Prescribing Services

PRIME

Data Protection by Design

VERSION DATE	NOTES	AUTHOR
2021-03-24	Redraft. Previous versions available at PSL DPIA	Emma Cooper, Kafico Ltd

KAFICO

INFORMATION · GOVERNANCE · CONSULTANCY

1. PROJECT CONTEXT

During the COVID 19 health crisis, it was recognised that the health service did 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.

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. This involve providing a patient engagement portal, providing the ablity for patients to complete questionnaires and have their welfare monitored by a multi agency team.

As a result of a very succesful programme, it was identified that the ability to engage with patients in this way would be useful for other key patient cohorts and so the project developed from COVID Protect to PRIME.

As COVID Protect was covered by the COPI Notices[1], it is the intention of this DPIA to demonstrate how the use of the service beyond the pandemic may be legitimised within the post-pandemic data protection landscape.

2. DATA FLOWS

1. PSL are instructed by the Data Controllers to add a flag to their current data set that identifies a particular cohort of patients (for example those requiring cervical screening)
2. The practice must therefore approve and enable an identified list of patients to be extracted from the clinical system into the PSL environment.
3. The patient list extracted will include name, address, contact details and NHS Number

[1] https://digital.nhs.uk/coronavirus/coronavirus-covid-19-response-information-governance-hub/control-of-patient-information-copi-notice

4. The PRIME interface within software allows the user to review lists of high-risk patients.
5. 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 advice and complete questionnaires about their health and their needs.
6. Those accessing the portal are then able to see a view of those patients and whether they have performed the identified actions.
7. Nominated support organisations such as CCGs Medicines Management, Healthcare Hubs, Community Providers are provided with a list from daily extractions taken by PSL and then are able to access the PRIME part of NHS Pathways.org.
8. 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 questionnaires and show them how to log on.

Risk Assessment

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)

Information Commissioner - Data Protection Impact Assessments

KAFICO

INFORMATION · GOVERNANCE · CONSULTANCY

1. INTRODUCTION

The UK Information Commissioner and the European Data Protection Board provide that Data Protection Impact Assessments are necessary, in certain circumstances, to assess the level of risk to the rights and freedoms of individuals.

Controllers must consider both the likelihood and the severity of any impact on individuals. High risk could result from either a high probability of some harm, or a lower possibility of serious harm.

The risk assessment serves to support Controller customers to identify the level of inherent risk so that the measures being put in place to mitigate the risk are proportionate to the impact that projects or initiatives might have on data subjects.

2. ACCOUNTABILITY

Prescribing Services Ltd (PSL) are a Processor and are therefore required to provide assurance that their technical and organisational measures that are comparable to those implemented by the Controller and proportionate to the risk.

Unlike the Controller, they are not in a position to assess the risk to the rights and freedoms of particular data subjects since they are not in control of establishing the lawful basis or a direct route for giving effect to data subject rights. However, due to the nature and scope of processing, it seems reasonable to assume that implementing the described project 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 for mitigation of those risks.

3. ASSET CRITICALITY SCORING GRID

Typically, critical national services. Absence of system leads to complete failure of dependent systems and services with a high possibility of personal safety issues. Service interruption results in severe reputational damage	5
Predominantly transactional services. Absence leads to operational difficulties that can be coped with for a limited period. May lead to increased risk to stakeholders or organisation.	4
Predominantly data capture, batch processing. Absence leads to operational difficulties, but these are manageable for an extended 2period. Eg. 1 day. Absence of system may lead to a slight increase in risk to stakeholders or organisation.	3
Business Hours Support (8am-6pm) Mon-Fri (not BH). Service Availability 98%. DR optional - dependant on outcome of BIA.	2

4. DATA RISK SCORING GRID

Data is aggregated and anonymised.	2
Low volume of personal data involved or high volumes of anonymised data.	3
High-volume personal data or low volume special category data.	4
High volume and special category data or includes stigmatised information (i.e. mental health data).	5

5. RISK SCORING MATRIX

		Asset Criticality			
Impact of data breach		2	3	4	5
	2	Bronze			
	3		Silver		
	4			Gold	
	5				Platinum

6. ASSESSMENT AND RATIONALE

What score has the project been given in terms of criticality of resulting asset or service?	Predominantly transactional services. Absence leads to operational difficulties that can be coped with for a limited period. May lead to increased risk to clinical care.
Rationale	Whilst the systems and services provided by PSL are ordinarily supplementary to core clinical services, they are increasingly being used to identify cohorts of patients who require specific interventions in relation to cancer pathways, for example, or as a result of the pandemic. To reflect that, this assessment has heightened the potential critically based on the fact that some customers may rely more on the services that others. By assessing the service in this way, it allows the design and underlying

	compliance to reflect a potential future state whereby PSL services are fundamental to supporting core health and care services.
What score has the project been given in terms of the nature and volume of data being processed?	High volume and special category data and includes stigmatised information.
Rationale	PSL are supporting many GPs and CCG across the country which results in thousands of patients' data being extracted on a daily basis. This includes read coded, identified personal data that this includes health information - including stigmatised information.
Overall risk score given to the processing activity / project in question.	GOLD
Does the project involve introduction of a cloud service to be assessed?	Introduces cloud services that will need to be assessed

6. RISK ASSESSMENT CONCLUSION

The project has been assessed to have an overall risk score of GOLD and so the measures to be applied will be proportionate to reduce the inherent risk levels to a suitable level such that they can be accepted by the Controller.

