KAFICO

INFORMATION · GOVERNANCE · CONSULTANCY

Version Control

Date	Notes	Author
July 2020	Initial Draft	Kafico Ltd

Sources

Data Protection Act 2018 (DPA)

General Data Protection Regulations (EU) 2016/679 (GDPR)

Information Commissioner – Guide to the General Data Protection Regulations (ICO Guide)

ICO Guidance - Data Controllers

European Data Protection Board (EDPB) Opinion 00264/10/En Wp 169 (WP29O)

GDPR Lawful Processing - IGA

Control of Patient Information Notice

1. Project Context

During the COVID 19 health crisis, it is recognised that the health service does not have the capacity to respond to thousands of vulnerable or elderly individuals requiring ventilation.
An effective solution is instant identification of those most likely to need hospitalisation, proactive support of these individuals to ensure they are effectively self-isolated and then utilising the large number of self-isolated medical personnel in remotely supporting these vulnerable individuals. This enables effective reduction in the utilisation of ITU beds ensuring that we can manage all patients requiring intensive medical support.

PSL undertook the rapid development of a Covid 19 Clinical Support Tool which is fully integrated with its existing core products to make COVID Protect available to its customer base.

The Data Flows are;

- PSL are instructed by GP practices to add a flag to their current data set that indicates which shielded patients have been contacted by Cabinet Office
- There are also additional risk flags that align with additional risk categories as identified by CMO
- Additionally controllers may provide their own lists of identified vulnerable patients (such as local authority)
- The COVID19 interface within software allows the user to review lists of high-risk patients.
- These can be sent a letter and a booklet including a unique code. The code is entered along with their DOB allowing the patient to access isolation advice and complete questionnaires about their health and their needs whilst in isolation.
- Those accessing the portal are then able to see a view of those patients and whether they have been contacted by cabinet office, contacted by the practice or nominated support organisations and whether they have completed initial questionnaires and (if they have identified C19 symptoms or other concerns) the daily follow up questionnaires.
- Nominated support organisations such as CCGs, Meds Mgnt, healthcare hubs are provided with a list from daily extractions taken by PSL and then are able to access the COVID19 part of NHS Pathways.org. They are only able to see the information necessary to perform their specific tasks i.e. only enough to allow them to contact the patient and support completion of the initial questionnaire and show them how to log on.
- Certain responses to the questionnaire will trigger 'calls to action' such as where a person requires food – this will trigger a call to action for the Council.
- The information is then processed by PSL who will send to the appropriate supporting organisation (as identified by the CCG / GP). PSL obtain permission from the GP practices or CCGs to share information in this way.
- This is done by running a query daily and sending via NHS Net.
- PSL get consent from practice and keep a record

- The CCG may also request permission to share identified data internally with the wider team so they can support with some of the additional functions such as contacting patients.
- The nominated teams are not able to see the wider clinical information, they have the basic information required to contact the patient and can see a copy of the questionnaire itself.

2. Controllers and Processors

This DPIA Addendum extends the existing DPIA for core PSL Services and Products. The original DPIA identifies the Data Controllers and Processors as follows;

- GPs and other healthcare providers are individual Data Controllers
- CCG are Data Controllers
- PSL are Processors
- Apollo are Sub Processors

The COVID Protect service potentially creates additional relationships as below.

- GPs and other healthcare providers may engage the CCG to undertake activities around contacting patients which would make them a Processor on behalf of the GP or healthcare provider as Controller
- GPs and other healthcare providers may engage GP Support Organisations or Federations to undertake triage or delivery of clinical support to patients identified by COVID Protect. This would likely be a peer to peer Controller relationship

Both of these new relationships are outside of scope for PSL (as processor) but it is anticipated that Controllers will put in place the appropriate contracts / sharing agreements in order to legitimise this additional data sharing.

3. Lawful Processing

This DPIA Addendum extends the existing DPIA for core PSL Services and Products. The original DPIA confirms the following with respect to the lawful processing of personal data;

- 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

PSL recognises that the lawful basis for processing will be determined by the customer as Controller, however, it is likely that the lawful basis will remain the same for COVID Protect as it is for the PSL the core products and services (namely, public task and direct care).

The COVID Protect Service also takes account of an additional lawful basis; Notice under Regulation 3(4) of the Health Service Control of Patient Information Regulations 2002 (COPI Notice)1. The COPI notice requires healthcare providers to process confidential patient information for purposes set out in Regulation 3(1).

