DATA PROTECTION IMPACT ASSESSMENT - Public Health sexual health services v1.0

Reference number: DPIA-317

Author: Jeremy Lyn-Cook
Email: jeremy.lyncook@nottinghamcity.gov.uk

DATA PROTECTION IMPACT ASSESSMENT

When to complete this template:

Start to fill out the template at the beginning of any major project involving the use of personal data, or, where you are making a significant change to an existing process that affects personal data. Please ensure you update your project plan with the outcomes of the DPIA.

Table of Contents

1. Document Control

1. Control Details

Author of DPIA:	
Owner of project:	Uzmah Bhatti
Contact details of Author:	Uzmah.bhatti@nottinghamcity.gov.uk

2. Document Amendment Record

Issue	Amendment Detail	Author	Date	Approved
V1.0	Initial draft	Jeremy Lyn-Cook		

3. Contributors/Reviewers

Name	Position	Date
Jeremy Lyn-Cook	Information Policy Specialist	27/11/2021

4. Glossary of Terms

Term	Description
NCC	Nottingham City Council

Author: Jeremy Lyn-Cook
Email: jeremy.lyncook@nottinghamcity.gov.uk

2. Screening Questions

1. Does the project involve personal data? **Yes/No**	**If 'Yes', answer the questions below. If 'No', you do not need to complete a DPIA but make sure you record the decision in the project documentation.**
2. Does the processing involve any of the following data: medical data, ethnicity, criminal data, biometric data, genetic data and any other special/ sensitive data?	**Yes/No**
2. Does the processing involve any systematic or extensive profiling?	**Yes/No**
3. Does the project involve processing children's data or other vulnerable citizen's data?	**Yes/No**
4. Does the processing involve decisions about an individual's access to a product, service, opportunity or benefit that is based on any evaluation, scoring, or automated decision-making process?	**Yes/No**
5. Does the processing involve the use of innovative or new technology or the novel application of existing technologies?	**Yes/No**
6. Does this project involve processing personal data that could result in a risk of physical harm in the event of a security breach?	**Yes/No**
7. Does the processing combine, compare or match data from multiple sources?	**Yes/No**
8. Does the project involve processing personal data without providing a privacy notice?	**Yes/No**
9. Does this project process data in a way that tracks on line or off line location or behaviour?	**Yes/No**
10. Will the project involve using data in a way it has not been used before?	**Yes/No**
11. Does the project involve processing personal data on a larger scale?	**Yes/No**
12. Will the project involve processing data that might prevent the Data Subject from exercising a right or using a service or entering into a contract?	**Yes/No**
If you answered 'Yes' to any <u>two</u> of the questions above, proceed to Question 3 below. If not seek advice from the DPO as you may not need to carry out a DPIA.	

Project Title: Locally Commissioned Public Health Services (LCPHS) Sexual Health

Team: Public Health

Directorate: People

DPIA Reference number: *(This will be allocated by the Information Compliance Team or the DPO and must be quoted in all correspondence)*

Has Consultation been carried out? No consultation required – this is an approval to continue to commission an existing service.

1. DDM attached?	**Yes/No** Commissioning and Procurement Exec Committee draft paper attached
2. Written evidence of consultation carried out attached?	**Yes/No**
3. Project specification/ summary attached?	**Yes/No** See Commissioning and Procurement Exec Committee draft paper attached – link to specs are here https://www.nottinghamcity.gov.uk/information-for-business/business-information-and-support/procurement/pharmacy-lcphs-accreditation/ https://www.nottinghamcity.gov.uk/information-for-business/business-information-and-support/procurement/gp-lcphs-accreditation/
4. Any existing or previous contract / SLA / processing agreement attached?	**Yes/No** See links above
5. Any relevant tendering documents attached?	**Yes/No** See links above
6. Any other relevant documentation attached?	**Yes/No**

