KAFICO®

INFORMATION · GOVERNANCE · CONSULTANCY

``

Version Control

Date	Notes	Author
2018	Initial Draft	Kafico Ltd

PSL DPIA Data Protection Impact Assessment Summary Conclusion

Data Controllers and Processors

- Clinical Commissioning Groups are Commissioners

``

- Source Providers (Including CCG) are Controllers or Joint Controllers depending on how the project is structured
- PSL are Processors
- Apollo are Sub Processors
- The Bunker are not Data Processors

Lawful Processing

- The information being processed constitutes personal and special categories of personal data
- The data being collected and processed is personal data to be used in connection with public tasks, particularly the delivery of healthcare to individuals (in the first instance)
- Case finding, is compatible with delivery of healthcare and does not require an additional lawful basis
- Risk Stratification purposes are supported by s 251
- NHS Digital mandated data processing is likely legitimised supported by “legal obligation” as a legal gateway

``

- The lawful basis is established by the provider parties as Controllers
- Obligations of secrecy are placed on Prescribing Services as Data Processors
- Processing for direct healthcare is presumed to be necessary due to statutory obligations under HSCA

Data Minimisation

- Where data is able to undergo minimisation – PSL supports Controller customers to achieve this through predefined data sets.
- It is accepted that, there are occasions where use of data cannot always be anticipated and therefore data can be processed 'speculatively'.

Fair and Transparent Processing

- PSL have undertaken appropriate measures to ensure their own transparency but, as Processors, the responsibility is largely with Controller partners that are responsible for collecting the personal data.

KAFICO®

INFORMATION · GOVERNANCE · CONSULTANCY

``

Retention of Personal Data

- Advice and Guidance (Eclipse Live) creates an aggregated pool of data already held by stakeholder parties and PSL is merely processing this data for the purposes of extraction, application of algorithms and display at source.
- In accordance with Schedule 1 and 2 of the Data Processing Contract, PSL will act at the discretion of the Controller to return the data or securely destroy it in line with international standards of destruction.

Information Rights

- Since no new information is created as a result of the project, it seems logical that, where an individual seeks a copy of information held about them, this is provided at source by the Data Controller that is contributing the information.
- In order to ensure that individuals understand what information is being collected and accessed as a result of the project itself, PSL should develop a standard process to provide live information about the various reports and extractions drawn from the data and to whom they have been disclosed. This may include preparing to provide access audits where necessary.

``

- Since no new information is created as a result of the project (barring alerts), it seems logical that, where the data subject identifies an inaccuracy and seeks to have the information rectified, the request is managed by the contributing Controller of the information so that it can be amended at source.
- PSL however, as a recipient of the data, should be prepared to ensure that any rectification of data will be reflected in the presentation of the aggregated information to Controller customers as promptly as possible.
- It is presumed that the Controller is using the identified lawful basis for the project is Public Task and Medical Purposes. Therefore, the right to portability is not applicable to the project.
- It is presumed that the Controller is using the identified lawful basis for the project is Public Task and Medical Purposes. Therefore, the right to erasure is not applicable to the project.
- PSL should draft a protocol for a proactive and comprehensive approach to satisfying the right to object on behalf of Controller customers.

``

- Since the processing does not fully match the definition for profiling and automated decision making, it is presumed that the Controller may proceed with processing without the additional restrictions under Article 22 and ensuring that information rights and transparency requirements are observed.

Accuracy and Data Quality

- PSL will provide evidence to Controller customers of validation / accuracy measures undertaken for the following processing activities; Data Extraction, Data Transfer, Algorithm Application, De-identification, Re-identification, Display / Query.

Technical and Organisational Measures to Protect Personal Data

- The parties have put in place measures to protect data at rest and in transit
- Access to personal data is controlled, authorised and able to be audited.
- Appropriate contracts in place with employees and with third party processors are required by the agreement.

``

- There are measures in place to back up critical assets and to respond in the event of a data breach.
- Incidents shall be responded to in line with data protection legislation and will be monitored.
- Physical locations are protected through staff protocols and professional conduct.
- Reflecting on the nature and scope of the information, it is concluded that PSL have put in place technical and organisational measures such that the risk level is at an acceptable level.

