sources to materialize the threat by exploiting the properties of supporting assets (e.g.: theft of paper documents stored in the public lobby).



Risk Mapping

Severity of Impact	Serious Harm	Low Risk	High Risk	High Risk
	Some Impact	Low Risk	Medium Risk	High Risk
	Minimum Impact	Low Risk	Low Risk	Low Risk
		Remote	Reasonable Possibility	More Likely than not
		Likelihood of Harm		



Definitions

Encryption

Measure making personal data unintelligible to anyone without access authorization (symmetric or asymmetric encryption, use of public algorithms known to be strong, authentication certificate, etc.).

Anonymisation

Process removing the identifying characteristics from personal data. To assess the robustness of an anonymization processes, see the [WP29 guidelines](#).

Pseudonymisation

Processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person. Pseudonymisation reduces the linkability of a dataset with the original identity of a data subject; as such, it is a useful security measure but not a method of anonymisation.

Data partitioning

Data organization methods that reduce the possibility that personal data can be correlated and that a breach of all personal data may occur. For instance, by identifying the personal data useful only to each business process and logically separating them.

Logical access controls

Means implemented to limit the risks that unauthorized persons will access personal data electronically, it requires among other things to:

- **Manage users' profiles** by separating tasks and areas of responsibility (preferably in centralized fashion) to limit access to personal data exclusively to authorized users by applying need-to-know and least-privilege principles.



- **Withdraw the rights of employees, contracting parties and other third parties when they are no longer authorized to access a premises or a resource or when their employment contract ends.**

Password

Passwords shall be composed of a minimum of eight characters; must be renewed if there is the least concern that they may have been compromised and, possibly, periodically (every six months or once a year) and must include a minimum of three of the four kinds of characters (capital letters, lower case letters, numerals and special characters); when a password is changed, the last five passwords may not be reused; the same password should not be used for different accesses; passwords should not be related to one's personal information (including name or date of birth.). Define a maximum number of attempts beyond which a warning is issued, and authentication is blocked (temporarily or until it is manually unblocked).

Authentication

Every person with legitimate access to personal data (employees, contracting parties and other third parties) should be identified by a unique identifier. Choose an authentication method to open sessions that is appropriate to the context, the risk level and the robustness expected. Recommendations: if the risks are not elevated, a password may be used; however, if the risks are higher, use a one-time password token but change the default activation password, or, when part of the password is sent by SMS, a card with a PIN code, an electronic certificate or any other form of strong authentication.

Surveillance

Set up a logging architecture to allow early detection of incidents involving personal data and to have information that can be used to analyse them or provide proof in connection with investigations.

Archiving

Procedures preserving and managing the electronic archives containing the personal data intended to ensure their value (specifically, their legal value) throughout the entire period necessary (transfer, storage, migration, accessibility, elimination, archiving policy, protection of confidentiality, etc.).



Filtering and removal

When data are being imported, different types of metadata (such as EXIF data with an image file attached) can unintentionally be collected. Such metadata must be identified and eliminated if they are unnecessary for the purposes specified.

Reducing sensitivity via conversion

Once sensitive data have been received, as part of a series of general information or transmitted for statistical purposes only, these can be converted into a less sensitive form or pseudonymized. For example:

- if the system collects the IP address to determine the user's location for a statistical purpose, the IP address can be deleted once the city or district has been deduced
- if the system receives video data from surveillance cameras, it can recognize people who are standing or moving in the scene and blur them
- if the system is a smart meter, it can aggregate the use of energy over a certain period, without recording it in real time

Project Management

Measures taken to integrate the protection of personal data in all new processing operations (trusted names, guidelines, methodology for risk management or other internal methodology).

Personal data breach

Breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Reducing the identifying nature of data

The system can ensure that:

- the user can use a resource or service without the risk of disclosing his/her identity (anonymous data)
- the user can use a resource or service without the risk of disclosing his/her identity, but remain identifiable and responsible for this use (pseudonymous data)
- the user can make multiple uses of resources or services without the risk of these different uses being linked together (data cannot be



correlated)

- the user can use a resource or service without the risk of others, third parties in particular, being able to observe that the resource or service is being used (non-observability)

The choice of a method from the list above must be made on the basis of the threats identified. For some types of threat to privacy, pseudonymization will be more appropriate than anonymization (for example, if there is a traceability need). In addition, some threats to privacy will be addressed using a combination of methods.