Controllers and Processors

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

KAFICO

INFORMATION · GOVERNANCE · CONSULTANCY

1. DEFINITIONS / CONTEXT

“It is essential for organisations involved in the processing of personal data to be able to determine whether they are acting as a data controller or as a data processor in respect of the processing. This is particularly important in situations such as a data breach where it will be necessary to determine which organisation has data protection responsibility.

The data controller must exercise overall control over the purpose for which, and the manner in which, personal data are processed. However, in reality a data processor can itself

exercise some control over the manner of processing – e.g. over the technical aspects of how a particular service is delivered.

The fact that one organisation provides a service to another organisation does not necessarily mean that it is acting as a data processor. It could be a data controller in its own right, depending on the degree of control it exercises over the processing operation.”[1]

2. DATA CONTROLLERS

GP Practices have been assessed to be a Data Controller.

This is because;

- They decided to collect or process the personal data.
- They decided what the purpose or outcome of the processing was to be.
- They decided what personal data should be collected.
- They decided which individuals to collect personal data about.

[1] https://ico.org.uk/media/for-organisations/documents/1546/data-controllers-and-data-processors-dp-guidance.pdf

- They make decisions about the individuals concerned as part of or as a result of the processing.
- They exercise professional judgement in the processing of the personal data.
- They have a direct relationship with the data subjects.
- They have complete autonomy as to how the personal data is processed.
- They have appointed the processors to process the personal data on their behalf

3. DATA PROCESSORS

Prescribing Services Limited has been assessed to be a Data Processor.

This is because;

- They are following instructions from someone else regarding the processing of personal data.
- They were given the personal data by a customer or similar third party, or told what data to collect.
- They do not decide to collect personal data from individuals.
- They do not decide what personal data should be collected from individuals.
- They do not decide the lawful basis for the use of that data.
- They do not decide what purpose or purposes the data will be used for.
- They do not decide whether to disclose the data, or to whom.
- They do not decide how long to retain the data.
- They may make some decisions on how data is processed, but implement these decisions under a contract with someone else.
- They are not interested in the end result of the processing.

Wellbeing Software (Apollo) has been assessed to be a Sub Processor.

This is because;

- They are following instructions from someone else regarding the processing of personal data.
- They were given the personal data by a customer or similar third party or told what data to collect.
- They do not decide to collect personal data from individuals.
- They do not decide what personal data should be collected from individuals.
- They do not decide the lawful basis for the use of that data.
- They do not decide what purpose or purposes the data will be used for.
- They do not decide whether to disclose the data, or to whom.
- They do not decide how long to retain the data.
- They may make some decisions on how data is processed, but implement these decisions under a contract with someone else.
- They are not interested in the end result of the processing.

The Bunker has also been assessed to be a Sub Processor.

This is because;

- They are following instructions from someone else regarding the processing of personal data.
- They were given the personal data by a customer or similar third party, or told what data to collect.
- They do not decide to collect personal data from individuals.
- They do not decide what personal data should be collected from individuals.
- They do not decide the lawful basis for the use of that data.
- They do not decide what purpose or purposes the data will be used for.
- They do not decide whether to disclose the data, or to whom.

- They do not decide how long to retain the data.
- They may make some decisions on how data is processed but implement these decisions under a contract with someone else.
- They are not interested in the end result of the processing.

4. THIRD PARTY RELATIONSHIPS

The PSL Account Holder (GP Practice) may engage the CCG to undertake non-clinical activities, for example contacting patients and assisting with completion of questionnaires. It is likely that this would make them a Processor, acting on behalf of the GP or CCG.

This is because

- They are following instructions from someone else regarding the processing of personal data.
- They were given the personal data by a customer or similar third party, or told what data to collect.
- They do not decide to collect personal data from individuals.
- They do not decide what personal data should be collected from individuals.
- They do not decide the lawful basis for the use of that data.
- They do not decide what purpose or purposes the data will be used for.
- They do not decide whether to disclose the data, or to whom.
- They do not decide how long to retain the data.
- They may make some decisions on how data is processed but implement these decisions under arrangements with the GP or other health provider.
- They are not interested in the end result of the processing.

Queried whether CCGs are directing activities under PRIME or whether it is largely GPs with CCGs providing some support activities

GPs and other healthcare providers may engage GP Support Organisations, Federations or other parties to undertake clinical activities such as triage or delivery of clinical support to patients identified through PRIME. This would likely mean that the GP Support Organisations or other third party providers are a Controller of the data they receive through or via PRIME.

This is because;

- They decided what the purpose or outcome of the processing was to be (i.e. onward referrals)
- They decided what personal data should be collected (for triage for example)
- They make decisions about the individuals concerned as part of or as a result of the processing.
- They exercise professional judgement in the processing of the personal data.
- They have a direct relationship with the data subjects.
- They have complete autonomy as to how the personal data is processed (as healthcare providers).

The relationships that the PSL account holder (GPs) have with those providing additional services for PRIME are out of scope for PSL. It is expected that GPs will put in place the appropriate contracts / sharing agreements in order to legitimise this additional data sharing.

Where GPs are providing access to PRIME to third parties, it is anticipated that they will make arrangements directly with those parties and advise PSL to authorise access. Similar to how third-party access is granted to clinical systems.

5. APPROPRIATE SHARING DOCUMENTS

.

“It is good practice for you to have written data sharing agreements when controllers share personal data. This helps everyone to understand the purpose for the sharing, what will happen at each stage and what responsibilities they have. It also helps you to demonstrate compliance in a clear and formal way. Similarly, written contracts help controllers and processors to demonstrate compliance and understand their obligations, responsibilities and liabilities.”2

The stakeholders have the following in place;

- A Processing Contract between GP Practices and PSL
- A Processing Contract between PSL and Apollo
- A Processing Contract between PSL and The Bunker

Arrangements with third parties are out of scope for PSL.