1 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/874509/Coronavirus__COVID-19___notice_under_regulation_3_4__of_the_Health_Service_Control_of_Patient_Information_Regulations_2002.pdf

The COPI purposes that would be relevant to the use of the COVID Protect services are assessed to be;

- Understanding Covid-19 and risks to public health, trends in Covid-19 and such risks, and controlling and preventing the spread of Covid-19 and such risks

COVID Protect allows for identification of at-risk patients and supports remote delivery of healthcare and therefore supports to control and prevent the spread of COVID-19.

- Identifying and understanding information about patients or potential patients with or at risk of Covid-19, information about incidents of patient exposure to Covid-19 and the management of patients with or at risk of Covid-19 including: locating, contacting, screening, flagging and monitoring such patients and collecting information about and providing services in relation to testing, diagnosis, self-isolation, fitness to work, treatment, medical and social interventions and recovery from Covid-19

COVID Protect allows for identification of at-risk patients and provides them with a questionnaire such that they can be screened, flagged and monitored. This includes the monitoring of tests, diagnosis and self-isolation.

- Understanding information about patient access to health services and adult social care services and the need for wider care of patients and vulnerable groups as a direct or indirect result of Covid-19 and the availability and capacity of those services or that care

COVID Protect allows for identification of at-risk patients and provides them with a questionnaire such that they can be screened, flagged and monitored. This includes identifying access to care services and can also flag a call to action for clinical or social intervention.

- Delivering services to patients, clinicians, the health services and adult social care services workforce and the public about and in connection with Covid-19, including the provision of information, fit notes and the provision of health care and adult social care services.

COVID Protect allows for identification of at-risk patients and provides them with a questionnaire such that they can be screened, flagged and monitored. This includes identifying access to care services and can also flag a call to action for clinical or social intervention.

Opt Outs

It is determined that the National Data Opt Out (and in fact other objections set at practice level) do not apply to disclosures made under the COPI Notice. This is because there is an overriding public interest in the disclosure, since the public interest in disclosing the data overrides the public interest in maintaining confidentiality.

Whilst patients may still exercise their right to object to particular interventions or treatment and the inherent information sharing involved, it is determined that, in order to satisfy the COPI requirement to monitor and control infection, the objections that patients have raised with respect to their information being shared outside of the GP practice should and can be overridden.

4. Data Minimisation

This DPIA Addendum extends the existing DPIA for core PSL Services and Products which confirms the following with respect to data minimisation;

- The data set used for Care Records projects is agreed by the relevant stakeholder groups as Controllers and therefore PSL are assured that the data is the minimum necessary for the identified lawful purpose.
- This has been confirmed through clinical assessment as the minimum necessary data set to achieve the intended purposes for the initiative. This is reviewed periodically with the customer to ensure that it remains adequate.

The COVID Protect project involves integrating some of the data sets collected for the core products (Advice and Guidance, VISTA) being repurposed to support the COVID Protect purposes (see Core Product DPIA).

It is suggested that this additional purpose is compatible with the original purpose of collection in accordance. GDPR Recital 50 provides that "If the [further or additional] 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, Union or Member State law may determine and specify the tasks and purposes for which the further processing should be regarded as compatible and lawful". It is clear that the COPI purposes provide a directive that information held by provider may and should be shared to satisfy the identified COPI purposes.

Additionally, new data fields are collected for COVID Protect and justification for the use of each of these data fields is provided below;

Title	Collection Source	Use / rationale
First Name	Provided to PSL via GP Patient List.	Allows identification of the data subject and linkage with them within the source systems of health and social care providers
Last name	Provided to PSL via GP Patient List.	Allows identification of the data subject and linkage with them within the source systems of health and social care providers
Address	Provided to PSL via GP Patient List.	Allows identification of the data subject and linkage with them within the source systems of health and social care providers. Also allows for allocation of support such as medication delivery.
DOB	Provided to PSL via GP Patient List.	Allows identification of the data subject and linkage with them within the source systems of health and social care providers. Also allows to particular categorisation with regards to risk i.e. shielding patients of a certain age.
NHS Number	Provided to PSL via GP Patient List.	Legally required as a patient identifier
Telephone	Provided to PSL via GP Patient List.	Allows contact to be made with the individual as requested below.

