NHS
Kent and Medway
Clinical Commissioning Group

Full Data Protection Impact Assessment (DPIA)

Project name:	Ardens EMIS Templates Alerts Reports	
Project lead	**Name:**	David Hadley
	Designation:	Informatics Senior Project Manager
	Telephone:	07432700869
	Email:	david.hadley@nhs.net
Information Asset Owner: ***(if different to above)***		Andrew Brownless
Date:		24/02/2021

Data Protection impact assessment (DPIA) screening questions

Name and short description of project and data sets to be used:

Ardens provide EMIS clinical system templates, standardised referral forms data quality and clinical safety alerts, and searches and reports for GP surgeries. Ardens uses the functionality already available in EMIS and as such does not extend the scope of how EMIS is used for direct patient care but provides enhancements, including:

- Clinical templates and alerts improve the quality of the data being entered into the system and assists practices with recording data and complying with local contract specifications,
- Referral forms ensure consistency with local criteria and provides auto population features,
- Clinical safety alerts and reports based on MHRA and NICE guidance,
- Searches and reports based on national and local contract requirements to assist Practices, PCNs, or CCGs with monitoring performance.

The searches and reports are run locally within each Practices EMIS system and are intended to help clinicians by presenting relevant information in an accessible manner.

The Ardens Pro package allows Practices to upload aggregated counts, based on Ardens standardised searches and reports, to the Ardens Manager UK Amazon Web Services cloud hosted dashboard tool. Currently, data is uploaded by Practices manually using CSV files. Automated extracts are currently not available and may well be an additional cost option. Ardens Manager allows Practices to use activity visualisation tools to benchmark their performance at Practice, PCN and CCG levels. Practice aggregated data can only be shared once a Data Sharing Agreement (DSA) has been signed by individual Practices and the Practice uploads data (this is within Practices' control). The DSA allows Practices control of

how their aggregated data can be viewed using “Access Levels” and “Connected Groups”:

- **Access Levels:** Ardens Manager allows three different access levels:
  - Entire Organisations Dataset: Member organisations can view aggregated reporting data of all organisations.
  - Restricted Organisations Data: Member organisations can only view aggregated reporting data to benchmark individual reports.
  - Group Aggregate: Member organisations can view aggregated group data.
- **Connected Groups:** Member organisations can view aggregated group data of connected groups within the group.

It should be noted that Ardens Manager does not process patient level data and this is specifically forbidden in the terms of service set out within the DSA. The DSA is inserted below, this is a PDF version of the document held within the Ardens Manager application.

Ardens Manager
Data Sharing Agreem

Will this project lead to:	Yes	No	Unsure	Comments
The use of special category, criminal offence data on a large scale		**x**		
The use of special category, criminal offence data being used in a new way		**x**		
Does this project use new technologies or AI		**x**		
Will this lead to systematically monitoring of publicly accessible places on a large scale (i.e. CCTV)		**x**		
Will this project result in the profiling of special category data to decide on access to services		**x**		
Will information about individuals be disclosed to organisations or people who have not previously had routine access to it?		**x**		

Use of personal information			
Description of data: National and local data flows containing personal and identifiable personal information As described above this DPIA is about the tool itself, rather than the system it is being used on. The tool does not save the information being entered, or access identifiable information.			
Personal Data	**Please tick all that apply**	**Sensitive Personal Data**	**Please tick all that apply**
Name		Racial / ethnic origin	
Address (home or business)		Political opinions	
Postcode		Religious beliefs	
NHS No		Trade union membership	
Email address		Physical or mental health	
Date of birth		Sexual life	
Payroll number		Criminal offences	
Driving Licence [shows date of birth and first part of surname]		Biometrics; DNA profile, fingerprints	
		Bank, financial or credit card details	
		Mother's maiden name	
		National Insurance number	
		Tax, benefit or pension Records	
		Adoption, employment, school, Social Services, housing records	
		Child Protection	
		Safeguarding Adults	
Additional data types (if relevant)		N/A	

Lawfulness of the processing				
Conditions for processing for special categories: to be identified as whether they apply				
Condition	**Please tick all that apply**			
Explicit consent unless or allowed by other legal route	Explicit consent	☐	Other legal route	
Processing is required by law				
Processing is required to protect the vital interests of the person				
Is any processing going to be by a not for profit organisation, e.g. a Charity				
Would any processing use data already in the public domain?				
Could the data being processed be required for the defence of a legal claim?				
Would the data be made available public, subject to ensuring no-one can be identified from the data?				
Is the processing for a medical purpose?				
Would the data be made available publically, for public health reasons?				
Will any of the data being processed be made available for research purposes?				