3. Project - impact on individual's privacy

Issue	Questions	Examples	Yes/No	Initial comments on issue & privacy impacts
Purpose and means		Profiling, data analytics, Marketing. Note: The GDPR requires a DPIA to be carried out where there is systematic and extensive evaluation of personal aspects relating to individuals based on automated processing, including profiling, and on which decisions about individuals are based.		
	Please give a summary of what your project is about (*you can also attach or embed documents for example a project proposal*).			Under the provisions of the Health and Social Care Act (2012) Nottingham City Council (NCC) has a statutory responsibility to provide, or secure the provision of, open access sexual health services in its area including: i) preventing the spread of sexually transmitted infections (STIs) ii) treating, testing and caring for people with STIs and their partners iii) contraceptive services including advice on preventing unintended pregnancy and sexual health promotion. The current contracts are due to expire in March 2022 with no option to extend. These contracts are usually awarded to GPs and community pharmacy providers based on an accreditation type procurement process.
	Aims of project Explain broadly what the project aims to achieve and what types of processing it involves.			Due to the administration based complexities in establishing these multiple contracts with individual GP practices and pharmacy providers it is deemed to be more efficient and better for continuity in services for citizens to adopt a cycle of 9-year flexible contracts (3+3+3) where NCC would retain a contract severance clause. The current contract allows for new providers to apply through an open accreditation process and it is anticipated that this arrangement is replicated in the new contract in order to ensure that this reflects the changing ownership and staffing seen within community pharmacies.
	Describe the nature of the processing How will you collect store and delete data? Will you be sharing with anyone? You might find it useful to refer to a flow diagram or			GP practices and pharmacy providers are separate data controllers. NCC has no involvement in operational delivery of the sexual health services. As a result, it has no interaction with citizens using the services and collects no information from them directly. However, the system for paying the providers means that they have to submit invoices and these are likely to include a limited amount of personal demographic data.

	another way of describing data flows. What types of processing identified as likely high risk are involved? Who will have access to the project personal data, how is access controlled and monitored and reliability of staff assessed? Will data be separated from other data within the system?		Pharmacies use a secure database (Pharmoutcomes) to invoice NCC including personal demographic data. GPs, send their payment information on email to the 'Contracts' inbox. It includes demographic data but no medical data.	
	Privacy Implications Can you think of any privacy implications in relation to this project? How will you ensure that use of personal data in the project is limited to these (or "compatible") purposes?			• GPs transfer invoice information (including personal data) to NCC insecurely. • NCC stores personal information from providers insecurely.
	New Purpose Does your project involve a new purpose for which personal data are used?		No.	
	Consultation Consider how to consult with relevant stakeholders: Describe when and how you will seek individuals views- or justify why it's not appropriate to do so. Who else do you need to involve in NCC? Do you plan to consult Information security experts, or any other experts?			It is not necessary to consult externally as the project involves back office processes (tendering for a contract) that should not have any impact on the way that providers deliver sexual health services to citizens. There will be no changes in the way that NCC and sexual health service providers process personal information.

Individuals (data subjects)	Will the project:	Expanding customer base; Technology which must be used by individuals; Hidden or complex uses of data; Children's data		
	Affect an increased number, or a new group, or demographic of individuals (to existing activities)?		No.	
	Involve a change to the way in which individuals may be contacted, or are given access to services or data? Are there any areas of public concern that you should factor in?		No.	
	Affect particularly vulnerable individuals, including children?		Possibly.	Payment information covers a wide range of different individuals who have accessed the sexual health services.
	Give rise to a risk that individuals may not know or understand how their data are being used?		No.	
Parties	Does the project involve:	Outsources service providers; Business partners; Joint ventures		
	The disclosure of personal data to new parties?		No.	
	The involvement of sharing of personal data between multiple parties?		No.	
Data categories	Does the project involve:	Special personal data; Biometrics or genetic data; Criminal offences; Financial data; Health or social data; Data analytics: Note: the GDPR requires a DPIA to be carried out where there is processing on a large scale of special categories of data or of data relating to criminal convictions and offences		
	The collection, creation or use of new types of data?		No.	

	Use of any special or privacy-intrusive data involved? • Political opinions • Religious beliefs or philosophical beliefs • Trade union membership • Genetic data • Biometric data • Sexual life • Prosecutions • Medical data • Criminal data (Criminal data processing, i.e. criminal convictions, etc. also has special safeguards under Article 10).		Yes.	GP practices and pharmacy providers submit payment for services they have provided to individuals. The invoices may include a limited amount of demographic data. Whilst this is not explicitly 'medical' data, all the information relates to sexual health and consequently, 'medical' information may be inferred from it.
	New identifiers, or consolidation or matching of data from multiple sources? (For example a unique reference number allocated by a new management system)		No.	
Technology	New solutions:	Locator or surveillance technologies; Facial recognition; Note: the GDPR requires a DPIA to be carried out in particular where new technologies are involved (and if a high risk is likely)		
	Does the project involve new technology that may be privacy-intrusive?		No.	