Mobile	Provided to PSL via GP Patient List.	Allows contact to be made with the individual as requested below.
Government Shielding Status	Provided to PSL via NHSD derived Files.	Allows supporting organisations to adapt the support provided based on particular circumstances.
Questions about COVID symptoms (cough, fever, sense or smell / taste,	Provided to PSL by data subject (patient) having logged into COVID Protect patient portal	Allows flagging of patients that are experiencing known potential COVID19 symptoms such that they can be monitored, supported and treatment provided.
Do you have support available for food or medicines delivery?	Provided to PSL by data subject (patient) having logged into COVID Protect patient portal	Allows flagging of patients that require immediate support to maintain wellbeing.
Food for next 3 days	Provided to PSL by data subject (patient) having logged into COVID Protect patient portal	Allows flagging of patients that require immediate support to maintain wellbeing.
Medicines for next few days	Provided to PSL by data subject (patient) having logged into COVID Protect patient portal	Allows flagging of patients that require immediate support to maintain wellbeing.
Would you like help	Provided to PSL by data subject (patient) having	Allows flagging of patients that require assistance from the council to maintain wellbeing.

from council?	logged into COVID Protect patient portal	
Do you want your GP to contact you?	Provided to PSL by data subject (patient) having logged into COVID Protect patient portal	Allows flagging of patients that require support from their GP to maintain wellbeing.
Do you want contact about non-medical needs from council?	Provided to PSL by data subject (patient) having logged into COVID Protect patient portal	Allows flagging of patients that require assistance from the council to maintain wellbeing.
Do you want regular contact?	Provided to PSL by data subject (patient) having logged into COVID Protect patient portal	Allows flagging of patients that require ongoing contact from the wider health and social care team to maintain wellbeing.
Contact by email or phone? Enter details	Provided to PSL by data subject (patient) having logged into COVID Protect patient portal	Confirms communication preferences in line with NICE guidelines
Free text notes	Provided to PSL by data subject (patient) having logged into COVID Protect patient portal	Allows individual to provide any additional information they feel is relevant.

5. Fair and Transparent

KAFICO

INFORMATION · GOVERNANCE · CONSULTANCY

This DPIA Addendum extends the existing DPIA for core PSL Services and Products. The original DPIA confirms the following position with respect to fairness and transparency.

"Whilst consent is not the recommended lawful basis for processing of healthcare data and the legal gateway under data protection law is likely to be "public task" and "medical purposes", there is a still a legal requirement to ensure that the patient population are informed about the processing and have the opportunity to ask questions or to object to processing. Additionally, there is a need to ensure that the common law duty of confidentiality is also satisfied.

The duty can be overridden where it is deemed that the individual reasonably expects such a disclosure.

It is therefore presumed that fair processing / transparency materials will be put in place by Controllers to make the patient population are aware of the COVID Protect services and to ensure that the "reasonable expectations" of the population align with that of the project.

It is anticipated that Controllers will have already had existing materials that provided patients with information about when their information might be shared because the law compels it – such as for safeguarding, court orders and infectious diseases."

The position of the core product DPIA around transparency is not altered by the introduction of the COVID Protect service however, PSL has not previously had a direct relationship with data subjects. The introduction of the patient portal makes it necessary for PSL to provide transparency information to data subjects about how their information will be collected and shared.

PSL have added the following statement to the patient portal for COVID Protect;

- Please be aware that the personal and sensitive data you enter into the portal will be collected will be shared with your local health and care providers.
- Certain symptoms you enter may send an alert to your local Clinical Commissioning Group who will share your information with local healthcare providers that can offer you support.
- If you tell us about any social care needs, requests will be sent to the local council who can offer you support.

- Relevant health and social care information will be added to your health records by your health and care providers.
- Your local healthcare providers have contracted Prescribing Services Ltd to provide this patient portal. You can find out more about us, including our privacy policy ***here***.
- For more information about your rights, including the right to object, please visit your local Clinical Commissioning Group website and search for 'COVID Protect'.

Commissioning organisations have been provided with the following information;

"Please see the privacy addition we have added to the COVID Protect patient portal. As you can see, it refers the patient to the CCG website to read a full privacy notice for the project. You may wish to ensure that patients searching the term "COVID Protect" are provided with necessary privacy information. If we can help at all, let us know"

The intention here is to support the Controller customers as much as possible with their obligations around transparency and the right to be informed. Data subjects are directed to the commissioner website which will provide them with information about their information rights.

