ISLINGTON

Data Protection Impact Assessment

A council-wide information document

Pinnacle Systems Management Ltd - PharmOutcomes for Locally Commissioned Services.

29/10/2021

PUPI-44363.0179

This template and additional guidance may be found on the DPIA SharePoint Page

1 PROJECT AND STAKEHOLDER INFORMATION

1.1 Project/Programme/Work outline

Project Name	Data administration system for Pharmacy Locally Commissioned Services (LCS)
The Purpose of the Project	Public Health currently commissions a number of individual services from pharmacists in Islington, called Locally Commissioned Services (LCS). The LCS include Emergency Hormonal Contraception (EHC), Needle Exchange (NEX) and Substance Misuse Supervised Administration (SSA). The project aims to replace the current data administration system ('Webstar') used by pharmacists who have signed up to one or all of the above LCSs, with a new system ('PharmOutcomes' provided by Pinnacle Systems Management Ltd). The preferred supplier is supported by the Local Pharmaceutical Committee. They are also contracted by NHSE for the provision of the hospital discharge service.
The desired outcomes of the project	To enable commissioned pharmacies to provide the LCS in an effective and appropriate manner, supported by a data administration system that is secure and fit for purpose. To enable the commissioners (Camden & Islington Public Health) to audit activity and administer/ process payments in a timely manner.
How is the processing of data necessary to the work?	This is a support contract which enables the above services to be carried out appropriately by providing a secure data management tool for the pharmacy providers. It also allows for non-personalised information to be collated for the purposes of audit and paying the providers for every intervention delivered. LCSs provided through pharmacists have been an important way of delivering public health services and ensuring delivery of proactive preventative health care. Pharmacists are among

	the most accessible services in the community, providing near universal population coverage, and the ability to target particular priority groups.
How much data will you be using and how often?	The pharmacy providers are contracted separately, so a DP Information Sharing Agreement for this contract is not needed (as the individual contracts with the pharmacies will cover DP) . We are happy to be advised otherwise for this.
Will the project collect new data or does it use existing data in a new way?	New data. The information on the pharmacy data administration system will include patient names and addresses, health information, etc. However, this will not be accessed by the Public Health department.
When is the processing expected to start? If the project is time limited, please note the expected end date	1st August 2021

1.1.1 Project/Programme/Work Description

You may use this box to provide a detailed description of the processing or to provide any additional information you feel is relevant.

Commissioned pharmacies will use the new data administration system ('PharmOutcomes'), under license. This system is widely used by pharmacists nationally, and has been commissioned by NHS England for the administration of hospital discharge, i.e. the electronic sharing of medicines information between hospital and community pharmacy.

However this will be a new system/contract for LBI.

The personal data will be processed by pharmacists as they deliver the LCS, from the LCS service users who opt to receive the service. Personal data will include vulnerable adults.

The data collection for the LCS by commissioned pharmacists is essential in order to deliver the services safely, appropriately and securely, and to retain an up-to-date service user record. Pharmacists will ask for consent to collect this information.

The Public Health department will access activity reports with no personal identifiable information, in order to manage the performance of and payments to LCS providers.

The contract will be between the Public Health Department and Pinnacle Systems Management Limited ("Pinnacle") as the provider. The council therefore, will be the data controller in this regard. The provider service will be the data processor.

1.2 Project Stakeholders

Role	Participant (name(s))			
Project manager/ Person responsible for delivery	Marina Chrysou			
Senior Responsible Officer for the Project	Johanna Tuomi Sharrock			
Information Asset Owner	*For guidance click here* Mahnaz Shaukat			
If the project requires the use of council datasets which belong to other directorates, please specify the directorate and the Information Asset Owner here.	N/A			
Does the NHS National Data Opt Out apply to any of the datasets?	*Is the project subject to Confidential Advisory Group (CAG) approval for purposes under Regulation 2 or 5 of the Control of Patient Information Regulations (2002), under s251 of the NHS Act 2006?* No – as this data is not shared with anyone else apart from the parties to this contract and the individual pharmacies (separate contract) who will use this system to deliver and record activity.			
Are there any joint data controllers in the project?	*For guidance click here* No, as the commissioner only receives anonymised data.			
Name(s) of Digital Services representatives	Abdikarim Gulaafe			
Is any of the project subject to a contract?	**Yes**	Yes	**No**	
If Yes, please state the contract number and contract term.	**Contract Number**		TBC	
	Contract Term		4 years	