6. PROCESSING CONTRACT REVIEWS

In accordance with s 56 of the Data Protection Act 2018, there is a need to ensure that the legally required processing clauses are included in any contract between a Controller and Processor or Processor and Sub Processors.

Name of Supplier: PSL

Contract reviewed: PSL GP Processing Contract

Clause	Status	Comments
Is the processor required to provide, on request evidence that they have implemented appropriate technical and organisational measures to protect Personal Data including storage and transmission of data, business continuity, staff training, auditing, access control and Cyber security?	Yes	Section 2.9.5

[2] https://ico.org.uk/for-organisations/accountability-framework/contracts-and-data-sharing/

Does the contract state that the processor shall not engage another processor without prior specific or general written authorisation of the controller?	Yes	2.5
Does the contract set out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller?	Yes	Schedule 1
Does the contract stipulate that the Processor processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by law and in those cases will notify the Controller?	Yes	2.9.4
Does the contract state that all staff employed by the processor have contracts that include confidentiality clauses and that Personal Data will not be shared with third party unless required to do so by law?	Yes	Yes
Does the contract require the Processor to assist the Controller to respond to requests for exercising the data subject's rights i.e. access to information, correction of errors?	Yes	2.9.7
Does the contract require the Processor to assist the Controller in reporting information incidents promptly including where it might be required to contact the data subject?	Yes	2.9.7
Does the contract state what should happen to the data at the end of the contract or in the event of termination such as return of the data or secure destruction?	Yes	Schedule 2
Does the contract require the Processor to allow for a comply with audits including inspections conducted by the Controller or a third party engaged by the Controller?	Yes	2.10

Name of Supplier: Wellbeing Software

Contract reviewed: Apollo Services Agreement

Clause	Status	Comments
Is the processor required to provide, on request evidence that they have implemented appropriate technical and organisational measures to protect Personal Data including storage and transmission of data, business continuity, staff training, auditing, access control and Cyber security?	Yes	s 4.10.2 (c)
Does the contract state that the processor shall not engage another processor without prior specific or general written authorisation of the controller?	Yes	4.2.10 (e)
Does the contract set out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller?	Yes	Specified in the customer Project Order (separate)
Does the contract stipulate that the Processor processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by law and in those cases will notify the Controller?	Yes	s 5.8.2
Does the contract state that all staff employed by the processor have contracts that include confidentiality clauses and that Personal Data will not be shared with third party unless required to do so by law?	Yes	Yes
Does the contract require the Processor to assist the Controller to respond to requests for exercising the	Yes	4.2.10 (i)

data subject's rights i.e. access to information, correction of errors?		
Does the contract require the Processor to assist the Controller in reporting information incidents promptly including where it might be required to contact the data subject?	Yes	4.2.10 (m)
Does the contract state what should happen to the data at the end of the contract or in the event of termination such as return of the data or secure destruction?	Yes	6.3
Does the contract require the Processor to allow for a comply with audits including inspections conducted by the Controller or a third party engaged by the Controller?	Yes	4.2.10 (j)

Name of Supplier: The Bunker

Contract reviewed: The Bunker GDPR Addendum

Clause	Status	Comments
Is the processor required to provide, on request evidence that they have implemented appropriate technical and organisational measures to protect Personal Data including storage and transmission of data, business continuity, staff training, auditing, access control and Cyber security?	Yes	s 2.5.2
Does the contract state that the processor shall not engage another processor without prior specific or general written authorisation of the controller?	Yes	s 2.6
Does the contract set out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and	Yes	Data Processor Addendum

categories of data subjects and the obligations and rights of the controller?		
Does the contract stipulate that the Processor processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by law and in those cases will notify the Controller?	Yes	s 2.5.1
Does the contract state that all staff employed by the processor have contracts that include confidentiality clauses and that Personal Data will not be shared with third party unless required to do so by law?	Yes	Yes
Does the contract require the Processor to assist the Controller to respond to requests for exercising the data subject's rights i.e. access to information, correction of errors?	Yes	2.5.5
Does the contract require the Processor to assist the Controller in reporting information incidents promptly including where it might be required to contact the data subject?	Yes	s 2.5.5
Does the contract state what should happen to the data at the end of the contract or in the event of termination such as return of the data or secure destruction?	Yes	s 2.5.7
Does the contract require the Processor to allow for a comply with audits including inspections conducted by the Controller or a third party engaged by the Controller?	Yes	s 2.5.8

Lawful Processing

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)

The Health and Social Care (Safety and Quality) Act 2015: Duty to share information (HSCA)

KAFICO

INFORMATION · GOVERNANCE · CONSULTANCY

1. DEFINITIONS / CONTEXT

Controllers must have a valid lawful basis in order to process personal data.

There are six available lawful bases for processing. No single basis is 'better' or more important than the others – which basis is most appropriate to use will depend on your purpose and relationship with the individual.

Most lawful bases require that processing is 'necessary'. If Controllers can reasonably achieve the same purpose without the processing, they won't have a lawful basis.

Controllers must determine the lawful basis before they begin processing, and should document it.

Controller's privacy notices should include your lawful basis for processing as well as the purposes of the processing.

If the purposes change, Controllers may be able to continue processing under the original lawful basis if the new purpose is compatible with the initial purpose (unless the original lawful basis was consent).

If Controllers are processing special category data, they will need to identify both a lawful basis for general processing and an additional condition for processing this type of data.