6. Retention of Records

This DPIA Addendum extends the existing DPIA for core PSL Services and Products. The original DPIA confirms the below position with respect to retention of records.

"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."

The COVID Protect project does involve a deviation from the core product DPIA on this matter for two reasons.

1. PSL are now collecting new information, entered by the patient or by the providers in relation to COVID status and actions taken
2. Destruction / return of data collected and disclosed for COVID purposes in line with the COPI directive, has an intended end date of September 2020. Meaning that there must be a plan to cease such activity and to return or destroy the data at this time.

To that end, the following separation of concerns is in place;

- PSL have a specific process for importing the personal data for COPI processes. This is just a single file for each practice provider which PSL refer to as the 'COVID import'. This is separate from core processes and will be disabled when the COPI order ends.
- The data extracted by this report is uploaded to the HSCN server, imported and the source file is deleted. The data is imported into specific tables only available from the HSCN network. These tables will be truncated and deleted when COPI ends.

7. Information Rights

This DPIA Addendum extends the existing DPIA for core PSL Services and Products. The original DPIA confirms the below position with respect to information rights

Information Rights are supported by PSL as described below and the text in bold are additions to the core assessment brought about by COVID Protect.

Right to Access	Data subjects have the right to access their personal data and the right helps individuals to understand how and why you are using their data, and check you are doing it lawfully. End users can view, add notes to an alert, or an action plan connected to a priority patient. All this activity is retained within the system and can be retrieved for the purposes of providing copies to data subjects. The system provides an audit trail of extractions and reports such that these can also form part of a subject access request response as well.

	Patients can make a request for any personal data collected by PSL through the COVID Protect project. Disclosures will be made in collaboration with the Controller customer.
Right to Rectification / Restriction	Data subjects have the right to request that inaccurate information is corrected. Since patients largely do not have a direct relationship with PSL and PSL would be unable to identify a particular individual, it is anticipated that these rights would be actioned by the healthcare provider at source. Where an Eclipse user identifies an inaccuracy at source, and adds a read code or alters basic demographics, this will automatically be included in the Eclipse data extraction. For example, the GP adds a new allergy to the record because the patient has flagged it. The next extraction performed by Eclipse will include that information and this will be available to other users. For COVID Protect, patients will now have a direct interface to PSL. A revised / new questionnaire overrides previous questionnaire. This enables patient to correct / update any answers given
Right to Erasure	Where, the lawful basis is public task and medical purposes, the right to have request that personal data is erased is not available to data subjects.
Right to Portability	Where, the lawful basis is public task and medical purposes, the right to portability of personal data is not available to data subjects.
Right to Object	Advice and Guidance (Eclipse Live) will create an aggregated version of data, pulled from the Controller systems and stored by Prescribing Services and then presented to the Controller customer at source. Currently, where a patient has already "opted out" of their information being processed beyond their GP practice, these are excluded through automatic recognition of the related "opt out" read codes. If the patient has an opt out read code assigned to them and they don't have a more recent opt in code their data isn't taken either by the manual extracts or Apollo's automatic extracts. Sensitive codes are also removed at source and Prescribing Services undertake an additional check on arrival, deleting any data that may have been extracted inappropriately. Where the data subject identifies an objection to their data being processed as part of the Advice and Guidance (Eclipse Live) project after the fact, and

	seeks to have the information excluded, Controllers are required to consider this in a timely and consistent manner. Controllers are presumed to have a documented process for considering whether there are legitimate reasons to not give effect to such rights on a case by case basis. It is likely that this will result in an alteration to the read code at source but, if the patient only objects to Advice and Guidance (Eclipse Live) in isolation, this may be a more manual process and will be led by the Controller customer.

8. Accuracy and Data Quality

This DPIA Addendum extends the existing DPIA for core PSL Services and Products. The original DPIA confirms the following position with respect to accuracy and data quality.

Data Extraction

PSL have devised an algorithm that identifies when the extracted data set falls outside of expected parameters. Irregularities are highlighted through the presence of unexpected elements i.e. the size of the data set, number of data lines, number of drugs, blood pressure readings. Where the data has characteristics which could be deemed as outliers, the extraction would not be accepted by the system and this would trigger manually scrutiny.

Data Transfer

The extracted data is encrypted for transit, in order for the data set to effectively 'land', it must decrypt which means that it must be complete. It will only allow decryption and therefore accept the file if the file is complete. The systems have interoperability so rather than show corrupt data, the system will reject it.