2 SCREENING QUESTIONS

Screening Questions	Y/N
Is there a requirement under GDPR to carry out a DPIA? See the guidance here for further details. If you answer "Yes" to this question you do not need to answer the remainder of the screening questions and may proceed to Section 3 of this form.	Y
Does the project involve new or significantly changed processing of personal data about each individual?	Y
Will the project compel individuals to provide information about themselves?	Y
Will information about individuals be shared with organisations or people who have not previously had routine access to the information?	N
Will the project use information about individuals for a purpose it is not currently used for, or in a way it is not currently used?	N
Does the project involve you using new technology that might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition.	N
Will the project result in you making decisions or treating individuals in ways which can have a significant impact on them?	N
Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union information, biometric data, sex life or sexual orientation or other information that people would consider to be private?	N
Will the project require contact with individuals in ways they may find intrusive, for example, unexpected telephone calls?	N
Does the project involve new or significantly changed consolidation, inter-linking, cross referencing or matching of personal data/special category data from multiple sources?	N
Comments	
You may use this space to provide any supplementary comments regarding the answers you have given above. JL – Data processing is not novel. Existing pharmacy system is already in place. This DPIA reflects the move to a new provider. Pharmoutcomes IG and security documentation attached.  PharmOutcomesTechnicalAndIGSpecificatic	

If **all** questions are **"NO",** please return this document to the Information Governance Team at dp@islington.gov.uk and **do not** complete the remainder of this Data Protection Impact Assessment.

If **any** of the screening questions have been answered **"YES**", then please continue with the remainder

of the Data Protection Impact Assessment.

3 DATA PROTECTION IMPACT ASSESSMENT

3.1 Dataflow Map

Data Mapping Assessment	Y/N
Has a Records of Processing Activity (ROPA) exercise been carried out? *If "Yes" please provide a copy of the ROPA log entries when you submit this assessment.If "No" please ensure this is completed before processing starts. Speak to your local Information Lead for guidance.* ***Please note that DPIAs will NOT be approved without at least an initial draft of ROPA being completed prior to submission.***	N/A

3.2 Transfers of Data

Is personal data transferred in an identifiable form? *If yes,please use this space to describe how the information moves either internally, between departments or externally if other organisaitons are involved.* *Where is the data stored at the start of its journey and will it be moved to different locations?Who will have access to the data at different stages?* *Who are the recipients of the data? Consider internal and external recipients, including teams outside of your immediate team.*	Not with regards to the council. Pharmacies enter records directly into PharmOutcomes.
Please describe all the media used for the transfer of data. NB This could be in a number of formats: courier, post, email, FTP.	N/A as Commissioners will have access to the system to download anonymised data.

3.3 Controllers and Processors

	Y/N
Are multiple organisations involved in the processing of the data? *For guidance click here* *If you have answered "Yes" please fill out the table below. If you have answered "No" please move on to the next question.*	Yes – the provider and pharmacies on a separate contract.

Name of organisation	Controller or Processor?
LBI	Controller
Pinnacle Systems Management Ltd	Processor
Pharmacies	Controllers

3.4 Describe the specific classes of data to be collected or processed

Personal data is any information which identifies a living person. Add "Y" to each field where applicable, otherwise leave blank.

Personal Data	**Y**	**Comments**
Name	Y	EHC and SSA only
Address data / postcode	Y	Postcode only
Email Address	N	
Date of Birth	Y	
Government issued ID – passport, driving licence	N	
Payroll Number	N	
HR / Employment data	N	
NHS Number	N	
Housing Data	N	
Online identifiers, including IP address and cookies	N	
Location data, GPS etc.	N	
Special Category Data / Elevated Risk	**Y**	**Comments**
Ethnicity	Y	EHC and SSA only
Political Opinion / Affiliation	N	
Religious Beliefs	N	
Trade Union Membership	N	
Physical or Mental Health	N	
Sexuality / Sexual Life	Y	EHC only
Criminal Offences	N	
Biometrics: Fingerprints, Retina, DNA profile	N	
Bank, credit card or financial details	N	
National Insurance Number	N	
Pension, Benefit or Tax Data	N	
Health and/ or Social Services Records	Y	The data entered into Pharmoutcomes by the pharmacies can form part of a clinical record for a healthcare provider.
Children's data, child protection, school records, adoption	N	

Please specify any other types of data not listed in the previous table.	Gender EHC only: current medication or over-the-counter medicines/ remedies; specific medical condition history. NEX only: Name is NOT collected; in treatment for drug use; Hepatitis B vaccination status.

