Version: **5.0**
Date: **October 2022**

This template is for use by Practices to Comply with the UKGDPR requirement to have a Data Protection Impact Assessment and that new processing of Patient Data undergo a DPIA process if appropriate. The template is Generic in design as PCIG Consulting have clients across the UK, local sharing arrangements and area specific sharing or processing will need to be added by the practice.

Change Control

Version	To	Change	Date
1	2	Reformatting and spelling corrected	13 August 2019
2	3	Reviewed and Updated	1 May 2020
3	4	Reviewed and Updated	14 February 2022
4	5	Reviewed and Updated	11 October 2022

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:	11 October
Version Number:	5.0
Status:	FINAL
Next Revision Due:	October 2023
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 General Data Protection Regulation (UKGDPR) became law on 24th May 2016, is a single regulation on the protection of confidential and sensitive information. It enters into force on the 25th May 2018, repealing the Data Protection Act (1998).

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 UKGDPR as above, however Consent modelling / Fair Processing modification should be addressed by separate UKGDPR 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	**Patient Full Online Access**

Description and purpose of the initiative – From 01 November 2022, patients with online accounts such as through the NHS App will be able to read new entries in their health record. This applies to patients whose practices use the TPP and EMIS systems. Arrangements with practices which use Vision as the clinical system are under discussion.

This is an NHS England and NHS Improvement programme supported by NHS Digital. The change supports the NHS Long-Term Plan commitments to provide patients with digital access to their health records.

It means GPs and practice staff will need to consider the impact of each entry, including documents and test results, as they add them to a patient's record. Patients will not see personal information – such as positive test results – until they have been checked and filed, giving GPs the chance to contact and speak to patients first.

Key Points

- No historical information will be available to patients; however, this is the programme pipeline for 2023
- Patients will only see information from their current registered practice, previous practice information will not be available
- Patients will not have access to administrative tasks or communications between practice staff
- Patients get access to their future record by default and have access to all correspondence, SNOMED and free text information
- GPs can decline patients access to their own records in particular circumstances
- Under 16 will not be able to see their record unless the GP gives access.
- If a patient moves practice they will only have full record access from the date they register with the new practice and will lose access to historic data.

Safeguarding

- For vulnerable adults it may be appropriate to redact or prevent specific information entered into the GP medical record from being shared within the patient's access and view. To help manage these situations, further materials are being produced in collaboration with the Royal College of General Practitioners and safeguarding experts.

Details of any link to any wider initiative (if applicable)	NHS England and NHS Improvement programme supported by NHS Digital

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: Staff / Processes** **External: NHSD?NHSE?NHSX _ Patients**
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)	Different Way patients having more access to their data online.
Are potential new purposes likely to be identified as the scope of the initiative expands?	No
What is already available? Any Previous PIA, Research or Consultation undertaken.	NHSX guidance At:- https://digital.nhs.uk/services/nhs-app/nhs-app-guidance-for-gp-practices/accelerating-patient-access-to-their-record/giving-patients-online-access-to-their-medical-records-guidance-for-gp-practices

Step 2 – Contacts

Who is completing this assessment?	
Name	Lisa.Wolverson
Job Title	Practice Manager
Department/Directorate name	Lockstown Practice
Contact address	Gomer Street, Willenhall, WV13 2DR
Email address	
Telephone number	01902 600833
Connection to Project	Practice Manager or GP Surgery

Other person(s) with responsibility for this initiative e.g. Project Manager/Director, Senior Responsible Officer (SRO)	
Name	**Dr Wasima Mandal**
Job Title	**GP Partner**
Department/Directorate name	**Lockstown Practice**
Contact address	**Gomer Street, Willenhall, WV13 2DR**
Email address	
Telephone number	**01902 600833**
Connection to project	**GP Partner**