Algorithm Application

The algorithm is programmed to create alerts when a combination of particular data points are in existence. For example a patient who is on combination of certain medicines known to react with one another might trigger an alert for a medication review.

The algorithm is programmed using NHS England guidance and is subject to a quarterly clinical review within PSL to ensure that the data upon which the alerts are based remains accurate and best practice. The clinical team within PSL will also undertake periodic audits of alert numbers and other outliers to identify anomalies – for example, a sudden spike in the number of alerts being issued would trigger a closer look at the data being produced.

Additionally, there is a feedback button available to all end users of the system. This allows users of the system to identify where there might be gaps in the information or perhaps an alert has been inappropriately generated. So, PSL are in receipt of around 10,000 reviews supporting the ongoing development of the service.

Re-identification

The system involves a brand-new build of the integrated data sets each week. Each build requires the extraction of the data, the replacement of the identifier with the Eclipse integer.

This means that there is low risk of a mismatch between the identifying data (NHS No, Patient Name) and the other extracted items (read codes) when they are pulled back together to facilitate the identification of a particular patient.

There have been no mismatches of this data since the system inception in 2011. The only example where a mismatch between the extracted data and the patient identity would be possible is where the wrong NHS No has been attributed to the patient within the source data and this is outside the scope of control for PSL.

The following additional elements are relevant for the COVID Protect project;

1. There is a risk that, if a practice does not maintain regular extractions, the risk flags added will not be visible to the Clinical Users. The onus is on the Controller customer to ensure that regular extractions are undertaken to mitigate this risk.
2. The introduction of a new algorithm – identification of priority group patients for COVID 19 – requires validation to remain accurate. The data is being regularly reviewed to ensure it reflects both government advice or the steer of the particular commissioner in respect to their patient population's needs.

3. Patients understanding and communication needs may vary and so the quality of patient entered data may fluctuate. PSL have enabled additional processes whereby the patient can be contacted directly by a call handler and supported with the questionnaire. PSL transfer the COVID code to the call handler and there is an expectation that validation of the contents of the questionnaire will be undertaken by those making the call or responding to calls to action.
4. There is a need to ensure that calls to action sent to the various support organisations are of good quality and appropriate. PSL are attending Operational Governance Meetings twice a week with all key stakeholders present. Feedback around quality of alerts and any significant events is provided including feedback from patients allowing data quality to be actively monitored.

9. Technical and Organisational Measures to Protect Personal Data

As a Processor, PSL are required to assurance that their technical and organisational measures that are comparable to those implemented by the Controller and proportionate to the risk.

Unlike the Controller customer, PSL is not in a position to assess the risk to the rights and freedoms of particular data subjects since they are not in control of the purpose and manner of processing.

However, due to the nature and scope of processing, it seems a reasonable to assume that implementing PSL products and services represents at least a moderate to high degree of risk to the rights and freedoms of data subjects in the event that appropriate technical and organisational measures are not put in place at all.

This assessment will therefore explore each of the elements drawn out within data protection legislation and guidelines for mitigation of those risks.

Security of Data Hosting

The data centres holding the bulk of the extraction data (NHS Number removed and replaced with integer – Eclipse No) are hosted by The Bunker. Their secure hosting solutions are based in

an ex-nuclear bunker in Kent, UK. They have achieved ISO27001, have completed their NHS Data Protection and Security Toolkit and are G-Cloud Accredited. The Bunker are contracted by virtue of an Article 28 compliant Processing Contract.

Using providers with accreditations demonstrates that there are evidenced technical and organisation measures in place commensurate to the level of risk posed by the information in question.

The identifiers that have been removed (Eclipse No, Encrypted NHS No, Encrypted Name, Encrypted Address, Encrypted DOB) are stored at the Queen Elizabeth Hospital Kings Lynn (QEHKL) server which is based on the Health and Social Care Network (HSCN) and only set up for access by the PSL Server which is also on HSCN.

By using servers on the HSCN, PSL have demonstrated that they have engaged with approved mechanisms for network protection. The HSCN will soon include NHS Secure Boundary, a security solution which offers protection against the most sophisticated network security threats for NHS organisations.