Reducing data accumulation

The system can be organized into independent parts with separate access control functions. The data can also be divided between these independent sub-systems and controlled by each sub-system using different access control mechanisms. If a sub-system is compromised, the impacts on all of the data can thus be reduced.

Restricting data access

The system can limit data access according to the "need to know" principle. The system can separate the sensitive data and apply specific access control policies. The system can also encrypt sensitive data to protect their confidentiality during transmission and storage. Access to temporary cookies which are produced during the data processing must also be protected.



List of GP's across Lancashire and South Cumbria as included on the Data Sharing Agreement (DS002065) on the Information Sharing Gateway (ISG)

A82003 DR G R MURRAY AND PARTNERS
A82005 CENTRAL LAKES MEDICAL GROUP
A82007 DUKE STREET (ICO REGISTERED AS DRS MACDONALD WEAR & WILKINSON)
A82008 NORWOOD MEDICAL CENTRE (ICO REGISTERED AS DR J COUTTS AND PARTNERS)
A82009 BRIDGEGATE MEDICAL CENTRE (ICO REGISTERED AS DR WAIND AND PARTNERS)
A82010 ABBEY ROAD SURGERY
A82025 CAPTAIN FRENCH SURGERY (ICO REGISTERED AS DRS M BRENNAN AND PARTNERS)
A82026 THE JAMES COCHRANE PRACTICE
A82027 STATION HOUSE SURGERY (Registered with ICO as DR ELLIOTT & PARTNERS)
A82030 THE LUNESDALE SURGERY (DRS, KAYE, BEAGAN, WEEKS, BRUNT AND UNDERWOOD)
A82033 WATERLOO HOUSE SURGERY (ICO REGISTERED AS DRS ADEBAYO, STANGROOM AND WALKER)
A82039 MARKET STREET PRACTICE (ICO REGISTERED AS DR O'DONOVAN AND PARTNERS)
A82046 WINDERMERE AND BOWNESS MEDICAL PRACTICE (ICO Registration through One Medical Ltd)
A82053 NUTWOOD MEDICAL PRACTICE
A82062 ATKINSON HEALTH CENTRE PRACTICE (Drs Wiejak & Jebur)
A82068 Dr Johnston & Partners
A82070 ST MARY'S SURGERY (ICO REGISTERED AS Dr WINTER-BARKER & PARTNERS)
A82071 BURNETT EDGAR MEDICAL CENTRE
A82072 RISEDALE SURGERY
A82077 LIVERPOOL HOUSE SURGERY
A82608 SEDBERGH MEDICAL PRACTICE
A82621 DR PRAKASH JAIN
A82629 DR KARAMCHANDANI & DR JAVERIA (known as The Family Practice)
A82647 CARTMEL SURGERY (ICO Registered Dr J A Colclough)
A82650 HAVERTHWAITE SURGERY (ICO REGISTERED AS DR Philip Edwards)
A82651 DUDDON VALLEY MEDICAL PRACTICE
Ansdell Medical Centre



Ash Tree House Medical
ASH TREES SURGERY
B82061 BENTHAM MEDICAL PRACTICE
Beechwood Surgery
BROADWAY MEDICAL CENTRE (FLEETWOOD)
FCMS(NW) Ltd
FERNBANK SURGERY
Fleetwood Community Care Limited
Fleetwood Health Centre Limited
Fleetwood Surgery
Garstang Medical Practice
Holland House Surgery
Kirkham Health Centre
Lancaster Medical Practice
Lockwood Surgery
P81003 ST JAMES MEDICAL CENTRE
P81004 ELIZABETH STREET PRACTICE (ico reg. Dr Sanjeev Maharah
P81005 LITTLE HARWOOD HEALTH CENTRE
P81008 YORKSHIRE STREET SURGERY
P81010 WITHNELL HEALTH CENTRE ico reg. DRS JONES ROBINSON & NARLA
P81014 Ormskirk Medical Practice
P81015 LYTHAM ROAD SURGERY
P81016 WATERLOO MEDICAL CENTRE
P81017 SABDEN & WHALLEY MEDICAL GROUP
P81018 ST FILLANS MEDICAL CENTRE (ico reg. DR O'CONNOR & PARTNERS)
P81020 Burnley Group Practice
P81022 WITTON MEDICAL CENTRE (ico reg. DRS FOURIE, AHMED, TOOR)
P81025 RICHMOND HILL
P81027 IRWELL MEDICAL PRACTICE
P81032 REEDYFORD HEALTH CARE GROUP