2. DATA CATEGORIES

The UK GDPR / DPA 18 and EU GDPR governs the processing of data that identifies living individuals and provides that Special Categories of Data is personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, data concerning health or data concerning a natural person's sex life or sexual orientation.

The initiative involves processing of Personal Data and Special Category Data and therefore requires both a lawful basis under Art 6 UK GDPR and an condition for processing of Special Category Data

PSL as Data Processors, are not in a position to determine the purpose and means of processing. However, for the purposes of supporting customers with their assessments, the following assumptions have been made.

3. LAWFUL BASIS FOR PROCESSING PERSONAL DATA

UK GDPR Article 6 (e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

4. CONDITION FOR PROCESSING SPECIAL CATEGORY DATA

Article 9 2 (h) Health or social care (with a basis in law)

4 (a). COPI NOTICE PURPOSE

Where PRIME is being used to support activities during the pandemic, it is possible that the activities may fall under the Coronavirus (COVID-19): notice under regulation 3(4) of the Health Service (Control of Patient Information) Regulations 2002. The notice provides a number of purposes that require the dissemination of patient data and it is anticipated that the Controller will identify the appropriate purpose to support the activity involved.

5. OBLIGATIONS OF SECRECY

Both Data Protection Act 2018 and GDPR indicate that healthcare data may be processed by healthcare providers - where the law makes provision for such services (i.e. registered healthcare professionals) or by a third party “pursuant to a contract” that creates an obligation of secrecy or “a person who in the circumstances owes a duty of confidentiality”.

Controllers are permitted to delegate their processing functions to another organisation, who collect, store, retain, display, link and destroy the data on their behalf as Processors.

There is a Processing Contract in place with the Processor to ensure that they are bound to secrecy. Query an update on this to reflect the new activities for PRIME.

6. NECESSITY

As previously identified, the Controller has responsibility to ascertaining lawful basis however, the following presumptions are made.

The processing is ***necessary*** for healthcare purposes because there is a statutory duty under HSCA for healthcare providers to;

Share information between health or adult social care commissioners or providers

This project will involve sharing information between health and social care commissioners and providers

Where lawful and the individual has not objected

Any existing objections to data being processed will be observed by virtue of excluding patients that have “opted out” from the proposed activities.

For the purposes likely to facilitate the provision of health services or adults social care

The sharing will provide information that supports consultations, emergency care, diagnosis directly to the individual patient and broader healthcare management.

Where it is in the individual's best interest.

Improved and informed patient care is at the heart of the project.

7. EXPECTATIONS / COMMON LAW CONFIDENTIALITY

Whilst consent is the identified lawful basis for processing, there is a still a legal requirement to ensure that data subjects 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.

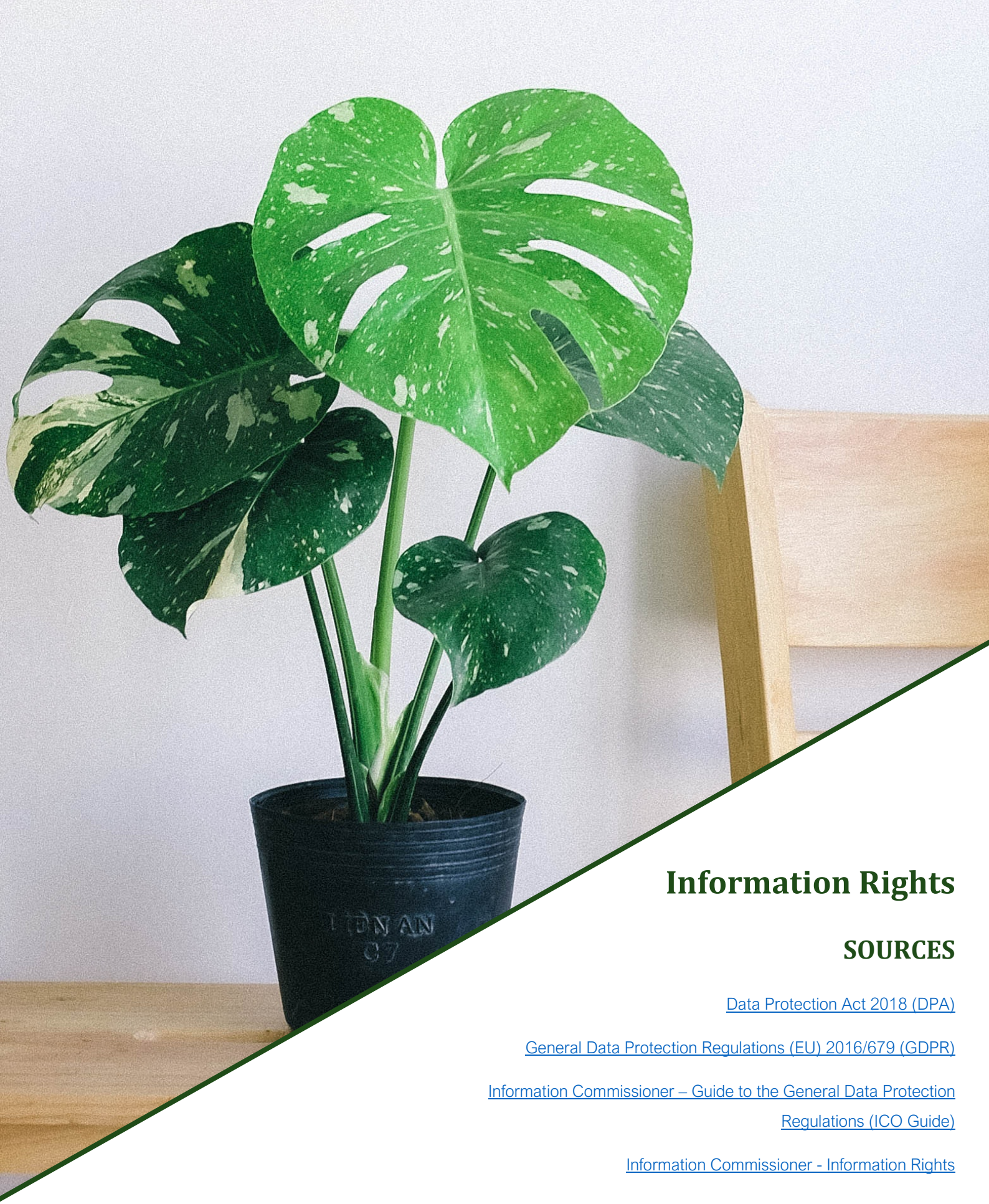
The test for a breach of confidence has developed (in correlation with the application of the Human Rights Act 1998 and Article 8 (1) of ECHR) and now concerns whether individuals have a ***reasonable expectation*** of privacy such that sharing information may constitute misuse of private information.