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?	Yes			Patients will only see their information once it has been checked and entered, or filed, onto the GP practice clinical system. This means general practice staff will continue to be able to prevent patients from seeing any sensitive information before patients can see it. General practice will also be able to remove access for the very small number of exceptional circumstances where access is inappropriate, considered harmful or where there may be safeguarding concerns. These changes only apply to a patient's general practice record. Other health services records will not be visible to patients. Even if other services use the same clinical system, information will not be viewable by the patient, unless it has been filed into the general practice record. If a patient downloads the NHS App or other patient facing app after the 'go-live' date, they will see any information entered onto their record from the 'go-live' date, unless it has been hidden by the general practice. There will be a requirement to review information as it is entered into the clinical system. In circumstances where it is deemed inappropriate for a patient to see all or part of a record, for their safety, this information can be redacted and hidden from the patient view as necessary. There are benefits to giving patients access to their health record, including improvements in a range of healthcare quality and safety outcomes, and enabling patients to take greater control of the

					management of their health conditions. We also know patients want to see their records. A lack of record access is the most complained about feature in the NHS App. We want to make it easier for GPs to provide record access and for patients to get access to their records.
ii	Will the initiative involve the collection of new information about individuals?		No		
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?		No		
iv	Will the initiative require you to contact individuals in ways which they may find intrusive[1]?		No		
v	Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?		No		
vi	Does the initiative involve you using new technology which might be perceived as being privacy intrusive e.g. biometrics or facial recognition?		No		
vii	Will the initiative result in you making decisions or taking action against individuals in ways which can have a significant impact on them?		No		
viii	Will the initiative compel individuals to provide information about themselves?		No		

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		
Family, lifestyle and social circumstances	Marital/partnership status Next of kin Carers/relatives Children/dependents Social status e.g. Housing	*Article 6, e) 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;"* *Article 9, (h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems*
Education and training details	Education/ Qualifications Professional training Not applicable	*Article 6, e) 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;"* *Article 9, (h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems*
Employment details	Employment status ☐ Career details ☐ Other ☐ specify: Not applicable	*Article 6, e) 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;"* *Article 9, (h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems*

Description	Specific data item (s)	Justification Reason that the data item(s) is/are needed
Financial details	Income ☐ Salary ☐ Bank details ☐ National Insurance number ☐ Benefits ☐ Other ☐ specify: Not applicable	N/A
Sensitive Data: **Racial or ethnic origin**	Racial/ethnic origin ☐	*Article 6, e) 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;"* *Article 9, (h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems*
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 ☐	*Article 6, e) 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;"* *Article 9, (h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems*
Sensitive Data: **Sexual identity and life**	☐ List the data items: Not applicable ☐	*Article 6, e) 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;"* *Article 9, (h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems*

Description	Specific data item (s)	Justification Reason that the data item(s) is/are needed
Sensitive Data: **Religious or other beliefs of a similar nature**	☐ Not applicable ☐	*Article 6, e) 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;"* *Article 9, (h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems*
Sensitive Data: **Trade union membership**	☐ Not applicable ☐	N/A
Sensitive Data: **Offences including alleged offences**	☐ List the data items: Not applicable ☐	*Article 6, e) 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;"* *Article 9, (h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems*
Sensitive Data: **Criminal proceedings, outcomes and sentences**	☐ List the data items: Not applicable ☐	*Article 6, e) 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;"* *Article 9, (h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems*

Step 3 – The Information Asset

How will the data be obtained and from where?	**Patient and other NHS sources**
How will the data be used?	Direct Patient Care
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	Practice Manager / GP for patient Record
Who will be the Information Asset Administrator? (IAA) This is usually the Business Manager or person with day-to-day access and control	Practice Manager
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	System Supplier Patient
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?	N/A

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?

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 UKGDPR.	**Lockstown Practice**
Name any data processors and provide contact details A data processor means any organisation which processes the data on behalf of the data controller.	System Supplier
What is the legal basis for processing the data? Eg. Consent, Required by Law, etc.	*Article 6, e) 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;"* *Article 9, (h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems*

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?	National Programme advertising patient access by NHSD	Inform patients of access rights. There is an existing professional responsibility to ensure that records are legible and patients understand and are informed about the care that is being provided - clinicians need to write notes bearing in mind that patients may see them. While this is a common concern, our engagement with practices where record access is routinely available, and as wide international experience suggests, this is not a significant issue for patients. Within the NHS App there is currently a 'help with abbreviations section' that supports users with abbreviations commonly found in medical records. We are continuing to improve our national resources to support patients to become more actively involved in their care, and as more people have access to their information this will help justify further investment into improving services and systems to improve the record access experience.