P81033 COPPULL MEDICAL PRACTICE
P81035 COLNE ROAD SURGERY
P81036 PEEL HOUSE MEDICAL CENTRE
P81038 The Chorley Surgery
P81039 Manor Primary Care
P81040 LONGTON HEALTH CENTRE
P81041 PARKGATE SURGERY
P81042 ADELAIDE STREET SURGERY (Dr Augustine and partners)
P81043 THE MEDICAL CENTRE SOUTH KING STREET BLACKPOOL
P81044 LIBRARY HOUSE SURGERY
P81045 THE ELMS
P81046 PARK VIEW SURGERY
P81047 PRESTIGE MEDICAL GROUP
P81051 Darwen Healthcare
P81053 BRIERCLIFFE MEDICAL CENTRE
P81054 MARTON MEDICAL PRACTICE (DRS RAJNISH LUTHRA, BINEETA CHOUDHARY, HAROON CHOUDHRY & EIRINI TSOUMA)
P81055 BERRY LANE MEDICAL CENTRE
P81057 WORDEN MEDICAL CENTRE ico. reg: Dr Campbell and Partners
P81058 ST GEORGES SURGERY
P81059 GREAT ECCLESTON HEALTH CENTRE (ico reg. DR CASSELS & PARTNERS)
P81061 REDLAM SURGERY (ico reg. DRS CALOW, McKEATING & AHMED)
P81062 REGENT HOUSE SURGERY
P81063 ST PAUL'S MEDICAL CENTRE
P81065 The Pendle Medical Partnership - Earby and Colne Corner
P81066 LAYTON MEDICAL CENTRE
P81067 DRS WILSON, BROOKS, ACTON, MALIK & CHESWORTH (The Healthcare Centre)
P81069 PENDLESIDE MEDICAL PRACTICE
P81070 PENDLE VIEW MEDICAL CENTRE
P81071 THE NEW HALL LANE PRACTICE
P81072 GLENROYD MEDICAL CENTRE (ico reg. DRS SHEARER, NOLAN)



P81073 CLEVELEYS GROUP PRACTICE
P81074 HIGHFIELD SURGERY (ico reg. DR PRIESTLEY & PARTNERS)
P81076 SANDY LANE SURGERY ico reg. DRS GRACE AND PARTNERS
P81078 BARNOLDSWICK MEDICAL CENTRE
P81081 ARNOLD MEDICAL CENTRE (ico reg. MANISH RAUT & PARVATHI SHAJIL)
P81082 THE RYAN MEDICAL CENTRE
P81083 ROSLEA SURGERY, PR5 6PE
P81084 HALL GREEN SURGERY
P81088 WHITWORTH MEDICAL CENTRE
P81092 THE CRESCENT SURGERY (ico reg. DRS ECCLESTON & MATTHEWS)
P81095 THURSBY SURGERY
P81096 Parbold Surgery
P81099 DR MACKENZIE AND PARTNERS
P81100 THE CASTLE MEDICAL GROUP
P81103 North Preston Medical Practice
P81107 STONEBRIDGE SURGERY (ico reg. DRS HAWARD, EVANS, MUKERJI, TAYLOR, MASON)
P81112 BEACON PRIMARY CARE
P81113 PARK VIEW SURGERY
P81115 BLOOMFIELD MEDICAL CENTRE
P81117 CENTRAL PARK SURGERY
P81118 ILEX VIEW MEDICAL PRACTICE
P81119 Lane Ends Surgery
P81123 PWE Pendle Valley Mill/ Brierfield Practice
P81125 OAKENHURST MEDICAL PRACTICE (ico reg. DRS MOODIE, RANDALL, SMITH, GAVAN & BUTTERWORTH)
P81127 THE SURGERY CHORLEY
P81130 PADIHAM GROUP PRACTICE
P81132 WATERFOOT GROUP OF DOCTORS
P81136 Dr A K Bisarya & Partner
P81137 BURNLEY WOOD MEDICAL CENTRE
P81138 BURSCOUGH FAMILY PRACTICE