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

The importance of managing patient / service user expectation is further demonstrated by the introduction of the 8th Caldicott Principle which aims to ensure 'no surprises' for patients and service users by making sure providers are fully transparent.

Processors such as PSL are not considered to be a 'third party' but rather acting as a proxy for the Controller who is lawfully able to delegate their Controller activities. The customers should ensure that PSL are included as a Processor in their transparency materials.

Additionally, it is likely that customers using PRIME will be disclosing information to third party providers or allowing them access to the system and so the onus is placed on Controller customers to undertake transparency campaigns such that patient expectations are effectively managed.



Information Rights

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)

Information Commissioner - Information Rights

KAFICO

INFORMATION · GOVERNANCE · CONSULTANCY

1. DEFINITIONS / CONTEXT

The UK and EU GDPR provides the following rights for individuals: The right to be informed, the right of access, the right to rectification, the right to erasure, the right to restrict processing, the right to data portability, the right to object, rights in relation to automated decision making and profiling.

Processors are contractually bound to supporting Customer Controllers with their information rights requests by virtue of Data Processing Contract. This means that they will work to support the Controller towards a timely and complete response to any request made by data subjects.

2. FACILITATION OF INFORMATION RIGHTS

Information Right	Applies?	How Supported
Right to Access	Yes, data subjects do have a right to request access to their information under this lawful basis.	The PSL systems and architecture allows personal data to be extracted / printed and provided to data subject on request. Patients can make a request for any personal data collected by PSL through PRIME. Disclosures will be made in collaboration with the Controller customer. 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.
Rectification and Restriction	Yes, data subjects do have a right to request the rectification and restriction of their personal data under this lawful basis.	The PSL systems and architecture allows personal data to be amended / access restricted and provides an audit trail of such amendments.

		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. 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. Query whether patients' updated contact details are regularly re-extracted? Or can patients update with the NHS Patients portal?
Portability	The right to data portability only applies when your lawful basis for processing this information is consent or for the performance of a contract and so would not apply to processing under this DPIA.	Not Applicable
Erasure	The right to Erasure does not apply when processing is for Public Task and Medical Purposes and so would not apply to processing under this DPIA.	Not Applicable
Object	Yes, the data subject does have a right to object to processing of their personal data under this lawful basis.	The data subjects' ability to raise objections via the Controller is unaffected by this project. The extractions already exclude patients that have exercised objections via the NHS National Data Opt Out programme.

3. PROFILING AND AUTOMATED DECISION MAKING

Data Protection Law has provisions on:

- automated individual decision-making (making decisions solely by automated means without any human involvement) and;
- profiling (automated processing of personal data to evaluate certain things about an individual). Profiling can be part of an automated decision-making process.

Article 22 protects individuals if you are carrying out solely automated decision-making that has legal or similarly significant effects on them;

Where automated decisions are made, the Controller must give individuals information about the processing; introduce simple ways for them to request human intervention or challenge a decision; carry out regular checks to make sure that your systems are working as intended.

Profiling is: Any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects about the person including concerning health.

Patients have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning them or similarly significantly affects them.

A legal effect is something that adversely affects someone's legal rights. Similarly, significant effects are more difficult to define but would include, for example, automatic refusal of an online credit application, and e-recruiting practices without human intervention.

Article 22 applies to solely automated individual decision-making, including profiling, with legal or similarly significant effects.

If your processing does not match this definition then you can continue to carry out profiling and automated decision-making.

DETERMINATION

PSL products and services create an aggregated version of data, pulled from the Controller systems and stored by Prescribing Services and then presented to the Controller customer for use. This effectively sorts patients into particular categories for risk or health

management purposes to allow the Controller customer to make decisions about suitable interventions or healthcare management decisions, including the use of PRIME patient engagement platforms. There is clearly profiling taking place that results in a decision that will affect the care options available to the individual.

The patient, in this case, is subject to care decisions made as a result automated profiling into specific patient groups or the automated identification of risk factors.

In this case, there does not appear to be an impact on the legal rights of the individual nor any significant negative effect for those having decisions made about them. Where a clinician has identified risk and feel an intervention or care option is appropriate, the individual being profiled is likely to benefit from any decisions made. Additionally, the data subject retains choice and control about whether to take options provided to them such as referral to a third-party healthcare provider.

Since the processing does not fully match the definition, it is asserted that the Controller may proceed with processing without the additional restrictions under Article 22 and ensuring that information rights and transparency requirements are observed.