Principle	Response	Actions required
What processes are in place to ensure that data required for secondary purposes is pseudonymised (or anonymised)?	N/A	
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?	N/A	
Principle2: Personal data shall be collected for specified, explicit and legitimate purposes		

Principle	Response	Actions required
What procedures are in place to ensure that privacy implications are considered prior to using data for a different purpose to that originally specified?	Practices will continue to be able to hide individual elements from patient view or remove access from individual patients after the changes have been made. This is existing functionality that is already available in general practice clinical systems as part of the current record access functionality. It will also be possible for practices to identify individual at-risk patients to be excluded from these changes by adding a SNOMED code to their record. These patients will then require an individual review and have their settings manually applied if access can be provided without a risk of serious harm. There are small numbers of patients who are at risk of significant harm from access to their records, less than 2% have risk factors and a smaller number would be appropriate to be refused access. Practices may already have a safeguarding list which should be reviewed to identify individual patients where they think giving access may cause significant harm. It is important to consider all patients and not just those who currently have online access, as patients may have online access at any point in the future.	Ensure Staff are aware of changes to snow codes to review item from patient view.
Principle 3: Personal data shall be adequate, relevant and limited to what is necessary		

Principle	Response	Actions required
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?	Reliant of patient and staff	N/A
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?	Practices will continue to be able to hide individual elements from patient view or remove access from individual patients after the changes have been made. This is existing functionality that is already available in general practice clinical systems as part of the current record access functionality. It will also be possible for practices to identify individual at-risk patients to be excluded from these changes by adding a SNOMED code to their record. These patients will then require an individual review and have their settings manually applied if access can be provided without a risk of serious harm.	
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?	For lifetime of patient record	

Principle	Response	Actions required
What procedures are in place to provide data subjects access to their records?	Prospective access to full records from April 2022 is subject to the same safeguarding requirements and management of third-party information as applied when patients have access to their detailed coded record (DCR). When recording third party information, and if it is unknown to the patient, GP practices will need to ensure that this information becomes redacted from patient view. Practices should also ensure that information is recorded in a way which makes it easy for the patients to understand it. Guidance on safeguarding, sensitive data, and data recording is available within the records access section of the RCGP toolkit. GP records sometimes contain information that is confidential about a third party, or information that may be considered sensitive to the patient which would cause harm. Prospective access to full records from April 2022 is subject to safeguarding requirements and checks.	

Principle	Response	Actions required
What procedures are in place for data subjects who may require the rectification, blocking, erasure or destruction of inaccurate data?	It is important to note that although patients have a 'right to rectification' and a 'right to erasure', diagnoses (even incorrect ones) should remain in the record (with an indication that they are incorrect). Other 'matters of fact' can be rectified if they are incorrect. Examples are • Right to rectification • When a patient wants to amend their medical records The responsibility for information lies with the creator of the document. The patient may disagree with the content held on the record and this may be recorded. If information held within the record is agreed to be incorrect this should be recorded and remedied.	Refer to practice policy and DPO when request are received.
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?	Yearly staff training to comply with DS&P Toolkit	Yearly Requirement
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?	**Patients consent is when they request full access**
Is the disclosure in the overriding public interest?	**NO**

Is there a legal duty to do so, for example a court order	
Is there a statutory basis that permits disclosure such as approval under Section 251 of the NHS Act 2006	**Requirement by law to provide access.**

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?**
None.

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:** **Date:** **Signature:**
Reasoning behind the decision to accept or reject the identified privacy risks	
Caldicott Guardian (only where the personal data are about patients)	**Name:** **Date:** **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:** **Date:** **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.