P81140 DARWEN HEALTHLINK
P81143 WHITTLE SURGERY
P81146 MYRTLE HOUSE MEDICAL PRACTICE
P81147 BLACKBURN ROAD MEDICAL PRACTICE
P81154 GRANVILLE HOUSE MEDICAL CENTRE ico reg. DRS D McALLISTER, J EDWARDS, A BRICKWOOD
P81155 Brownhill Surgery
P81159 STONYHILL MEDICAL PRACTICE (ico reg. DR ANDREW GARSTANG & PARTNERS)
P81160 OSWALD MEDICAL CENTRE
P81165 IGHTEHILL MEDICAL CENTRE
P81166 DR BELLO'S SURGERY
P81167 Stepping Stone Practice (ico reg. DRS Mridul K Datta, Harmeet Singh & Saroj Datta)
P81169 FISHERGATE HILL SURGERY
P81170 NELSON MEDICAL PRACTICE
P81171 EUXTON MEDICAL CENTRE
P81172 NEWTON DRIVE HEALTH CENTRE
P81179 LOSTOCK HALL MEDICAL CENTRE
P81180 CLAYTON BROOK SURGERY
P81181 KINGSFOLD MEDICAL CENTRE
P81182 RICHMOND MEDICAL CENTRE
P81184 RIBBLETON MEDICAL CENTRE
P81185 RIVERSIDE MEDICAL CENTRE
P81186 MOSS SIDE MEDICAL CENTRE ico reg. DR UDAY KANITKAR
P81196 ISSA MEDICAL CENTRE
P81197 ROSEGROVE SURGERY
P81201 ASHURST PRIMARY CARE
P81204 EWOOD MEDICAL CENTRE (Dr S Ray & Dr P Mashar)
P81208 Excel Primary Care
P81212 THE SURGERY
P81213 PENWORTHAM ST MARYS MEDICAL GROUP
P81214 LIMEFIELD SURGERY (ico reg. DRS GEBBIE, BURN & BROWN)



P81218 CLAYTON MEDICAL CENTRE
P81620 SLAIDBURN HEALTH CENTRE
P81622 SHIFA SURGERY
P81633 SPRINGFIELD/ FENISCOWLES HEALTH LINK SURGERY(ico reg. AJEET GUPTA)
P81646 LATHOM HOUSE SURGERY
P81647 Gutteridge Medical Centre
P81655 CROSTON VILLAGE SURGERY
P81664 THE PARK MEDICAL GROUP, PR2 1JR
P81674 Stanley Court Surgery
P81681 NORTH SHORE SURGERY
P81683 OLIVE MEDICAL PRACTICE
P81685 DR R ALI
P81686 Rossendale Valley Medical Practice
P81687 NEW LONGTON SURGERY
P81692 BEECHES MEDICAL CENTRE
P81694 THE FAMILY PRACTICE
P81695 AUGHTON SURGERY
P81699 HIGHER HEYES SURGERY
P81701 PRESTON ROAD SURGERY ico reg. DR GHADEER HAMAD
P81704 Blakewater Healthcare
P81707 WILLIAM HOPWOOD
P81709 ROMAN ROAD HEALTH CENTRE
P81710 TARLETON GROUP PRACTICE
P81711 DILL HALL SURGERY
P81713 THE SURGERY, DINMORE AVE, GRANGE PARK ESTATE (ico reg. DR GOSKEL CELIKKOL)
P81714 ABBEY DALE MEDICAL CENTRE
P81721 HOLLINS GROVE SURGERY (ico reg. PULLOORI JAGADESHAM)
P81724 PRINGLE STREET SURGERY
P81726 KING STREET MEDICAL CENTRE
P81727 County Road Surgery



P81730 GREAT HARWOOD MEDICAL GROUP
P81731 DR JEHANGIR'S SURGERY
P81732 HARAMBEE SURGERY
P81734- CORNERSTONE HEALTHCARE AND PRACTICES
P81735 Ribble Village Surgery (DR ASSAD HUSSAIN)
P81736 WHITEFIELD HEALTH CARE
P81738 RISHTON AND GREAT HARDWOOD
P81740 ADLINGTON MEDICAL CENTRE
P81741 STATION SURGERY ico reg: GEORGE WADIE AHAD
P81748 BRIARWOOD MEDICAL CENTRE
P81750 FRENCHWOOD SURGERY (ico reg. MARK WEBSTER)
P81755 THE WEAVERS PRACTICE
P81756 DANESHUSE MEDICAL CENTRE
P81757 BARROWFORD SURGERY
P81763 THE SURGERY (ico reg. HARA PROSAD CHAKRABARTI)
P81770 AVENHAM SURGERY (ICO DR ARIF DASU)
P81771 PRIMROSE BANK MEDICAL CENTRE
P81780 RIVERSIDE FAMILY PRACTICE
P81785 MEDICOM LIMITED Grtr Preston CCG
Parcliffe Medical Centre
POPLAR HOUSE SURGERY
QUEEN SQUARE MEDICAL PRACTICE
QUEENSWAY MEDICAL CENTRE
THE BAY MEDICAL GROUP
THE MOUNT VIEW PRACTICE
THE OLD LINKS SURGERY
The Over Wyre Medical Centre
The Thornton Practice
THE VILLAGE PRACTICE
Y00347 DR RAFFI BAGHJIAN (CHORLEY HEALTH CENTRE)