3.5 Data Source(s)

If the data has not come from the data subject, where does the personal data come from?

Source	Comments
Previously collected by department carrying out the change	N/A
Previously collected by another Islington Council department	N/A
Previously provided by a partner agency (eg, NHS, Police, Department of Work and Pensions)	N/A
Does ths project affect only data which will be collected once the change is made	Yes

3.5.1 Data Source Description

You may use this box to provide a detailed description of the data sources for complex projects or projects using linked data sources.

The data source is the via the contracted (separately for the LCS's services) pharmacies who may enter records on to the system.

3.6 Who will access the data?

Categories of users	How users access the system and their intended use of the system
Council staff	The system is configured so that licence holders have different levels of access to data held within the system. The system redacts patient identifiable data and provider information at different levels to ensure that confidentiality is maintained. Camden and Islington Public Health will be able to see information about the pharmacies and anonymised patient data but not patient identifiable info.
Third party staff	Only Pharmacies who are subject to separate contracts to deliver the activity of the LCS services using the system for which this DPIA is on. Pharmacies will have access to Patient Identifiable Info for data for which they are the

	controller
Members of the public	No.

3.7 The Data Protection Principles

Principle	Comments and risks
Are you processing data as a statutory duty and if so, under what legislation?	*You should be able to identify the obligation in question, either by reference to the specific legal provision or else by pointing to an appropriate source of guidance that sets it out clearly: for example, "Duty to levy and collect Council Tax under Section 1 of the Local Government and Finance Act (1992)"* The Health and Social Care Act 2012 created a framework for Health and Welbeing Boards and the responsibility for LAs to commission the majority of public health services since 2013
Data is processed lawfully, fairly and in a transparent manner in relation to the data subject. Examples include: • Consent of data subject, • Contract with data subject, • Council under legal obligation, • Necessary to protect the vital interests of data subject, • 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	*You will need to identify the legal basis using the GDPR article 6 (for personal data) and/or article 9 (for special category data) as referenced in Chapter 2, section 8 and 10 of the Data Protection Act 2018.* *Consent is not always necessary – however, where this is intended to be obtained, please provide a copy of the consent statement and a description of where consent is stored,* *(ICO Guidance on Lawful Basis for Processing)* ***Article 6 condition*** (e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law under Health and Social Care Act 2012 **Article 9 condition** (h) Health or social care (with a basis in law) Data Protection Act Schedule 1 Part 1, 2 (2)(f) - the management of health care systems or services or social care systems or services. Both the council and pharmacies will be relying on this condition.
The data is collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes	*How will you ensure that personal data is only processed for its original intended purpose and not processed for additional purposes? How will function creep be prevented?* Public Health will not use personal identifiable data. Public Health will use aggregate data to monitor and manage performance of pharmacists under the LCS contract. This will ensure a high quality service for residents.
Data is adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')	*You should collect only the minimum data required for the intended processing activity. On the other hand, the amount of data needs to be sufficient to ensure that it can support effective decision making.* The modules are designed to ensure that data asked for or used are the minimum necessary for the safe provision of the services. Some data on protected characteristics, e.g. ethnicity, are collected to monitor the equitable provision of services in different groups. No additional data is asked for or used.

