Project:	**Emis Record Viewer**
Document Title:	**Data Protection Impact Assessment**
Author:	**C Sims**
Version	**V1.0**
Status:	**In progress**

Version History

Revision Date	Version Number	Summary of Changes	Changes Marked

Reviewed by

This document (or its component) parts have been reviewed by the following

Name	Title & Company	Issue Date	Version

Approvals

This document requires the following approvals:

Name	Signature	Title	Date of Issue

Distribution

This document has been distributed to :

Name	Title & Company	Date

Contents

1. Introduction

A Data Protection Impact Assessment (DPIA), (formerly known as privacy impact assessment or PIA), is a method of helping organisations identify the most effective way to comply with their data protection obligations and meet individuals' expectations of privacy. An effective DPIA will allow organisations to identify and fix problems at an early stage, reducing the associated costs and damage to reputation, which might otherwise occur.
You must carry out a DPIA when:

- using new technologies; and the processing is likely to result in a high risk to the rights and freedoms of individuals

- Processing that is likely to result in a high risk includes (but is not limited to): systematic and extensive processing activities, including profiling and where decisions that have legal effects – or similarly significant effects – on individuals

- large scale processing of special categories of data or personal data relation to criminal convictions or offences; this includes processing a considerable amount of personal data at regional, national or supranational level; that affects a large number of individuals; and involves a high risk to rights and freedoms e.g. based on the sensitivity of the processing activity large scale, systematic monitoring of public areas (CCTV)

2. Data Protection Impact Assessment Process

- All new proposals for processing of data are required to undertake the screening process (see below) to establish whether a full DPIA is needed

- Completing the screening process and the DPIA are the responsibility of the Project Manager or Sponsor

- The DPIA must be reviewed and signed by an appropriate authorising officer (Data Protection Officer/Senior Information Risk Owner/Caldicott Guardian)

- Where appropriate, information risk should be recorded in existing documentation, e.g. project risk register, corporate risk register

- The DPIA must be updated if changes to the processing are proposed and reviewed at appropriate stages

- Remember to record all information assets and data flows on your Information Asset Register and Data Flow Map

3. Screening Questions

Project ID:	**Date: 2/1/2019**		
Project Manager:			
DPIA Screening Questions	**Yes (x)**	**No (x)**	**Comments**
Will the project involve the collection of new information about individuals?		x	Project uses existing patient information
Will the project compel individuals to provide information about themselves?		x	Patients can nominate a pharmacy for EPS2 scripts, they will then be able to give signed consent separately to allow the pharmacy to view their details on GP record viewer. Consent can be withdrawn at any time
Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?	x		The GP record viewer will permit pharmacies to securely view certain data in the patient record, medication, allergies and some key test results related to the medication prescribed. This is by explicit consent from the patient. Access to the record will be controlled by the smartcard role both at the practice and in the pharmacy.
Do you propose using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?		x	Records viewer will allow the practice and local pharmacy to work together through EPS to deliver a faster safer service.
Does the project involve you using new technology which might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition.		x	The software is already present in Emisweb and at Proscript pharmacies and is using existing smartcard roles to restrict access the patient data.
Will the project result in you making decisions or taking action against individuals in ways which can have a significant impact on them?		x	It should improve patient safety, reduce the potential issues arising from pharmacies being unaware

			of potential issues to dispensing, and allow them to support the GP in safe prescribing
Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? E.g. health records, criminal records or other information that people would consider to be particularly private.		x	Prescribing information is already shared via EPS2 and on FP10.
Will the project require you to contact individuals in ways which they may find intrusive?		x	Once the patient has consented to the pharmacy having access to the record viewer there will be no need to contact them. Patients can opt out at any time.
Will the project store information using cloud technology?		x	Data is hosted by Emis health as part of the existing patients clinical record.
Will the project transfer information outside the European Economic Area?		x	

- If you answered **no** to all the questions, you **DO NOT** need to proceed to a full Data Protection Impact Assessment. Save this document to evidence your assessment

- If you answer **yes** to any of these questions, you **DO** need to proceed to a full Data Protection Impact Assessment. Complete the following sections and save to evidence your assessment