The answers will not specifically identify the legality of the data flow; your responses to the questions below need to identify the specific legal route for processing.

Answer all the questions below for the processing of Personal Confidential Data	
What is the justification for the inclusion of identifiable data rather than using de-identified/anonymised data?	No identifiable data is processed
Will the information be new information as opposed to using existing information in different ways?	N/A
What is the legal basis for the processing of identifiable data? e.g. Conditions under the Data Protection Act 2018, the Section 251 under the NHS Act 2006 etc.	N/A
Where and how will this data be stored?	N/A
Who will be able to access identifiable data?	N/A
Will the data be linked with any other data collections?	N/A
What security measures will be used to transfer the data? Is this in line with cyber security requirements	All system access is via secure encrypted HSCN VPN
What confidentiality and security measures will be used to store the data?	Data about the GP surgery, location and contact details will be stored on Ardens password protected CRM software. No Patient-identifiable data will be stored.
How long will the data be retained in identifiable form? And how will it be de-identified? Or destroyed?	N/A

What governance measures are in place to oversee the confidentiality, security and appropriate use of the data and manage disclosures of data extracts to third parties to ensure identifiable data is not disclosed or is only disclosed with consent or another legal basis?	No identifiable data is being accessed or extracted; the Ardens tools are being installed on the GP systems. Only aggregated data is extracted
What rights will individuals have such as the right to object, and National data opt-out etc.	N/A
Will the privacy notices need to be updated	N/A
Detail audit trails that can be run to ensure information is not used inappropriately	EMIS Web has full audit-trail capability.
How long will this sharing take place?	No identifiable data is being accessed or extracted; only aggregated data is extracted. The extraction process into Ardens Manager is under the direct control of the Practice using manual uploads.

If there are multiple organisations involved in processing the data list below? *If yes, list below*			Yes/No
			No
Name	**Controller (C) or Processor (P)?**	**Information Commissioner Office registration**	**Completed and compliant with the Data Security & Protection Toolkit[1]**
			Yes/No
GP Practice	Controller	Yes	Yes
Ardens Health Informatics Limited.	Processor	Yes	Yes
Has a data flow mapping exercise been undertaken? (please provide details)			Yes/No
			No, only aggregated data is extracted

Review and Risk matrix
Are there any risks to the **Confidentiality** of personal data? *Confidentiality is defined as unauthorised disclosure of, or access to, personal data.* No risks to the reporting system as a whole have been noted, which is what the content of this DPIA covers, as no personal identifiable data is processed. **Deployment Risk** However, there is a transitory risk that occurs during deployment: deployment requires that Ardens associates are granted access to the Practice EMIS system temporarily. The recommended RBAC codes, *B0994 (Manage ad-hoc reports (local))* and *B1700 (Local System Configuration)* do not allow the user to view the clinical record. However, the RBAC code *B0994 (Manage ad-hoc reports (local))* does make it possible at deployment stage for Ardens associates to access some personal identifiable demographic data. RBAC code B0994 allows a list of patients to be viewed in the results. In order to do this, it requires Ardens staff to deliberately click on the 'Patients included' or 'Patients excluded' tabs, which they are trained not to do. The clinical record itself is not accessible with this RBAC access, only basic demographic details of the patients returned in a particular search result. In the normal course of installing or deleting search folders, it is not necessary for Ardens staff to use either of these tabs.

The RBAC code necessary for deployment of reports does not restrict this level of access.

The data visible, if accessed, would consist of a list of patient results within the 'patients included' tab of the search module. This would contain patient number, name, age, sex, usual GP and NHS number. It should be noted that all activity in EMIS is audited.

Small number risk

Some aggregated counts may have small numbers which may make it possible to identify individuals in a cohort. Practices need to be aware of this and make a risk based judgement if uploading aggregate counts with fewer than 10 patients.

Are there any risks to the **Integrity** of personal data? *Integrity is defined as unauthorised or accidental alteration of personal data.*

No

Are there any risks to the **Availability** of personal data? *Availability is defined as unauthorised or accidental loss of access to, or destruction of personal data.*

No

Are there any known or immediate technical / IT / Information Security / Cyber Security concerns?