TECHNICAL AND ORGANISATIONAL MEASURES

KAFICO

INFORMATION · GOVERNANCE · CONSULTANCY

1. DEFINITIONS / CONTEXT

- Personal data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures
- While information security is sometimes considered as cybersecurity (the protection of your networks and information systems from attack), it also covers other things like physical and organisational security measures
- Measures taken should consider available technology, costs, nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons
- The controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk
- The impact of non-secure data processing can be as serious as becoming a victim or fraud or being put at risk of physical harm or intimidation
- Additionally, individuals are entitled to be protected from less serious kinds of harm like embarrassment or inconvenience
- The data should be accessed, altered, disclosed or deleted only by those authorised to do so (and that those people only act within the scope of the authority given to them);
- The data held must be accurate and complete in relation to why it is being processed; and
- The data should remain accessible and usable, i.e., if personal data is accidentally lost, altered or destroyed, Controllers should be able to recover it and therefore prevent any damage or distress to the individuals concerned.

2. PROPORTIONALITY

In accordance with the above risk assessment, the project has been defined as having a GOLD 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 – based on the nature and volume of the data being processed.

This assessment will therefore explore each of the elements drawn out within data protection legislation for mitigation of those risks such that the residual risk is low enough to support implementation.

3. SECURITY OF DATA IN TRANSIT AND AT REST

Since the project involves the transfers of data through a network architecture, this assessment has obtained a number of assurances for data in transit.

- Primary care data extracts are fully encrypted to allow secure transmission of data to the PSL high security data centre using AES 256bit encryption via TLS V1.2 secure socket connections.
- Identifiable demographic data extracted from the practice are also transmitted via TLS V1.2 secure socket connections but these also transfer within the HSCN environment only.
- SUS data transferred from the CSU to secure SFTP site hosted by Prescribing Services Ltd within the HSCN. Secure AES-256bit encryption is utilised for the transmission.
- All web access is encrypted using SSL TLS V1.2.

With regards to The Bunker (PSL owned infrastructure);

Does The Bunker network architecture utilise strong (TLS Version 1.2 or above OR IPsec or TLS VPN gateway) cryptography as defined by NIST SP800-57 to encrypt communications internally between cloud components?

Does The Bunker network architecture utilise strong (TLS Version 1.2 or above OR IPsec or TLS VPN gateway) cryptography as defined by NIST SP800-57 to encrypt communications internally between cloud data centres?

Do The Bunker or PSL undertake regular (minimum yearly) penetration testing of the communication between the Cloud and the End-user, ensuring that the Penetration test is well scoped such that ‘Data in transit' is within scope?

Does PSL undertake annual assessment against a recognised standard such as ISO to test the security of the cloud communication?

With regards to the QEH Location (HSCN);

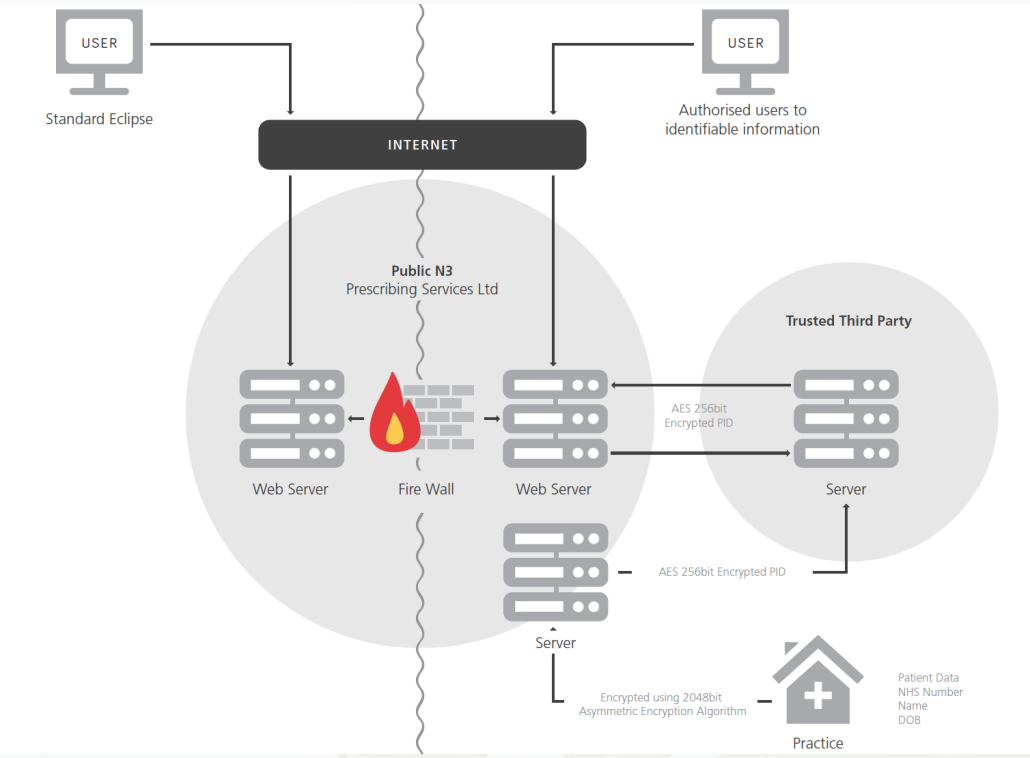
Does the QEH network architecture utilise strong (TLS Version 1.2 or above OR IPsec or TLS VPN gateway) cryptography as defined by NIST SP800-57 to encrypt communications internally between cloud components?

Does the QEH network architecture utilise strong (TLS Version 1.2 or above OR IPsec or TLS VPN gateway) cryptography as defined by NIST SP800-57 to encrypt communications internally between cloud data centres?