PSL uses multiple high-specification servers are used to create a virtualised cluster running SQL Server 2012 allowing load balancing and failover. Load balancing arrangements mean that the personal data is better able to withstand the high volume of requests used in many Denial of Service attacks2

Physical Premises Security

All Organisation servers are hosted within industry standard data centres that conform to industry best practices and standards for security as defined in the relevant contract terms and conditions.

Entry to the head office building is via a shared door access through which is controlled by a keypad and code. The door is also locked outside of normal working hours and entry to the building is not possible via the keypad alone. The company's office is then accessed by another

2 https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-44ver2.pdf

door which is also controlled by a keypad and code and locked outside of working hours. All visitors are required to sign in and out and be accompanied at all times whilst within the office premises. Filing cabinets are locked when applicable outside of normal working hours.

The office servers and communications hardware are located in a server room which is kept locked.

The offices include all firefighting equipment required under current regulations. These are provided and maintained under the terms of the office occupancy contract. Smoke detectors are present throughout the building.

Continuity and Availability

PSL uses multiple high-specification servers are used to create a virtualised cluster running SQL Server 2012 allowing load balancing and failover. Separate servers are used for web server requests, back-ups and monitoring.

Backups of Advice and Guidance (Eclipse Live) data are conducted, maintained, and tested periodically. Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) for Advice and Guidance (Eclipse Live) are in place and managed

Authentication of Users

For the customer user interface, there is a 2-factor authentication process is currently in operation. Users are required to log on using a username and strong password combined with a second layer of authentication, which sends a single-use time-limited access code to the user's personal mobile phone or email address. This aligns with Level 2 authentication standards described in NIST guidelines3 and is therefore considered to provide "high confidence" that the user accessing the system is the authorised individual.

Access privileges are delegated according user role as demonstrated below;

3 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf

KAFICO

INFORMATION · GOVERNANCE · CONSULTANCY

Role	System	Privilege	Access to Patient Data?	Internal / External
Internal Administrator	All	• Add and remove users • Audit • System and contained data for internal systems (QEHKL black box for patient identifiable information)	Yes	Internal
Internal Support	All	• Add and remove customer users • Support with patient extractions	No	Internal
Internal Development	All	• System and contained data for internal systems (QEHKL black box)	Yes	Internal
Clinical Assurance Lead	All	• System and contained data for internal systems (QEHKL black box)	Yes	Internal
Clinical Administrator	Advice and Guidance Eclipse Live Platform and Integrated Module	• Request and authorise users and removals • Audit access	Yes	External
Clinical User	Advice and Guidance Eclipse Live Platform and Integrated Module	• Access identified patient data (within HSCN environment) • Audit access	Yes	External
Virtual Clinical Hub / Specialist Clinical User / Ambulance	Advice and Guidance Eclipse Live Platform and Integrated Module	• Access identified patient data (within HSCN environment)	Yes	External

CCG Call Handler	Advice and Guidance Eclipse Live Platform and Integrated Module	• Access **restricted / limited** identified patient data (within HSCN environment)	Yes	External
CCG Population Health User	Advice and Guidance Eclipse Live Platform and Integrated Module	• Access to de-identified patient data • Audit	Yes	External
Patient Access User	COVID Protect Questionnaire	• Able to enter personal and special category data and transmit to Controller user	Provide only	External

In addition to the usual access for extracted data sets, patients are now able to directly enter their personal and sensitive personal data by way of the COVID Protect patient portal.

Before patients can access the questionnaire to complete, they are required to enter a combination of their data of birth and the code that has been sent to them by their GP practice or nominated support organisation. This will have been sent on the basis of the Controller customer reviewing a list of high-risk patients within COVID Protect.

It is therefore concluded that, beyond the inherent risk of the letter with the code being intercepted by a third party, the Controller can be reasonably confident that the person completing the questionnaire is the individual concerned.

Where the code has been intercepted and a person is able to access the questionnaire, rather than access and gain any personal data about the intended individual, they are required to *provide* information. This information will be used to trigger direct contact from health or social care providers who will use their usual protocols to validate identity and content of questionnaire before, for example, medication is dispatched.

Access Control

During the onboarding process, PSL are notified by the practice of 2 to 3 users that require access permissions for the system as well as the appropriate CCG Clinical Team Users.

Users are not added or removed without the express permission of the nominated authoriser within the customer and the defined access levels will be identified by that authoriser. As a Processor, PSL are not in a position to make determinations about how appropriate the access provided might be and will simply act on the instructions of the nominated authoriser.

