Park Lane Surgery

Data Protection Impact Assessment

Document History

Document Reference:	…
Document Purpose:	The purpose is to have the potential to detect and mitigate information risks, as well as to modify plans accordingly. A DPIA should be completed when the following activities occur: • Developing or procuring any new programme, policy, procedure, service, technology or system ("project") that handles or collects information relating to individuals. • Developing revisions to an existing programme, policy, procedure, service, technology or system which significantly change how information is managed.
Date Approved:	6 April 2021
Version Number:	4.0
Status:	FINAL
Next Revision Due:	April 2022
Developed by:	Paul Couldrey – IG Consultant
Policy Sponsor:	Practice Manager
Target Audience:	This policy applies to any person directly employed, contracted, working on behalf of the Practice or volunteering with the Practice.
Associated Documents:	All Information Governance Policies and the Information Governance Toolkit, and Data Security and Protections Toolkit 2020

Data Protection Impact Assessment (DPIA)

When to carry out a DPIA

The DPIA identifies and assesses privacy implications where information (data) about individuals is collected, stored, transferred, shared, and managed. It should be process rather than output orientated.

The purpose is to have the potential to detect and mitigate information risks, as well as to modify plans accordingly.

A PIA should be completed when the following activities occur:

- Developing or procuring any new programme, policy, procedure, service, technology or system ("project") that handles or collects information relating to individuals.
- Developing revisions to an existing programme, policy, procedure, service, technology or system which significantly change how information is managed.

The UK General Data Protection Regulation (UK GDPR) became law on 25th May 2016, with the Data Protection Act 2018 replacing all previous data protection laws in the UK.

The Regulation in Article 35 (recitals **84, 89, 90, 91, 92, 93, 95**) makes it obligatory to perform a Data Protection impact assessment in case of large scale processing of special categories of data **(as in this case health data and genetic data see article 9(1)**. This could help to ascertain the legal basis for processing, which will be helpful for public authorities now that the open door of 'legitimate interests' is closed. It is also important to note that "a single assessment may address a set of similar processing operations that present similar high risks". This could significantly help in reducing the administrative burden for hospitals and health and care providers when performing such an \\assessment.

A data protection impact assessment shall in particular be required in the case of:

(a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;

(b) processing on a large scale of special categories of data referred to in **Article 9(1),** or of personal data relating to criminal convictions and offences referred to in Article 10; or

(c) a systematic monitoring of a publicly accessible area on a large scale.

This DPIA has been designed to meet the requirements of current legislation and common law duties and the expanded requirements of the UK GDPR as above, however Consent modelling / Fair Processing modification should be addressed by separate Trust UK GDPR action plans and strategies as several of the policies currently in use will need to be updated to reflect legislative changes.

Step 1 – Project Details

Project name/title	**COVID Vaccine Invitation Project**
Description and purpose of the initiative – Include how many individuals will be affected by the initiative. A project to ensure all patients are invited for their Coronavirus vaccine, once they become eligible and available	
Details of any link to any wider initiative (if applicable)	This project will go ahead across the whole of Greater Derby and Derbyshire.
Stakeholder Analysis List those who may be affected (stake holder have been consulted prior to project start), eg. Service Users, Clients, Staff-managers and practitioners, Trade Unions, Visitors, Professional organisations, IT providers, Regulators and inspectorial bodies, MPs, Councillors, Partner organisations, Media, Carers	**Internal:** All staff **External:** Nil
Does the initiative involve the use of existing personal and/or confidential data: • **For new purposes?** • **In different ways?** **If so, please explain** (if not already covered above)	Uses existing personal data
Are potential new purposes likely to be identified as the scope of the initiative expands?	Likely to lead to a vaccine denied audit
What is already available? Any Previous PIA, Research or Consultation undertaken.	