Do the QEH or PSL undertake regular (minimum yearly) penetration testing of the communication between the Cloud and the End-user, ensuring that the Penetration test is well scoped such that ‘Data in transit' is within scope?

Does PSL undertake annual assessment against a recognised standard such as ISO to test the security of the QEH network communication?

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



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.

This should consider the time, cost and effort necessary to do so.

The data being held at the QEH Server is;

- Eclipse No (clear)
- Name (encrypted)
- Address (encrypted)

- NHS No (encrypted)
- DOB (encrypted)

All the other data is 256-bit encrypted and they key for which is only available on another server which is hosted by PSL at their own location.

The data held at PSL servers is the linked, pooled data set ***without***;

- Name (encrypted)
- Address (encrypted)
- NHS No (encrypted)
- DOB (encrypted)

And ***with*** the Eclipse Identifier.

This information is also 256-bit encrypted but the decryption key for this information is within the same location and available to a limited number of individuals.

Practice data set extracted manually or by Wellbeing Software (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.

It is also worth noting that the data is read coded which provides another layer of protection should the information be inappropriately disclosed.

It is therefore determined that, due to the de-identification, creation of a unique integer, encryption and location of the data across multiple locations, the risk of reidentification of the data sets by a motivated intruder is low.

4. PHYSICAL SECURITY

The following security measures have been confirmed as in place for the physical locations of project data;

- Data held by PSL / The Bunker are hosted within industry standard data centres that conform to industry best practices (ISO27001) and standards for security as defined in the relevant contract terms and conditions.
- Entry to the PSL premises 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 door which is also controlled by a keypad and code and locked outside of working hours.
- The office servers and communications hardware are located in a server room which is kept locked.
- All visitors are required to sign in and out and be accompanied at all times whilst within the office premises.
- The offices include all fire fighting 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.

- There is CCTV in place

5. DATA SUBJECT USER AUTHENTICATION

In line with NIST and UK GOV guidelines and the DCB3051 Identity Verification and Authentication Standard for Digital Health and Care Services, the assurances below have been obtained.

PRIME introduces patient engagement and so, for this product, the system permits direct system access for data subjects.

When patients engage with PRIME, can they access of their own information or whether they are simply providing new information every time. Once confirmed, we will align with single or two factor authentication.

- The system provides the user with a Privacy Statement which they may review prior to access.
- Does patient access to PRIME support access by carers, parents and other proxy individuals?
- Does the PRIME proxy access functionality records what level or type of access has been granted to the proxy?
- Does the PRIME proxy access record the person granting it, when it was granted?
- Does the PRIME proxy proxy access functionality record the person the person to whom it was granted?
- Does the PRIME proxy access functionality record other pertinent information such as consent, justification (for example: Power of Attorney for Health and Care), or response to coercion questions?
- Does the PRIME data subject interface allow the user to see when the credentials were last used, such that a potential or actual exposure / misuse of credentials (username or password for example) is highlighted?

- For the purposes of two factor authentication, the patient is required to provide;
    1. Something they know: NHS Number.
    2. Something they have: Code sent via letter.
- Queried the above with JY since the code now seems to be absent and instead the user is providing another of the same factor - DOB.
- Which measures are in place to prevent replay attacks?
- If a data subject enters their account details incorrectly, does the system conceal whether they got the username or password wrong? At the moment, it looks as if it tells the user that it's the NHS Number they got wrong.

6. SYSTEM AUDIT

The project introduces a new system or software and so there is a need to ensure that the audit functionality for the asset is appropriate such that transparency is supported and Administrators have the necessary oversight.

The following assurances have been sought and obtained;

- The system / software enables and supports investigations for any reason (e.g. inappropriate access or cyber security incident)
- The system / software allows identification of any changes which have been made to clinical or administrative data, Patient/Service User data. This includes identifying what changes were made, by what user and at what time.
- Does PRIME allow monitoring of whether access controls are working as intended. Administrators may audit the movements of all staff, so it is possible to check that they are not accessing areas which they shouldn't be, or seeing things or doing things they shouldn't be?

- Does PRIME satisfy the data subject's legal right to see who has accessed or modified their record, because the audit trail includes who, when and why that user accessed the information?
- Does the PRIME audit trail include updates, backups, any maintenance activities or reference data changes (e.g. an update to the clinical coding scheme data or adding in a drug data base)?
- For PRIME, is there a way of viewing, or restoring an individual Patient/Service User record as it was on any previous date. Using something like “version history” or “snapshots”?
- For PRIME does successful login audit data include User id, date and time (to the second)?
- For PRIME, does unsuccessful login audit data include number of attempts, Date and time, Access point (if available), User id (if available)?
- Does the PRIME Password Change audit data include user id, User whose password was changed, Date and time, end-user device (or Solution) identification information?

7. PROFESSIONAL USERS - AUTHENTICATION

To ensure that the authentication of professional users of the system is in line with Gov.UK and NIST standards, the following assurances have been sought and confirmed;

- For PRIME, is the professional user log in single or two factor? Please describe.
- For PRIME professional users, is the password at least 8 characters long but does NOT set a maximum length?
- For PRIME, does the system prevent the use of commonly used passwords?
- For PRIME professional users, when password is changed, does the user receive an alert making them aware that their password has recently been changed?
- For PRIME, does the system explain the password constraints to professional users?