Data quality, scale and storage	Data:	New data		
	Does the project involve changes to data quality, format, security or retention? What are the benefits of the processing? i.e. will the new system have automatic retention features? Will the system keep the information in a safer format etc.?		No.	
	Does the project involve processing data on an unusually large scale?		No.	
Monitoring, personal intrusion	Monitoring:	Surveillance; GPS tracking; Bodily testing; Searching; Note: the GDPR requires a DPIA to be carried out where the project involves systematic monitoring of a publicly accessible area on a large scale		
	Does the project involve monitoring or tracking of individuals or activities in which individuals are involved?		No.	
	Does the project involve any intrusion of the person?		No.	
Data transfers	Transfers	Transfers outside the EEA		
	Does the project involve the transfer of data to or activities within a country that has inadequate or significantly different data protection and privacy laws?		No.	

4. Legal Framework and Governance – Compliance

Ref.	Question	Response	**Further action required** (and ref. to risk register as appropriate)
1. Applicable laws and regulation			
1.1	Which data protection laws, or laws which impact data protection and privacy, will be applicable to the project?	• UK General Data Protection Regulation • Data Protection Act 2018 • Human Rights Act 1998	
1.2	Are there any sector-specific or other regulatory requirements or codes of practice, which should be followed?	Health and Social Care Act (2012)	
2. Organisation's policies			
2.1	Is the project in compliance with the organisation`s information management policies and procedures (including data protection, information security, electronic communications)?	Yes.	

2.2	Which policy requirements will need to be followed throughout design and implementation of the project?	Data Protection Policy Information Security Policy Records Management Policy	
2.3	Are any changes/updates required to the organisation`s policies and procedures to take into account the project? **Note: new requirements for *"Accountability"* under the GDPR, including record-keeping, DPOs and policies**	No.	
3. Training and roles			
3.1	Will any additional training be needed for staff in relation to privacy and data protection matters arising from the project?	No.	

5. Personal Data Processing Compliance

Ref.	Question	Response	Further action required (and ref. to risk register as appropriate)
1.	**Personal Data Processing**		
1.1	Which aspects of the project will involve the processing of personal data relating to living individuals?	GP practices and pharmacy providers submit payment for services they provide to individuals. The invoices may include a limited amount of demographic data which NCC processes when making the due payment.	
1.2	Who is/are the data controller(s) in relation to such processing activities?	Nottingham City Council GPs and pharmacies service providers	
1.3	Who is/are the data processor in relations to such processing activities?	N/a.	
2.	**Fair and Lawful processing - GDPR Articles 5(1)(a), 6, 9, 12, 13**		
2.1	Which fair processing conditions are you relying on? GDPR: Article 6(1) (legal basis for processing) and, for sensitive personal data, Article 9(2).	6(1). **Choose at least one of the following for personal data**, **usually (e)**-(Cross out the rest) ~~a) Consent~~ ~~b) Performance of contract~~ ~~c) Legal obligation~~ ~~d) Vital interests~~ **e) Public interest / exercise of Authority** 9(2) Choose at least 1 for special data- usually g (cross the rest out) a) ~~Explicit consent~~ ~~b) Employment / social security / social protection obligations~~ ~~c) Vital interests~~ ~~d) Non-profit bodies~~ ~~e) Processing made public by data~~	GPs and pharmacies are data controllers separate from NCC. They have their own legal basis upon which to provide personal information to NCC.