The Clinical Administrator role held by practice customers allows the user to audit access of the authorised users within their organisaton.

The CCG Population Health role held by the CCG allows the user to audit access of the authorised users within their organisation.

With PSL, the Internal Administrator role allows the user to audit access of the authorised users within PSL.

The COVID Protect Project widens the scope of potential users for the PSL products and service to those within support organisations, local authorities and identified data being disclosed to the CCG. As a processor, the CCG are very much dependant on the practice to identify the nominated recipients of the access and any particular data sets.

Pseudonymisation and Encryption of Personal Data in Transit and at Rest

Advice and Guidance (Eclipse Live) employs pseudonymisation to protect data both in transit and at rest. This is demonstrated at Appendix A.

Recital 26, the GDPR limits the ability of a data handler to benefit from pseudonymized data if re-identification techniques are “reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly.”

To determine how effectively the linked data has been pseudonymised (and therefore further minimised where a large and somewhat speculative data set exists), it is necessary to consider how “reasonably likely” it is that the Controller (or Processor) or another person could directly or indirectly identify a person.

Practice data set extracted manually or by Apollo

- Demographics
- age (years)
- gender
- clinical system no
- Coded event data
- Clinical sys no
- Read Code (Value 1 value 2)
- Medication data
- medication name
- medication read codes
- Date issued
- status (repeat etc)
- Instructions - free text)

The data is 256-bit encrypted which is regarded as requiring significant cost, time and effort in order to decrypt without the necessary key.

Policy, Training and Confidentiality

PSL staff are provided with the following Information Governance Policies and Protocols;

- Information Governance Policy
- Information security and Cyber Security Protocol
- Freedom of Information Protocol
- Information Rights Protocol
- Information Lifecycle and Data Quality Protocol
- DPIA Protocol
- Information Risk and Audit Protocol
- Information Sharing and Privacy
- Information Incident Protocol

They are provided with annual training on data protection and security and have a contract that binds them to confidentiality.

PSL have nominated a qualified and experienced Data Protection Officer.

10. Risk Management

KAFICO

INFORMATION · GOVERNANCE · CONSULTANCY

KAFICO

INFORMATION · GOVERNANCE · CONSULTANCY

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	Inherent Likelihood of harm	Inherent Severity of harm	Inherent Overall risk	Options to reduce or eliminate risk	Effect on risk	Residual risk	Measure approved
There is a risk that the Controller and Processor relationship has not been sufficiently defined and documented. This may result in ineffective management of risk and could result in improper management of data subjects' personal data.	Moderate	Moderate	Moderate	PSL confirmed as Data Processor and contracted to act on instructions from Controller	Eliminated	Low	DPO approved Jul 2020
There is a risk that the Processor is not engaged by virtue of an Art 28 compliant processing contract. This could result in the Processor managing data subjects' personal data improperly.	Moderate	Moderate	Moderate	PSL are engaged by virtue of an Art 28 compliant processing contract Customer required to put in place sharing agreements between Controllers	Eliminated	Low	DPO approved Jul 2020
There is a risk that the Controller's obligations under Art 9 (2) (h) para 3 are compromised by not having in place appropriate 'obligations of secrecy' for the Processor. This could result in data subjects' personal data being disclosed inappropriately.	Moderate	Moderate	Moderate	PSL are engaged by virtue of an Art 28 compliant processing contract They are provided with annual training on data protection and security and have a contract that binds them to confidentiality.	Eliminated	Low	DPO approved 2020

KAFICO

INFORMATION · GOVERNANCE · CONSULTANCY

There is a risk that, whilst data protection is satisfied, the common law duty of confidentiality is breached. This could result in damage and distress being caused to data subjects where they had not reasonably expected a use of their private information.	Moderate	High	High	PSL have added a transparency statement to the patient portal for COVID Protect. It is ultimately the Controller responsibility to ensure that the patient population expectations are managed with respect to the processors they engage and the purpose and manner of processing.	Out of Scope for PSL	Out of Scope for PSL	Out of Scope for PSL
There is a risk that data has not been effectively minimised, and this would result in a greater risk, in the event of a breach, to the rights and freedoms of data subjects.	Moderate	Low	Moderate	Justification for each data field has been provided within the impact assessment	Eliminated	Low	DPO approved 2020
There is a risk that article 12 has not been satisfied and data subjects are not effectively informed about processing, including any processors or sharing partners involved and in particular in relation to their right to object. This may result in data subjects losing trust and having their data processed in a way they would not reasonably expect – opening the Controllers to a claim under the Tort of Misuse of Private Information.	Moderate	Low	Moderate	PSL have added a transparency statement to the patient portal for COVID Protect. It is ultimately the Controller responsibility to ensure that the patient population expectations are managed with respect to the processors they engage and the purpose and manner of processing.	Out of Scope for PSL	Out of Scope for PSL	Out of Scope for PSL