Retention. The data must be held for no longer than required for this purpose. How long should this data be held? How will it be securely disposed or/permanently deleted?	*Where there are concerns about the appropriate retention of data, this section will be reviewed by the Information Governance Team.* *Islington Retention Schedule* **Retention from the Pharmacies' perspective** The records entered onto PharmOutcomes by providers (pharmacies) remain their data because it can form part of a clinical record for a healthcare professional/provider. This information is held by PharmOutcomes for as long as necessary under the current NHS guidelines Records Management Code of Practice for Health and Social Care 2016 Appendix 3 indicate minimum retention periods and required final actions). Providers (pharmacies) are able to download and print a copy of their records in order to retain them for the appropriate period of time. After that period providers will be contacted regarding the redaction, archiving or deletion of the information depending on existing NHS guidelines at that time. Pinnacle will not remove data from the system without written instructions from the relevant data controller Records should not ordinarily be kept for longer than 30 years. The Public Records Act does, however, provide for records which are still in current use to be legally retained. Additionally, under separate legislation, records may be required to be retained for longer than 30 years (e.g. Control of Substances Hazardous to Health Regulations). The minimum retention periods should be calculated from the beginning of the year after the last date on the record. For example, a file in which the first entry is in February 2011 and the last in September 2014, and for which the retention period is seven years, should be kept in its entirety at least until the beginning of 2022. Each organisation should produce its own retention schedules in the light of its own internal requirements **From Commissioners' perspective** Public Health will only have access to anonymised data for monitoring purposes. 6 years after contract ends. The provider has procedures in place for the secure destruction of data when this is required.
Are there measures in place to deal with data subjects' rights?	*Where LBI controls the data, data subjects' rights will be managed using existing Islington processes. However, where data is processed by a third party please detail the measures which are in place. If new technology is being introduced, consider how the technology helps us meet our obligations.*

Data subjects have the right to ask for a copy of their data – this must be provided within 30 days. Data subjects have the right to have incorrect data corrected Data subjects may ask the council to 'cease processing.' This could involve deleted data there is no legal reason to hold, or to desist from contacting them.	*(ICO Guidance on Data Subject Rights)* Subject access requests will be made and dealt with by individual pharmacies as the data controllers, and if they require assistance with accessing the data they need, the provider will support with the process.
Data must not be transferred outside the EEA without appropriate provisions. Please confirm where the data will be stored, sent and where it will be accessed from. If a third party hosts or accesses the data you will need to confirm the location of the data in a written contract.	*EEA (European Economic Area) consists of EU member states and three European Free Trade Association (EFTA) states (Iceland, Liechtenstein, and Norway). Due to Britain leaving the EU, our current requirement is that Servers should be UK based.* Data is hosted within the UK by their hosting partner Memset Ltd, Building 87, Dunsfold Park, Stovolds Hill, Cranleigh, GU6 8TB. https://www.memset.com/about/security-compliance/accreditations/ Their two data centres are situated in Dunsfold and Reading. Dual site resilience with both data centres data centres connected by a dedicated fibre line separate from the main internet

3.8 Risk Management

3.8.1 Identify and assess risks

All contributors to the DPIA should consider risks associated with the project and record any identified risks here:

Please attach a completed version of the DPIA Risk Register when you submit this form.



DPIA_Pinnacle Systems Pharmacy Ri

3.9 Privacy Impact assessment: COMMENTARY

This section is to be completed by the Information Governance team

3.9.1 DP Lead Comments

See IG Panel Comments

3.9.2 IG Panel Comments

This DPIA was reviewed at IG Panel on 29th October 2021 where it was provisionally approved with the following caveats:

- The DPIA needs to be countersigned by IDS to provide assurance that they have completed their cyber-security assessment of the PharmOutcomes product and are satisfied that it meets their requirements.
- Contracts between Public Health, Pinnacle and the Pharmacies should be signed at the earliest opportunity and must be in place and finalised before any personal data is entered into the system.

Proposed Review Date:	01/04/2022

4 RISK ASSESSMENT: AUTHORISATION

Use this section to authorise projects where the data is under the control of the directorate initiating the project. In cases where the project requires the use of data from other directorates, please use section 5 instead.

4.1 Service Area IGWG representative (guidance)

Name	Jasmin Suraya
Job Title	Commissioning , Gov & Contracts Officer
Telephone	+442075278344
Signature	
Date	

4.2 Islington Digital Services authorisation (where applicable)

Name	Abdikarim Gulaafe
Job Title	Solutions Architect
Telephone	+442075275981
Signature	Approved by Duncan Harris via email on 2nd November 2021.  20211102 Duncan Harris CyberSec Appr
Date	2/11/2021
IDS Risk Assessment	*Please attach a copy of the Risk Assessment if one was carried out on this project.*

4.3 Information Asset Owner

Name	Mahnaz Shaukat
Job Title	Head of Public Health Intelligence
Telephone	
Comments	*Where risks have been identified with the use of your data, please explicitly state that you understand the risks and your desired approach for mitigating those risks. If you wish to accept the*

	risks without mitigation, or if you do not accept the risks, please state this here and explain your reasons.
Authorisation to proceed	*Please tick the appropriate box* Proceed with proposed use of data ☐ Reject proposed use of data ☐
Signature	Approval granted by email on 25th November 2021 20211125 Mahnaz Shaukat IAO approval
Date	25th November 2021

On behalf of my service area, I agree with this risk assessment and accept the risks as described in this document. I confirm that I have read the "Islington ICT Security Policy Framework'" and assert that nothing in this risk assessment is in conflict with this overarching framework.