Risk Register

Risk / Gap	Action	Status	Responsible Party
There is a risk that the Controllers will not be subject to appropriate agreements in order to systematically share data with one another	Providers to put in place a peer information sharing agreement to which PSL is not party	Out of scope for PSL action	Healthcare partners (practices / CCGs)

KAFICO®

INFORMATION · GOVERNANCE · CONSULTANCY

``

There is a risk that the Processing Contract in place between PSL and its healthcare providers does not comply with GDPR Article 28 or s 59 DPA 2018	Review current Commitment Agreement and replace with Data Processing Contract	Complete	PSL
There is a risk that sub processors may not be appropriately notified and authorised to Controller customers and therefore to data subjects	Provide confirmation of any sub processors used by PSL and ensure that contracts are compliant with Art 28 and s 59 DPA	Complete	PSL
There is a risk that the appropriate obligations of secrecy are not in place for PSL as a Processor	Check clauses of Processing Contract against Art 28 and DPA s 59	Complete	PSL
There is a risk that the appropriate legal gateways have not been established by the Controllers	Legal gateways to be documented in Controller information sharing documents	Out of Scope for PSL as Processor	Healthcare partners

``

			(practices / CCGs)
There is a risk that the data set being extracted is excessive for the identified purpose	Customer to obtain / undertake clinical review of data set and document rationale	Complete	PSL and Controller customer
There is a risk that changes to the project might result in "data creep" and inclusion of data sets that are not strictly necessary	Requests for additional data sets should be accompanied by a data minimisation rationale for PSL records	Out of Scope for PSL as Processor	PSL to draft form and healthcare partner / customer to complete
There is a risk that data subjects are not informed in relation to the project and are not provided with the opportunity to raise queries or object	Ensure that Advice and Guidance (Eclipse Live) is added to the transparency materials of all Controller stakeholders	Out of Scope for PSL as Processor	Healthcare partners

KAFICO®

INFORMATION · GOVERNANCE · CONSULTANCY

``

			(practices / CCGs)
There is a risk that PSL may not be able to assist Controllers with their transparency obligations	Provide a copy of this DPIA and the detail of any sub processors	Complete	PSL
There is a risk that, PSL may be undertaking "invisible processing" such that data subjects cannot obtain information directly from PSL about their activities	Update Privacy Notice for the website about how PSL processes personal data as a Processor and provide a link to Controller customers	Complete	PSL
There is a risk that PSL are not prepared to respond swiftly and accurately to destroy or return data in the event of exit from the contract	Define the protocol for such an event that includes confirmation of secure destruction or return of the data for evidence and audit purposes	Pending	PSL

KAHICO®

INFORMATION · GOVERNANCE · CONSULTANCY

``

There is a risk that PSL is not adequately prepared to assist Controller customers with their obligations in relation to data subject access	Ensure that there is adequate evidence of extractions and reports provided. Develop standard protocol for obtaining and providing this information as required	Complete	PSL
There is a risk that data subjects are not informed in relation to the project and are not provided with the opportunity to raise queries or object	Ensure that Advice and Guidance (Eclipse Live) is added to the transparency materials of all Controller stakeholders	Out of Scope for PSL as Processor	Healthcare partners (practices / CCGs)
There is a risk that PSL are not prepared to deal with requests for rectification or restriction appropriately	Draft a protocol for such requests and ensure it is communicated to relevant staff	Pending	PSL

KAFICO®

INFORMATION · GOVERNANCE · CONSULTANCY

``

There is a risk that PSL is not adequately prepared to assist Controller customers with their obligations in relation to data subject objections	Develop standard protocol for responding to such requests when they require more granular approach to “opt out” read code management	Complete	PSL
There is a risk that, as the project develops and technology advances, the threshold for the rights around automated decision making and profiling might be met.	Monitor project developments through the PSL governance arrangements and alert existing and potential customers when the threshold is met	Complete	PSL

KAFICO®

INFORMATION · GOVERNANCE · CONSULTANCY

``

There is a risk that PSL do not have suitable data validation protocols in place to ensure effective matching / linkage of data sets	PSL should draft an Accuracy and Data Quality document that identifies that steps are taken for each processing activity that ensure validation and accurate matching / linkage	Pending	PSL
There is a risk that stakeholders will not be subject to appropriate access control	Document Access Control protocol and monitor authorisation of new accounts and de-registration of accounts	Complete	PSL
There is a risk that stakeholders will not be aware of the privacy risks associated with the use of the system	Draft and implement training schedule	Complete	PSL