Step 2 – Contacts

Who is completing this assessment?	
Name	Louis Wood
Job Title	Assistant Practice Manager
Department/Directorate name	
Contact address	2 Park Lane, DE22 2DS
Email address	Louis.wood1@nhs.net
Telephone number	01332 552461
Connection to Project	Practice Project Lead

Other person(s) with responsibility for this initiative e.g. Project Manager/Director, Senior Responsible Officer (SRO)	
Name	Lesley Hutchinson
Job Title	Practice Manager
Department/Directorate name	
Contact address	2 Park Lane, DE22 2DS
Email address	Lesley.hutchinson@nhs.net
Telephone number	01332 552461
Connection to project	Vaccination Centre Lead Admin

Technical Lead(s) (if relevant)	
Name	
Email address	
Telephone number	

Step 3 – Screening Questions

The purpose of these questions is to establish whether a full Privacy Impact Assessment is necessary and to help to draw out privacy considerations					
		Yes	**No**	**Unsure**	**Comments - document initial comments on privacy impacts or clarification for why this is not an issue or why you are unsure**
I	Is the information about individuals likely to raise privacy concerns or expectations e.g. health records, criminal records or other information people would consider particularly private?		✓		
ii	Will the initiative involve the collection of new information about individuals?	✓			Collection of COVID vaccination refusals
iii	Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?		✓		
iv	Will the initiative require you to contact individuals in ways which they may find intrusive[1]?		✓		
v	Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?	✓			Sharing of patient information with Swiftqueue – a booking system for patients attending COVID vaccination appointments
vi	Does the initiative involve you using new technology which might be perceived as being privacy intrusive e.g. biometrics or facial recognition?		✓		
vii	Will the initiative result in you making decisions or taking action against individuals in ways which can have a significant impact on them?		✓		
viii	Will the initiative compel individuals to provide information about themselves?	✓			Provide information to input into Swiftqueue booking system

If you answered **No** to <u>all</u> of the above screening questions, and you can evidence/justify your answers in the comments box above, you do not need to continue with the PIA.

Should the project at any point in the future use personal information you will need to revisit the screening questions and the PIA.

If you answered or **Unsure** to any of the above, please continue with the PIA.

[1] Intrusion can come in the form of collection of excessive personal information, disclosure of personal information without consent and misuse of such information. It can include the collection of information through the surveillance or monitoring of how people act in public or private spaces and through the monitoring of communications whether by post, phone or online and extends to monitoring the records of senders and recipients as well as the content of messages

Step 4 – Data Collection

Please mark all information to be collected

Description	Specific data item (s)	Justification Reason that the data item(s) is/are needed
Personal Details	**Name** **DOB** **NHS No.** **Mobile Number** **Gender**	These specific details are required to ensure the patient is matched with the correct medical record, and that the COVID vaccination information transferred to the corresponding GP surgery.
Family, lifestyle and social circumstances		N/A
Education and training details		N/A
Employment details	Not applicable	N/A
Financial details	Not applicable	N/A
Sensitive Data: **Racial or ethnic origin**		N/A
Sensitive Data: **Physical or mental health or condition** NB. Includes treatment if applicable. Include Mental Health status eg. whether detained or voluntary under the Mental Health Act if applicable.	Not applicable ☐	N/A
Sensitive Data: **Sexual identity and life**	Gender	For adverse effects monitoring
Sensitive Data: **Religious or other beliefs of a similar nature**	Not applicable ☐	N/A
Sensitive Data: **Trade union membership**	Not applicable ☐	N/A
Sensitive Data: **Offences including alleged offences**	Not applicable ☐	N/A

Description	Specific data item (s)	Justification Reason that the data item(s) is/are needed
Sensitive Data: **Criminal proceedings, outcomes and sentences**	Not applicable ☐	N/A

Step 3 – The Information Asset

How will the data be obtained and from where?	Information will be obtained either from our existing records or provided by the patient themselves via the internet or telephone
How will the data be used?	The data will be used to book an appropriate appointment and to transfer vaccination information into our clinical system to match with the patient's record
Will the data be used locally or nationally? If National, list any available guidance	Locally
Who will be the owner of the information? Ie. the Information Asset Owner (IAO) This is usually the Director or Service Lead under which this asset sits	Park Lane Surgery
Who will be the Information Asset Administrator? (IAA) This is usually the Business Manager or person with day-to-day access and control	Park Lane Surgery
Will a Third Party have access to the information? If so, name the third party, the circumstances and details of how the data will be accessed	No
Will the data be shared with any other team or organisation? If so, name the organisation and the circumstances If so, is there a data sharing agreement in place?	Data will be shared between us and outcomes for health – the vaccination recording software – consent for this is gained at the time of the vaccination at their vaccination site.