I am aware that the council needs to adhere to the Data Protection Act (2018) and in particular Section 56 that all organisations commit to: "Each controller must implement appropriate technical and organisational measures to ensure, and to be able to demonstrate, that the processing of personal data complies with the requirements of this Part."

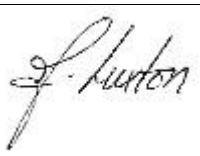
I am also aware that we must comply with the terms of the General Data Protection Regulations and any revised UK Data Protection legislation.

I confirm that while accepting the risks stated in this risk assessment, that I have not breached any of the above legislative requirements.

Sending this to the Information Governance Team
One authorised by IGWG representative and Service Director, this DPIA should be sent to your Corporate Data Protection Lead for final sign-off. If you have access to a Xerox MFD please use the scan-to-email function to send your completed forms to dp@islington.gov.uk

4.4 Corporate Data Protection Lead

Name	Joe Luxton
Job Title	Data Protection Lead
Telephone	020 7527 8002

Signature	
Date	25/11/2021

5 APPENDIX 1: GUIDANCE NOTES

5.1 Legal requirement to conduct a DPIA

Conducting a DPIA is a legal requirement of the GDPR in certain circumstances where there is a high risk to privacy. A DPIA will be mandatory where the council plans to:

- Use systematic and extensive profiling or automated decision-making to make significant decisions about people.
- Process special category data or criminal offence data on a large scale*.
- Systematically monitor a publicly accessible place on a large scale*.
- Use new technologies.
- Use profiling, automated decision-making or special category data to help make decisions on someone's access to a service, opportunity or benefit.
- Carry out profiling on a large scale*.
- Process biometric or genetic data.
- Combine, compare or match data from multiple sources.
- Process personal data without providing a privacy notice directly to the individual.
- Process personal data in a way which involves tracking individuals' online or offline location or behaviour.
- Process children's personal data for profiling or automated decision making or for marketing purposes or offer online services directly to them.
- Process personal data which could result in a risk of physical harm in the event of a security breach

*Large Scale - the GDPR does not contain a definition of large-scale processing, but to decide whether processing is on a large scale you should consider:

- the number of individuals concerned;
- the volume of data;
- the variety of data;
- the duration of the processing; and
- the geographical extent of the processing.

Examples of large-scale processing include:

- a hospital (but not an individual doctor) processing patient data;
- tracking individuals using a city's public transport system;
- a fast food chain tracking real-time location of its customers;

- an insurance company or bank processing customer data;
- a search engine processing data for behavioural advertising; or
- a telephone or internet service provider processing user data.
- Individual professionals processing patient or client data are not processing on a large scale.

Examples of where a DPIA would be appropriate

- A new IT system for storing and accessing personal data
- A data sharing initiative where two or more organisations seek to pool or link sets of personal data.
- A proposal to identify people in a particular group or demographic and initiate a course of action.
- Using existing data for a new and unexpected or more intrusive purpose.
- A new database which consolidates information held by separate parts of an organisation.
- Legislation, policy or strategies which will impact on privacy through the collection or use of information, or through surveillance or other monitoring.
- Cloud hosted applications
- The collection of new data on an existing system

Back to Screening Questions

5.2 Controllers and Processors

When answering this question, please consider that suppliers, software providers etc will count as other organisations as well as partner agenices.

'Controller' means alone or jointly with others, the name of the organisation that determines the purposes and means of the processing of personal data

'Processor' means the organisation that is processing personal data under the instruction of a Controller and does not determine the purposes and means of the processing

'Joint Controller' means two or more Controllers who decide the purposes and means of processing together – they have the same or shared purposes. Controllers will not be Joint Controllers if they are processing the same data for different purposes. (Article 26 (1), GDPR).

6 APPENDIX 2: LINKED DATA DPIA PROCESS

