



<b>Project:</b>	<b>Chain SMS - Accurx</b>
<b>Document Title:</b>	<b>Data Protection Impact Assessment</b>
<b>Author:</b>	<b>J Crowshaw</b>
<b>Version</b>	<b>1</b>
<b>Status:</b>	<b>Approved 30/09/19</b>

### Version History

Revision Date	Version Number	Summary of Changes	Changes Marked
08/08/19	1	New Assessment	

### Reviewed by

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

Name	Signature	Title	Date of Issue
J Crowshaw	See email	Practice Manager Caldicott Guardian	08/08/19

### Approvals

This document requires the following approvals:

Name	Signature	Title	Date of Approval
Dr J Tankel	See email	SIRO Managing Partner	10/08/19

### Distribution

This document has been distributed to :

Name	Title & Company	Date

## **Contents**

1. Introduction.....	3
2. Data Protection Impact Assessment Process.....	3
3. Screening Questions.....	4
4. Full DPIA .....	7
5. Linking the DPIA to Data Protection Legislation. ....	10

# 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. Security Questions

Project ID: Chain SMS text software	Date: 14/11/2018		
Project Manager:			
DPIA Screening Questions	Yes (x)	No (x)	Comments
Will the project involve the collection of new information about individuals?		X	
Will the project compel individuals to provide information about themselves?		X	Mobile phone numbers will already be provided as part of the patient registration.
Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?		X	
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	Simple text messaging to alert for appointments, to contact surgery and reminders about direct care, flu, chronic disease reviews etc.
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	
Will the project result in you making decisions or taking action against individuals in ways which can have a significant impact on them?		X	
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	
Will the project require you to contact individuals in ways which they may find intrusive?		X	Patients will be advised at the practice, when registering, on the website and given the option to opt out. No medical data or personal information will be transmitted.
Will the project store information using cloud technology?	X		Data stored on the London Microsoft Azure

			data centre. All data sent is encrypted. Full information is available at <a href="https://www accurx.com/gdpr-questions">https://www accurx.com/gdpr-questions</a>
Will the project transfer information outside the European Economic Area?		x	

## 4. Screening Questions

- 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

## 5. Full DPIA

<i>Steps</i>	<i>Requirements</i>	<i>Suggested Accompanying Documents</i>
<u><b>1. Identify the need for a DPIA</b></u>	<ul style="list-style-type: none"> <li>• Explain what the project aims to achieve, what the benefits will be to the organisation, to individuals and to other parties.</li> <li>• A system which allows the practice to easily send text messages to patients. It means the practice can be much more proactive about some communications, messaging patients quickly and securely, so they are not waiting around to hear from the practice</li> <li>• Reminders or notifications (e.g. prescription ready)</li> <li>• Responding to simple queries (e.g. if patients had a quick question about their medication)</li> <li>• Letting patients know we tried to call</li> <li>• Sending patients advice at the end of a consultation</li> </ul>	<ul style="list-style-type: none"> <li>• <b>Project Initiation Document</b> or other relevant project documents</li> </ul>
<u><b>2. Describe the information flows</b></u>	<ul style="list-style-type: none"> <li>• In order to send messages to patients, the message text, mobile number and NHS number are sent to the secure servers. The data is only processed when the practice sends a message.</li> <li>• Only patients receiving a message from the practice will be affected by this project initiative</li> <li>• Accurx use <a href="#">FireText</a> to send SMS messages. To ensure a reliable service, there is also a backup SMS gateway provided by <a href="#">Zensend</a>.</li> </ul>	<ul style="list-style-type: none"> <li>• <b>Flow diagram</b> or a similar method of describing data flows</li> <li>• <b>Stakeholder map</b> or similar</li> </ul>
<b>Note: Discuss the project with your IG Lead/Data Protection Officer</b>		
<u><b>3. Identify the privacy and related risks</b></u>	<ul style="list-style-type: none"> <li>• Cloud Served being hacked</li> <li>• Poor quality of data input at practice, resulting in wrong phone numbers</li> <li>• Shared mobile phones for U18 children with their parents</li> <li>• Incorrect patient data selected for SMS</li> <li>• Sensitive data being sent via SMS</li> </ul>	<ul style="list-style-type: none"> <li>• <b>Larger projects may require a separate project risk register</b>, categorise privacy risks.</li> </ul>

<b>Steps</b>	<b>Requirements</b>	<b>Suggested Accompanying Documents</b>
	<ul style="list-style-type: none"> <li>• Data Processor not complying with the NHS IG Toolkit requirements</li> <li>• Disclosure of patient data when receiving technical support</li> </ul>	
<b><u>Identify privacy solutions</u></b>	<ul style="list-style-type: none"> <li>• Personal data restricted to NHS number, EMIS number, mobile phone number and content of communication sent via AccuRx</li> <li>• Staff training and awareness of need for data accuracy</li> <li>• Data Processor to process data strictly in accordance with the DPA</li> <li>• Any sub-processing to be agreed with the Data Controller</li> <li>• Data Processor to maintain up to date compliance with the NHS IG Toolkit Level 2</li> <li>• Cloud hosting strictly in accordance with the NHS Digital guidance</li> <li>• Data Processor to notify Practice of any data breaches</li> <li>• Patients have the choice to opt out of receiving SMS messages at any time</li> <li>• Data Controller retains Cyber Essentials &amp; Cyber Essentials Plus certification</li> </ul>	
<b><u>Agree and</u></b>	<ul style="list-style-type: none"> <li>• Risk owners Clarendon Surgery &amp; The Angel Medical Practice</li> <li>• Risk assessed as LOW given limited use and content of messages</li> <li>• Service is IG Compliant and the Data Processor is Cyber Essentials certified &amp; registered with the ICO. Numer ZA202115</li> <li>• Compliant with Principle 1(a) Lawfulness, fairness &amp; transparency. Service delivered under Legal Basis 6(1)€ &amp; 9(2)(h)</li> <li>• Compliant with Principle 1(b) Purpose limitation</li> <li>• Compliant with Principle 1(c) Data minimisation</li> <li>• Compliant with Principle 1(d) Accuracy</li> <li>• Compliant with Principle 1(e) Storage Limitation</li> <li>• Compliant with Articles 12 to 23 Individual</li> </ul>	

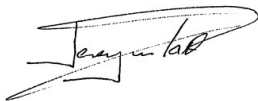


Steps	Requirements	Suggested Accompanying Documents
	rights <ul style="list-style-type: none"> <li>• Compliant with Article 5 Integrity &amp; Confidentiality</li> <li>• Compliant with Article 3 Territorial scope</li> </ul>	
<u><b>Integrate the DPIA outcomes back into the project plan</b></u>	<ul style="list-style-type: none"> <li>• Outcomes already in place</li> <li>• Contact for any concerns, breaches etc is the Practice Manager and or the Data Protection Officer, Senior Information Risk Officer or Caldicott Guardian</li> </ul>	<ul style="list-style-type: none"> <li>• <b>Project plan</b> with privacy actions included</li> </ul>

**Signoff by authorised officer:**

**Data Protection Officer/Senior Information Risk Owner/Caldicott**

**SIRO Name: Dr J Tankel**



**Date: 14/08/19**

## 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?