Step 8 – Data Flows

Please provide a process map or diagram if available, or complete the table below

The answer to most the questions for the data flows are the same, as described below.

Name of Flow	**What is the purpose of the data flow?**	**Will you be receiving data or sending it or both?**	**Where will you be receiving it from and/or sending it to?**	**Is the data anonymised?**	**Is the data electronic or paper?**	**How is the data to be transferred? Eg. via a system, email, fax, post, by hand**	**How will the data be secured in transit? Eg. nhs.net to nhs.net**	**How often will data be transferred?**	**How many records in each transfer?**	**Where will the data be stored?**	**How will the data in storage be secured?**
COVID Vaccine	Vaccination Status	Both	Received from pt > to Swiftqueue > to Outcomes for health > to Us	No	Eelectronic	Via secure internet – System to system	Secure NHS web	Once per vaccination	Varies from 1-1000 per day	Local secure medical system	Via smartcard + password protection

Step 9 – Data Protection Act Compliance

Name the data controller(s) The data controller is the organisation which, alone or jointly or in common with other organisations, determines the purposes for which and the manner in which any personal data are, or are to be, processed. The data controller takes responsibility for complying with the UK GDPR.	Park Lane Surgery
Name any data processors and provide contact details A data processor means any organisation which processes the data on behalf of the data controller.	Outcomes For Health
What is the legal basis for processing the data? Eg. Consent, Required by Law, etc.	Consent

Data Protection Act Principles

Principle	Response	Actions required
Principle 1: Personal data shall be processed lawfully, fairly and in a transparent manner.		
Individuals affected by the project must be informed about the processing of their data. Has a fair processing notice been provided or is a new or revised communication needed?	Consent gained from pt on booking	
What processes are in place to ensure that data required for secondary purposes is pseudonymised (or anonymised)?	Nil – personal data isn't used for secondary purposes	
If you are relying on consent to process personal data, how will consent be obtained and recorded, what information will be provided to support the consent process and what will you do if permission is withheld or given but later withdrawn?	Consent is gained either verbally or via SMS message and recorded in their medical record if processed by us.	
Principle2: Personal data shall be collected for specified, explicit and legitimate purposes		
What procedures are in place to ensure that privacy implications are considered prior to using data for a different purpose to that originally specified?	Any reports conducted within our clinical system do not use personal data	
Principle 3: Personal data shall be adequate, relevant and limited to what is necessary		
What procedures are in place for ensuring that data collection is adequate, relevant and not excessive in relation to the purpose for which data are being processed?	Collect only the information required by the external software	

Principle	Response	Actions required
How will you ensure that the data you are using is likely to be of good enough quality for the purposes it is used for?	Compare information given to that recorded in our clinical system	
Principle 4: Personal data shall be accurate and where necessary kept up to date.		
What procedures are in place for ensuring that data collection is accurate?	Data given verbally should match with that in our clinical system	
What procedures are in place for ensuring that data collection is kept up to date?	Any contact with patients confirms their most up to date information	
What procedures are in place to correct inaccurate data when requested to do so by a data subject?	Staff are adequately trained to make any necessary amendments	
Principle 5: Personal data shall be kept in a form which permits identification of the data subject for no longer than is necessary		
How long is the data to be retained for?	Unknown	
What procedures are in place for archiving / anonymisation / deletion / destruction of the data?	Use of PCSE / Outcomes for health Records retention policy	
Are there likely to be any exceptional circumstances for retaining certain data for longer than the normal period(s)?	Nil foreseeable	
What procedures are in place to provide data subjects access to their records?	NHS App / Systmonline	
What procedures are in place to prevent the processing of data which may cause damage or distress?	Redaction Software used upon request of records should it be necessary	
What procedures are in place for data subjects who may require the rectification, blocking, erasure or destruction of inaccurate data?	Staff adequately trained to action any inaccurate data	