4. Full DPIA

Steps	Requirements	Suggested Accompanying Documents
1. Identify the need for a DPIA	• Explain what the project aims to achieve, what the benefits will be to the organisation, to individuals and to other parties.	 EMIS GPRV Patient Information Leaflet
2. Describe the information flows	• Describe the collection, use and deletion of personal data • Identify individuals who are likely to be affected by the project	Patients nominate a pharmacy to deliver the medicines management service via EPS2. The patient can then give written consent for the pharmacy to be able to view their medication, allergies and review key blood results pertaining to the medication requested, this will enable pharmacists and practices to work together to deliver a safer service for patients and reduce the risk of information being lost, or prescriptions being dispensed when inappropriate.
Note: Discuss the project with your IG Lead/Data Protection Officer		
3. Identify the privacy and related risks	• Identify the key privacy risks and the associated compliance and corporate risks. • Activities may include discussions and workshops with stakeholders and the IG Lead • Data Protection Principles found below should be used to help identify the Data Protection Legislation related compliance risks.	The risk of patient information being lost or shared outside of the GP/pharmacy environment are reduced. Patient safety is increased as the pharmacy has direct access to the patient medication, allergies and blood results related to the prescribed medication. As patients have to provide written, signed consent for the pharmacy to use Record Viewer there is no further risk

Steps	Requirements	Suggested Accompanying Documents
Identify privacy solutions	• Describe the actions you could take to reduce the risks, and any future steps which would be necessary (e.g. the production of new guidance or future security testing for systems).	
Agree and record the DPIA outcomes	• Agree risk owners and action owners • Apply mitigation and reassess risk • Record recommendations here	
Integrate the DPIA outcomes back into the project plan	• Identify who is responsible for integrating the DPIA outcomes back into the project plan and updating any project management paperwork • Identify who is responsible for implementing the solutions that have been approved • Identify who the contact is for any privacy concerns which may arise in the future	

Signoff by authorised officer:

Data Protection Officer

Name: Caroline Sims

Role: Primary Care Information Governance Manager and DPO

Signature: 

Date: 2/1/2019

5. Linking the DPIA to Data Protection Legislation.

Answering these questions during the DPIA process will help you to identify where there is a risk that the project will fail to comply with the Data Protection Legislation and other relevant legislation, for example the Human Rights Act and the Common Law Duty of Confidentiality.

Principle 1 (a), from the GDPR Article 5 - Lawfulness, fairness and transparency

Previous DPA98 Principle 1 - Personal data shall be processed fairly and lawfully

- Have you identified the purpose of the project?
- What is the legal basis for processing?
- How will individuals be told about the use of their personal data?
- Do you need to amend your privacy notices?
- If you are relying on consent to process personal data, how will this be collected and what will you do if it is withheld or withdrawn?

If your organisation is subject to the Human Rights Act, you also need to consider:

- 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?

If your organisation is subject to the Common Law Duty of Confidentiality, you also need to consider:

- Will the information be given under a Duty of Confidentiality?

Principle 1 (b) from the GDPR Article 5 - Purpose limitation

Previous DPA98 Principle 2 - obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

- Does your project plan cover all of the purposes for processing personal data?
- Have potential new purposes been identified as the scope of the project expands?

Principle 1 (c) from the GDPR Article 5 – Data minimisation

Previous DPA98 Principle 3 - Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

- Is the information you are using of good enough quality for the purposes it is used for?
- Which personal data could you not use, without compromising the needs of the project?

Principle 1 (d) from the GDPR Article 5 - Accuracy

Previous DPA98 Principle 4 - Personal data shall be accurate and, where necessary, kept up to date.

- If you are procuring new software does it allow you to amend data when necessary?

- How are you ensuring that personal data obtained from individuals or other organisations is accurate?
- How will you maintain accuracy over time?

Principle 1 (e) from the GDPR Article 5 - Storage Limitation

Previous DPA98 Principle 5 - not be kept for longer than necessary for that purpose or those purposes.

- What retention periods are applicable for the personal data you will be processing?
- Are you procuring software which will allow you to delete information in line with your retention periods?
- Could you set the software to automatically delete information on its disposal date?

From the GDPR Articles 12 – 23 - Individual rights

Previous DPA98 Principle 6 - processed in accordance with the rights of data subjects

- Do you need consent of the individual to process this information?
- How can you take account of objections to the processing?
- Will the systems you are putting in place allow you to respond to subject access requests more easily?
- Are you processing information of children aged 13-16?
- If the project involves marketing, have you got a process for individuals to opt **IN** to their information being used for that purpose?
- How do you consider and action requests to cease processing?
- How do you consider and action requests to delete an individual's information?

Principle 1 (f) from the GDPR Article 5 – Integrity and Confidentiality

Previous DPA98 Principle 7 - Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of or damage to, personal data.

- Do the new systems provide adequate protection against the security risks you have identified?
- What training and instructions are necessary to ensure that all staff know how to operate a new system securely?
- If you are transferring data, how will this be done securely?
- How will you protect the data at rest?

From the GDPR Article 3 – Territorial Scope

Previous DPA98 Principle 8 - not transferred to a country or territory outside the European Economic Area (EEA) unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

- Will the project require you to transfer data outside of the EEA?
- If you will be making transfers, how will you ensure that the data is adequately protected?