There is a risk that records are retained for longer then their intended purpose. This could result in greater risk of a breach and impact to a greater number of data subjects in the event of such a breach.	Moderate	Low	Moderate	PSL have a specific process for importing the personal data for COPI processes. The data is imported into specific tables only available from the HSCN network. These tables will be truncated and deleted when COPI ends.	Eliminated	Low	DPO approved 2020
There is a risk that PSL are not prepared to support Controller customers with giving effect to data subjects' information rights. This could result in a breach of data protection law and potentially cause damage and distress to data subjects who may feel a loss of control over their personal data/	Moderate	Moderate	Moderate	PSL are prepared to respond to any information rights requests from data subjects and have a protocol in place. Staff are aware that such rights must be dealt with by referring to Controller customer and providing assistance.	Eliminated	Low	DPO approved 2020
There is a risk that data will be inaccurate or of poor quality. This could result in inappropriate flagging of risks against a patient and could impact on the care they receive.	Moderate	High	High	PSL has implemented a number of steps to ensure the quality and accuracy of data including a continual cycle of user feedback.	Reduced	Low	DPO approved 2020
There is a risk that an individual gains entry to the databases by exploiting a vulnerability in the operating system	Mod	Mod	Mod	Regular security patching is carried out by PSL so that the infrastructure remains active and supported Penetration testing is routinely performed by PSL to identify vulnerabilities and apply mitigations	Reduced	Low	DPO approved 2020

There is a risk that a rogue employee within PSL gains access to the databases.	Mod	Mod	Mod	Staff undergo pre employment screening Granted access is limited to who with a business need at the appropriate level All servers are monitored and alerts generated through all suspicious activity.	Reduced	Low	DPO approved 2020
There is a risk that access to the databases is gained through force	Mod	Mod	Mod	Access to the database is protected using secure VPN connections using 2 factor authentications (this uses a user known 4 digit pin and a generated 8 digit code) Data rests in encrypted form and so would require decryption upon access PSL have applications on the server which perform encryption a motivated intruder would need to obtain the decryption key within the app The encryption is EAS 256 bit requiring considerable time and effort to force	Reduced	Low	DPO approved 2020
There is a risk that access to the databases is gained through access to known credentials and security code generator	Mod	Mod	Mod	Data rests in encrypted form and so would require decryption upon access PSL have applications on the server which perform encryption a motivated intruder would need to obtain the decryption key within the app The encryption is EAS 256 bit requiring considerable time and effort to force	Reduced	Low	DPO approved 2020

There is a risk of inappropriate access by or too much access being provided to users of the system	Mod	Mod	Mod	The Clinical Administrator role held by practice customers allows the user to audit access of the authorised users within their organisation. The CCG Population Health role held by the CCG allows the user to audit access of the authorised users within their organisation. With PSL, the Internal Administrator role allows the user to audit access of the authorised users within PSL. Role based access is in place and the customer is able to determine what level of access is provided to their employees	Reduced	Low	DPO approved 2020

11. Sign Off

Item	Name / Position / Date	Notes
Measures approved by:	Emma Cooper, Kafico Ltd, July 2020	It is concluded that PSL have in place appropriate technical and organisational measures to protect personal data and, in so far as they are able as Processor, PSL have identified no reisual risks that would be considered high and require escalation to the ICO.
Residual risks approved by:	Emma Cooper, Kafico Ltd, July 2020	

KAFICO

INFORMATION · GOVERNANCE · CONSULTANCY

Data Protection Advice provided:	Emma Cooper, Kafico Ltd, April 2020	PSL DPIA is to identify measures in place predominantly. The Controller customer is ultimately responsible for determining the risks to the rights and freedoms of their patient population in line with their organizational risk profile and appetite.
Periodic DPIA review dates:	Emma Cooper, Kafico Ltd, July 2020	October 2020 Review Due