Principle	Response	Actions required
Principle 6: Appropriate technical & organisation measures shall be taken against unauthorised or unlawful processing of personal data & against accidental loss destruction or damage		
What procedures are in place to ensure that all staff who have access to the data undertake information governance training?	System warnings from our training portal to remind management and staff	
What procedures are in place to ensure that data, whether at rest or in transit, is secured?	Managed by NHSE and our IT contractor NECS	
What procedures are in place to prevent the unauthorised disclosure of data to third parties?	End to end encryption Password and smartcard access only to the data	
Please ensure that the Checklist for Third Party Supplier of Services is completed where any new system is being introduced		

Common Law Duty of Confidentiality

	Assessment of Compliance
Has the individual to whom the information relates given consent?	**Y**
Is the disclosure in the overriding public interest?	**N/A**
Is there a legal duty to do so, for example a court order	**N**
Is there a statutory basis that permits disclosure such as approval under Section 251 of the NHS Act 2006	**N**

Human Rights Act 1998

The Human Rights Act establishes the right to respect for private and family life. Current understanding is that compliance with the Data Protection Act and the common law of confidentiality should satisfy Human Rights requirements.

Will your actions interfere with the right to privacy under Article 8? – have you identified the social need and aims of the project? **Are your actions a proportionate response to the social need?**
N/A

Step 10 – Privacy issues identified and risk analysis

Any privacy issues which have been identified during the PIA process (for example: no legal basis for collecting and using the information; lack of security of the information in transit, etc.) should be documented in the risk register template embedded below. This risk register will enable you to analyse the risks in terms of impact and likelihood and document required action(s) and outcomes.

Note that where it is proposed that a privacy risk is to be 'accepted', approval for such acceptance should be sought from the Caldicott Guardian where patient data is concerned and the SIRO for all information risks.

The PMO holds the formal project risk register each IG lead should identify and records IG risks via the PMO.

Step 11 – Data Protection Principles Compliance and Authorisation

Please provide a summary of the conclusions that have been reached in relation to this project's overall compliance with the DPPs. This could include indicating whether some changes or refinements to the project might be warranted.

Information Asset Owner	**Name: Louis Wood** **Date: 22/04/2021** **Signature:** Louis Wood
Reasoning behind the decision to accept or reject the identified privacy risks	
Caldicott Guardian (only where the personal data are about patients)	**Name: Lesley Hutchinson** **Date: 22/04/2021** **Signature:**
Reasoning behind the decision to accept or reject the identified privacy risks	
Senior Information Risk Owner (where the identified privacy risks are significant)	**Name:** **Date:** **Signature:**
Reasoning behind the decision to accept or reject the identified privacy risks	
Information Governance Lead	**Name: Lesley Hutchinson** **Date: 22/04/2021** **Signature:**
Reasoning behind the decision to accept or reject the identified privacy risks	

References

- Data Protection Act 2018;
- General Data Protection Regulations 2016
- The Caldicott Principles;
- Common Law Duty of Confidentiality;
- The Freedom of Information Act 2000;
- The Mental Capacity Act 2005;
- Section 251 of the NHS Act 2006 (originally enacted under Section 60 of the Health and Social Care Act 2001);
- Public Health (Control of Disease) Act 1984;
- Public Health (Infectious Diseases) Regulations 1988;
- The Gender Recognition Act 2004;
- Confidentiality: NHS Code of Practice 2003;
- IGA Records Management Code of Practice for Health and Social Care 2016;
- Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 2013;
- Abortion Regulations 1991;
- Road Traffic Act 1988;
- ICO Data Sharing Code of Practice;
- Confidentiality and Disclosure of Information Directions 2013;
- Health and Social Care Act 2012;
- The Criminal Justice Act 2003;
- The NHS Information Security Management Code of Practice 2007;
- The Computer Misuse Act 1990;
- The Electronic Communications Act 2000;
- The Regulation of Investigatory Powers Act 2000;
- The Prevention of Terrorism Act 2005;
- The Copyright, Designs and Patents Act 1988;
- The Re-Use of Public Sector Information Regulations 2005;
- The Human Rights Act 1998;
- The NHS Care Record Guarantee 2007; and
- Anonymisation Standard for Publishing Health and Social Care Data Code of Confidentiality.