Y02466 BUCKSHAW VILLAGE SURGERY

Y02605 Accrington Victoria PWE

Y02606 FAIRMORE PWE

Y02657 CORNERSTONE COMMUNITY INTEREST COMPANY

Y03656 LEYLAND SURGERY

Appendix B - Sensitive codes/excluded list:



Read Description/Rubic	Read Code/Filter
HSA1-Therap. Abort. Green Form	956%
H/O: Venereal Disease	1415.%
Hysterotomy And Termination Of Pregnancy	7E066%
Dilation Of Cervix Uteri And Curettage Of Products Of Conception From Uterus	7E070%
Curettage Of Products Of Conception From Uterus NEC	7E071%
Suction Termination Of Pregnancy	7E084%
Dilation Of Cervix and Extraction Termination Of Pregnancy	7E085%
Termination Of Pregnancy NEC	7E086%
Cervical Smear - Wart Virus	4K36.%
Gonorrhoea carrier	65Q8.%
Venereal disease carrier NOS	65Q9.%
AIDS carrier	65QA.%
Notification of AIDS	65VE.%
Introduction of abortifacient into uterine cavity	7E0B%
Treatment for infertility	8C8%



Genital herpes simplex	A541%
Viral hepatitis B with coma	A702%
Viral (serum) hepatitis B	A703%
Viral hepatitis C with coma	A7040%
Viral hepatitis C without mention on hepatic coma	A7050%
Chronic viral hepatitis	A707%
Unspecified viral hepatitis	A70z%
Cytomegaloviral hepatitis	A7852%
Acquired immune deficiency syndrome	A788%
Human immunodef virus resulting in other disease	A789%
HIV disease resulting in cytomegaloviral disease	A7891%
Chlamydial infection	A78A.%
Chlamydial infection of lower genitourinary tract	A78A0%
Chlamydial infection of anus and rectum	A78A2%
Chlamydial infection of pelviperitoneum oth genitourinary organs	A78A3%
Chlamydial infection, unspecified	A78AW%



Chlamydial infection of genitourinary tract, unspecified	A78AX%
Human papilloma virus infection	A79B%
Papillomavirus as a cause of diseases classif to oth chapters	A7y05%
Syphilis and other venereal diseases	A9%
Trichomoniasis - trichomonas	AD1%
Phthirus pubis - public lice	AD22.%
HIV disease resulting/other infection + parasitic diseases	AyuC4%
Gender role disorder of adolescent or adult	E22y4%
Dementia in human immunodef virus (HIV) disease	Eu024%
[X]Gender identity disorders	Eu64%
[X]Gender identity disorder, unspecified	Eu64z%
Cystitis in gonorrhoea	K1545%
Prostatitis in gonorrhoea	K2144%
Prostatitis in trichomoniasis	K2146%
Chlamydial epididymitis	K2416%
Female chlamydial pelvis inflammatory disease	K40y1%



Chlamydia cervicitis	K4209%
Legally induced abortion	L05%
Illegally induced abortion	L06%
Unspecified abortion	L07%
Failed attempted abortion	L08%
Complications following abortion/ectopic/molar pregnancies	L09%
Failed attempted abortion	L0A%
Other specified pregnancy with abortive outcome	L0y%
Pregnancy with abortive outcome NOS	L0z%
Maternal syphilis in pregnancy/childbirth/puerperium	L170%
Maternal gonorrhoea during pregnancy/childbirth/puerperium	L171%
Other venereal diseases in pregnancy/childbirth/puerperium	L172%
Laboratory evidence of HIV	R109.%
Complications associated with artificial fertilization	SP0D%
Asymptomatic human immunodeficiency virus infection status	ZV01A%
Gonorrhoea carrier	ZV027%



Hepatitis B carrier	ZV02B%
Hepatitis C carrier	ZV02C%
[V] Pregnancy with history of infertility	ZV230%
[V] Admission for administration of abortifacient	ZV25B%
[V] In vitro fertilization	ZV267%



APPENDIX C: Data items stored for BI/stats on the LPRES VPC