		~~subject~~ ~~f) Legal claims~~ **g) Substantial public interest** ~~h) Health, social care, medicine~~ ~~i) Public interest for public health~~ ~~j) Archiving, statistics, historical research~~ **~~For any criminal Data~~** ~~Comply with Article 10 **if it meets a condition in Part 1, 2 or 3 of Schedule 1.**~~ • ~~Employment, social security and social protection~~ • ~~Health and social care purposes~~ • ~~Public health~~ • ~~Research~~ ~~Substantial public interest:~~ • ~~Statutory and government purposes~~ • ~~Equality of opportunity and treatment~~ • ~~Racial and ethnic diversity at senior levels of organisations~~ • ~~Preventing or detecting Unlawful Acts~~ • ~~Protecting the public against dishonesty etc~~ • ~~Regulatory requirements relating to unlawful acts and dishonesty etc~~ • ~~Journalism etc in connection with unlawful acts and dishonesty etc~~ • ~~Preventing fraud~~ • ~~Suspicion of terrorist financing or money laundering~~ • ~~Counselling~~ • ~~Safeguarding of children and of individuals at risk~~ • ~~Safeguarding of economic well-being of certain individuals~~ • ~~Insurance~~	

		~~• Occupational pensions~~ ~~• Political parties processing~~ ~~• Disclosure to elected representatives~~ ~~• Informing elected representatives about prisoners~~ ~~Additional Conditions~~ ~~• Consent~~ ~~• Vital interests~~ ~~• Personal data in the public domain~~ ~~• Legal claims~~ • ~~Judicial Acts~~	
Note: different conditions may be relied upon for different elements of the project and different processing activities. Also, the scope of special category data is wider under the GDPR, and in particular includes genetics & biometric data, and sexual orientation.			
2.2	How will any consents be evidenced and how will requests to withdraw consent be managed?	NCC is not using consent as the legal basis for processing personal information.	
Note: new requirements for obtaining and managing consents within the GDPR.			
2.3	Is the data processing under the project covered by fair processing information already provided to individuals or is a new communication needed (see also data subject rights below)?	Attach privacy notice or provide a working link to the relevant privacy notice	
Note: more extensive information required under the GDPR than under current law, and new requirements on how such information is provided. Also a general principle of "*transparency*". It is important to assess necessity and Proportionality			
2.4	If data is collected from a third party, are any data protection arrangements made with such third party?	Personal data is collected from GPs and pharmacies along with payment information under a contract for providing sexual health services from GPs and pharmacies.	 Locally Commissioned Public
2.5	Is there a risk of anyone being misled or deceived?	No.	
2.6	Is the processing "fair" and proportionate	Yes.	

	to the need's and aims of the projects?		
2.7	Are these purposes clear in privacy notices to individuals? (see above)	Not sure.	
3. Adequate, relevant and not excessive, data minimisation - GDPR Article 5(1)(c)			
3.1	Is each category relevant and necessary for the project? Is there any data you could not use and still achieve the same goals?	Yes.	
Note: GDPR requires data to be "limited to what is necessary" for the purposes (as well as adequate and relevant).			
3.2	Is/can data be anonymised (or pseudonymised) for the project?	Possibly.	
4. Accurate and up to date - GDPR Article 5(1)(d)			
4.1	What steps will be taken to ensure accurate data is recorded and used?	The personal information comes to the GP or pharmacy directly from the patient and checked with them during the consultation.	
For example: checks when receiving/sending information from/to third parties, or transcribing information from oral conversations or handwritten documents, any automatic checks on information not meeting certain criteria.			
4.2	Will regular checks be made to ensure project data is up to date?	See above.	
5. Data retention - GDPR Article 5(1)(e)			
5.1	How long will personal data included within the project be retained?	Any personal information submitted will be held together with the payment information for 6 years. It will be password protected and only accessible via a secure login (by individuals directly involved with the payment work).	
5.2	How will redundant data be identified and deleted in practice? Consider paper records, electronic records, equipment?	All data is electronic and can be sorted by date to be disposed of when redundant.	