No

If the answer is "Yes" to any questions in this section, how are these to be reduced or mitigated?

All Ardens deployment staff are aware of this risk and are aware of the parts of the system where this risk exists. There is no need to access these parts of the system for the deployment of the tools, but it is not possible to mitigate this risk further by Ardens. Practices may, if they wish, run audit reports to verify the data accessed by Ardens. All systems access is auditable by the Practices.

Where Ardens staff request authorised access Practice systems, access is strictly controlled and audited through Identity Access Management (IAM) and Role Based Access Control (RBAC). The practice grants and controls access to their EMIS system via the standard EMIS user access controls.

Only authorised personnel, with appropriate security training, can access data held in Practice systems and they may only do so if they have legitimate reason.

Ardens staff complete IG Data Security Awareness training module from e-Learning for Health training as part of their induction, and are required to update annually. Any data access is limited to technical support staff by request only.

Ardens system access terms are detailed in detailed in the Terms and Conditions. https://www.ardens.org.uk/terms/ with assurance provided that such information shall be

treated in confidence.

Once the mitigations are implemented, how would you score any remaining risk in the following Risk Assessment? If you consider that there are no remaining risks give a value of 1 for both Likelihood and Severity.

Likelihood *(please tick)*				**Severity** *(please tick)*				
1		Rare	**x**	**1**		Negligible	**=**	4
2	x	Unlikely		**2**	x	Minor		
3		Possible		**3**		Moderate		
4		Likely		**4**		Major		
5		Almost certain		**5**		Catastrophic		

LIKELIHOOD	IMPACT / CONSEQUENCES				
	NEGLIGIBLE 1	LOW 2	MODERATE 3	SIGNIFICANT 4	EXTREME 5
1 (rare)	**L**	**L**	**M**	**H**	**H**
2 (unlikely)	**L**	**L**	**M**	**H**	**E**
3 (possible)	**L**	**M**	**H**	**E**	**E**
4 (likely)	**M**	**M**	**H**	**E**	**E**
5 (almost certain)	**M**	**H**	**E**	**E**	**E**

Data Protection Risks

List any identified risks to Data Protection and personal information of which the project is currently aware.

Risks should also be included on the project risk register.

Risk Description **(to individuals, to the CCG or to wider compliance)**	**Current Impact**	**Current Likelihood**	**Risk Score (I x L)**	**Proposed Risk solution (Mitigation)**	**Is the risk reduced, transferred, or accepted? Please specify.**	**Evaluation: is the final impact on individuals after implementing each solution a justified, compliant and proportionate response to the aims of the project?**
Possibility of personal demographic information being visible to Ardens support staff when setting up the system	2	2	4	Only authorised personnel, with appropriate security training and legitimate reason can access basic demographic data held in Practice systems through the Practice issuing an RBAC code. All systems access is auditable by the Practices.	Accepted	Yes
Aggregated count data uploaded to the Ardens manager relating to less than 10 individuals could lead to identification.	3	1	3	Practices will be made aware that data relating to less than 10 individuals should be suppressed.	Accepted	Yes

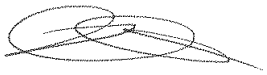
Actions to be taken –

Action to be taken	Date of Completion	Action Owner
Practices must be made aware of the risk that aggregated counts may have small numbers which may make it possible to identify individuals in a cohort. As such, practices should make a risk based judgement if uploading aggregate counts with fewer than 10 patients.	TBC	David Hadley/Comms

Consultation requirements Consultation should be completed by the Project lead, should consultant be required by the ICO the Data Protection Officer will lead.
n/a

DPO Comments and Recommendations	
The tool itself does not process identifiable information, as that is completed within EMIS. The tool is a guide to help GP's enter info into EMIS in a structured manner and any reports coming out are aggregated. The tool does not save the information being entered, or access identifiable information. As identified, there is a risk that some aggregated counts may have small numbers which may make it possible to identify individuals in a cohort. Practices need to be aware of this and make a risk based judgement if uploading aggregate counts with fewer than 10 patients. As such clear information on this risk and the actions that practices should take must be included in communications.	
DPO :	Helen O'Neil
Data and signature:	 4th March 2021

SIGN OFF

SIRO:	Nigel Scott
Date & Signature:	09/03/21 
Caldicott:	Paula Wilkins
Date & Signature:	08/03/21 

Once completed, and signed off, please send this form to: kmccg.kmccg.ig@nhs.net