- For PRIME, does the system gives professional users between 5 and 10 attempts to enter their password correctly before locking their account or do any further security checks?
- For PRIME, does the system hide professional user passwords by default
- For PRIME, does the system allow the professional user to paste their password?
- For PRIME are the Passwords of professional users stored salted and hashed, using algorithms and strengths recommended in NIST Cryptography Standards?
- When a professional user logs into PRIME, are they able to see when the credentials were last used?
- For PRIME, when a professional user enters their account details incorrectly, does the system conceal whether they got the username or password wrong?
- For PRIME, when locked out or changing password, the professional user is sent a time-limited password-reset code to the phone number or email that they registered with that does not use password reset questions and does not use password reminders?
- For PRIME, when a password is changed, does the professional user receive an alert making them aware that their password has recently been changed?
- The software allows different privileges for different job roles
- For PRIME, when a professional user is logged in, does the role that they are logged in under present itself on screen throughout their use of the system?
- For PRIME, when a professional user is logged in, does the organisation that they are logged in under present itself on screen throughout their use of the system?
- For PRIME, can professional users have more than one role. For example, they might be Privacy Officer and GP?

It has been confirmed that the system providers would only ever access personal data in the following scenarios;

Please confirm the limited scenarios in which PSL would access personal data held on behalf of the customer for PRIME.

8. COOKIE COMPLIANCE

“You must tell people if you set cookies, and clearly explain what the cookies do and why. You must also get the user’s consent. Consent must be actively and clearly given.

There is an exception for cookies that are essential to provide an online service at someone’s request (eg to remember what’s in their online basket, or to ensure security in online banking). The same rules also apply if you use any other type of technology to store or gain access to information on someone’s device.” ICO Cookie Guidelines

Following a review of the cookies being collected in relation to the service or system, the following assurances have been sought and obtained;

- Queried what cookies their online service either already uses or intends to use.
- Queried whether they have removed any cookies that aren't needed
- Queried whether they have confirmed the purposes of each cookie.
- Queried whether they have Identified what information each cookie processes, including whether they are linked to other information held about users or otherwise involve processing personal data.
- Queried whether they have confirmed whether cookies are session or persistent
- Queried whether they have confirmed whether cookies are first party or third party cookies.
- Queried whether they have appropriate arrangements in place for the use of any third-party cookies, including what information they share with any third party, how it is shared, and what users are told.
- Queried whether they have established how long cookies last and that this duration is appropriate.

- Queried whether they have identified cookies that are strictly necessary, and those that are not.
- Query whether they provide clear and easy to understand information about the cookies used
- Queried whether information is comprehensive and covers all the cookies used
- Queried whether consent mechanism that allows users of our online service to control the setting of all cookies that are not strictly necessary.
- Queried whether consent mechanism ensures the consent obtained is in line with the UK GDPR's requirements.
- Queried whether they keep any records of cookie consent for an appropriate period of time.
- Queried whether cookie process is fully documented
- Queried whether they have built in an appropriate review period.

9. COLLECTION OF DEVICE DATA

The following device / user information is collected, and a lawful basis has been identified for each.

Data Collected	Justification for Collection	Strictly Necessary (functional?)	Consent?	Legitimate interests?	LIA (fraud prevention, network and information security or

					indicating possible criminal acts or threats to public security)
Queried whether device network information is collected					
Queried whether device operating system data is collected					
Queried whether they collect data about Type of web browser used to access the Site					
Queried whether they collect Time zone setting					

Queried whether they collect Geographic location information					
Queried whether they collect details of use of the App / Site and the resources that user accesses					
Queried whether they collect domain server data, including IP Address					
Queried whether they collect Type of device browser used					
Queried whether they collect					

Type of device browser used					
Queried whether they collect data about Referring source which may have sent user to the Site					
["Queried whether they collect Other information associated with the interaction of the browser and the Site and cookies."]					

10. INTERNATIONAL TRANSFERS

No personal data is transferred outside of the UK for PRIME.

11. DUE DILIGENCE

The stakeholders have achieved the following accreditations that assist to reduce the risk to the rights and freedoms of data subjects;

- PSL has completed a compliant NHS Data Protection and Security Toolkit for the current year available at PSL Toolkit
- PSL has achieved ISO27001 accreditation – certificate number 1412892
- Wellbeing Software has completed a compliant NHS Data Protection and Security Toolkit for the current year available at Wellbeing Toolkit
- Wellbeing Software has achieved ISO27001 accreditation as confirmed via Wellbeing ISO27001
- The Bunker has submitted a compliant NHS Data Protection and Security Toolkit for the current year available at The Bunker Toolkit
- The Bunker has achieved ISO27001 accreditation as confirmed via The Bunker ISO27001

As part of the impact assessment, a review of media coverage was undertaken to determine whether there have been reports of breaches or complaints relating to suppliers or partners involve in the service delivery.

At the time of writing, the stakeholders had no media presence with regards to data breaches

Checks have been undertaken with regards to the UK Information Commissioner and all parties, where relevant, are registered and their registrations are below

- PSL are registered with the ICO under the registration number Z2536678
- Wellbeing Software are registered with the ICO under the registration number ZA640896

- The Bunker are registered with the ICO under the registration number Z8856975

The stakeholders have identified the following leads for data protection matters;

- Prescribing Services Ltd - Emma Cooper - emma.cooper@kafico.co.uk
- Wellbeing Software - wellbeingservice@wellbeingsoftware.com
- The Bunker - Christopher.scott@thebunker.net

PSL have policies that cover the following subjects;

- Information Governance
- Data Protection Impact Assessments
- Data Subject Rights
- Information Incidents
- Information Security
- Privacy / Confidentiality
- Risk and Audit

All employees of PSL have clauses within their contracts that include confidentiality and compliance with company Information Governance Policies.

All PSL employees that access personal data as part of their role have Data Protection and Security Training each year.