5.3	Can redundant data be easily separated from data which still need to be retained?	Yes, it is electronically stored and can be sorted by date.	
6. Data subject rights - GDPR Articles 12 to 22			
6.1	Who are the relevant data subjects?	Service users of sexual health services provided by GPs and pharmacies.	
6.2	Will data within the project be within the scope of the organisation`s subject access request procedure?	Yes.	
6.3	Are there any limitations on access by data subjects?	No.	
6.4	Is any data processing under the project likely to cause damage or distress to data subjects? How are notifications from individuals in relation to damage and distress managed?	No. If any notification is received they will be processed by the service area concerned in liaison with NCC's Information Compliance Team.	
6.5	Does the project involve any direct marketing to individuals? How are requests from data subjects not to receive direct marketing managed?	No.	
6.6	Does the project involve any automated decision making? How are notifications from data subjects in relation to such decisions managed?	No.	
6.7	How will other rights of data subjects be addressed? How will security breaches be managed?	These rights will be processed by the Information Compliance Team at Nottingham City Council. All breaches will be dealt with by the Information Compliance Team and the Data Protection Officer.	
7. Data Security - GDPR Articles 5(1)(f), 32			
For example: • **Technology**: encryption, anti-virus, network controls, backups, DR, intrusion detection;			

• **Physical**: building security, clear desks, lock-leads, locked cabinets, confidential waste; **Organisational**: protocols on use of technology, asset registers, training for staff, pseudonymisation, regular testing of security measures.			
Describe the source of risk and nature of potential impact on the individuals. Include associated compliance and corporate risks as necessary -What security measures and controls will be incorporated into or applied to the project to protect personal data? Consider those that apply throughout the organisation and those which will be specific to the project. N.B Measures that are appropriate to the nature of the data and the harm which may result from a security breach	**Likelihood of harm** Remote, Possible or Probable	**Severity of harm** Minimal, Significant or Severe	**Overall Risk** Low, Medium or High
• GPs transfer invoice information (including personal data) to NCC insecurely.	Possible.	Significant.	Medium.
• NCC stores personal information from providers insecurely.	Possible.	Significant.	Medium.

Identify measures to Reduce Risk- Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk that you have identified				
Risk	Options to reduce or eliminate risk	**Effect on risk** Eliminated/ Reduced or Accepted	**Residual risk** Low/Medium/High	**Measures approved** Yes/No
GPs transfer invoice information (including personal data) to NCC insecurely.	Information form GPs is received by NCC in a secure, password protected inbox.	Accepted.	Medium.	
NCC stores personal information from providers insecurely.	NCC will apply all current (and future) technical controls deployed across the NCC network in order to protect the information.	Reduced.	Low.	

8. Data processors - GDPR Article 28 & direct obligations in other articles				
8.1	Are any data processors involved in the project?	No.		
8.2	What security guarantees do you have?	N\a.		
For example: specific security standards or measures, reputation and reviews				
8.3	Please attach the processing agreement	N\a.		
For example: security terms, requirements to act on your instructions, regular audits or other ongoing guarantees Note: new requirements for the terms of contracts under the GDPR (much more detailed than current law).				
8.4	How will the contract and actions of the data processor be monitored and enforced?	N\a.		
8.5	How will direct obligations of data processors be managed?	N\a.		
Note: New direct obligations for processors under the GDPR, including security, data protection officer, record-keeping, international data transfers.				
For example: fair & lawful, lawful purpose, data subject aware, security, relevance.				
9. International data transfers - GDPR Articles 44 to 50				
9.1	Does the project involve any transfers of personal data outside the European Union or European Economic Area?	No.		
9.2	What steps are taken to overcome the restrictions?	N\a.		
For example: Safe Country, contractual measures, binding corporate rules, internal assessments of adequacy Note: GDPR has similar methods to overcome restrictions as under current law, but there are differences to the detail and less scope for an "own assessment" of adequacy.				
10. Exemptions				
10.1	Will any exemptions for specific types of processing and/or specific DP requirements be relied upon for the project?	N\a.		
For example: crime prevention, national security, regulatory purposes				

Note: Exemptions under the GDPR to be assessed separately, and may be defined within additional EU or UK laws.

6. Sign off and record outcomes

Item	**Name**	**Date**
Measures approved by: (project owner) This must be signed before the DP can sign off on the DPIA.		
Residual risks approved by: (If accepting any residual high risk, consult the ICO before going ahead)		
DPO advice provided: (DPO should advise on compliance, measures and whether processing can proceed)		
Summary of DPO advice:		
DPO advice accepted or overruled by		If overruled, you must explain your reasons
Comments:		
IT Security Officer: Where there are IT security issues		
IT Officer comments:		
SIRO Sign off: (For major projects)		
Consultation responses reviewed by:		
This DPIA will be kept under review by:		The DPO should also review ongoing compliance with DPIA